Форма № 24

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Комп'ютерних наук і технологій
(повне найменування факультету)

Комп'ютерні системи та мережі
(повне найменування кафедри)

Пояснювальна записка

до дипломного проєкту (роботи)
бакалаврський
(ступінь вищої освіти)

на тему РОЗРОБКА СУЧАСНОЇ МЕРЕЖІ ЗВО ІЗ ЗАСТОСУВАННЯМ MESH ТЕХНОЛОГІЇ

Виконав: студент 4 курсу, групи КНТ-522
Спеціальності 123 Комп'ютерна інженерія
(код і найменування спеціальності)
Освітня програма (спеціалізація)
Комп'ютерна інженерія

ЗАЙЦЕВ О. В.
(прізвище та ініціали)
Керівник КИРИЧЕК Г.Г.
(прізвище та ініціали)
Рецензент ТЯГУНОВ Д. В.
(прізвище та ініціали)

м. Запоріжжя
2026 рік

Форма № 25

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»
(повне найменування вищого навчального закладу)

Факультет Комп'ютерних наук і технологій
Кафедра комп'ютерних систем та мереж
Ступінь вищої освіти бакалаврський
Спеціальність 123 Комп'ютерна інженерія
(код і найменування)
Освітня програма (спеціалізація) Комп'ютерна інженерія
(назва освітньої програми (спеціалізації)

ЗАТВЕРДЖУЮ
Завідувач кафедри КУДЕРМЕТОВ Р.К.
_____
«14» квітня 2026 року

З А В Д А Н Н Я

НА ДИПЛОМНИЙ ПРОЄКТ (РОБОТУ) СТУДЕНТА(КИ)

ЗАЙЦЕВУ Олександру Віталійовичу
(прізвище, ім'я, по батькові)

1. Тема проєкту (роботи) Розробка сучасної мережі ЗВО із застосуванням mesh технології
керівник проєкту (роботи) к.т.н., доцент, КИРИЧЕК Г.Г.,
(науковий ступінь, вчене звання, ПРІЗВИЩЕ, ім'я, по батькові)
затверджені наказом закладу вищої освіти від « 14 » квітня 2026 року № 160
2. Строк подання студентом проєкту (роботи) 01.06.2026 р.
3. Вихідні дані до проєкту (роботи): проєктування мережевої інфраструктури закладу вищої освіти із застосуванням mesh-технологій. Стандарти та технології: Wi-Fi 6 (IEEE 802.11ax), Gigabit Ethernet, PoE, VLAN, Inter-VLAN Routing, NAT/PAT. Програмне забезпечення: GNS3, MS Windows 10. Протоколи та сервіси: OSPF, DHCP, DNS, RADIUS, AAA. Обладнання: маршрутизатор Cisco ISR 4331, комутатор ядра Cisco Catalyst 9300, комутатори доступу Cisco Catalyst 9200L-24P), внутрішні точки доступу Cisco Catalyst 9120AXI, зовнішні mesh-вузли Cisco Catalyst 1562I, контролер бездротової мережі Cisco Catalyst 9800-L, міжмережевий екран Cisco Firepower 1010, AD/RADIUS, файловий сервер, сервер моніторингу.
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) Технічне завдання та вимоги до мережі. Технології, стандарти, протоколи та вибір обладнання. Проєктування мережі ЗВО із застосуванням mesh технологій. Налаштування мереж і міжмережевих з'єднань.

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

6. Консультанти розділів проекту (роботи)

Розділ	ПРІЗВИЩЕ, ініціали та посада консультанта	Підпис, дата	
		завдання видав	прийняв виконане завдання
1-4	КИРИЧЕК Г.Г.		
Нормоконтроль	ГОЛУБ Т.В.		

7. Дата видачі завдання «14» квітня 2026 року.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1	Аналіз технічного завдання	18.04.2026	
2	Визначення та аналіз вимог до структури mesh-мережі	22.04.2026	
3	Проєктування моделі. Постановка завдань	24.04.2026	
4	Вибір технологій та обладнання	28.04.2026	
5	Розробка функціональної схеми мережі	01.05.2026	
6	Проєктування мережі в системі моделювання	05.05.2026	
7	Налаштування мережевих з'єднань в приміщеннях університету	12.05.2026	
8	Налаштування міжмережевих з'єднань та виходу до мережі Інтернет	22.05.2026	
9	Оформлення пояснювальної записки	25.05.2026	
10	Проходження нормоконтролю	27.05.2026	
11	Перевірка на наявність академічного плагіату	28.05.2026	
12	Проходження рецензування	01.06.2026	

Студент(ка) _____ Олександр ЗАЙЦЕВ
(підпис) (Ім'я ПРІЗВИЩЕ)

Керівник проєкту (роботи) _____ Галина КИРИЧЕК
(підпис) (Ім'я ПРІЗВИЩЕ)

РЕФЕРАТ

Пояснювальна записка до дипломної кваліфікаційної роботи бакалавра: 87 с., 1 табл., 36 рис., 2 дод., 28 джерел.

КОМП'ЮТЕРНА МЕРЕЖА, WI-FI, MESH-СИСТЕМИ, MESH, GRAPHICAL NETWORK SIMULATOR, CISCO, МАРШРУТИЗАТОР, КОМУТАТОР, DHCP, DNS, IP-АДРЕСА, MAC-АДРЕСА

Об'єктом розробки є процес проєктування мережевої інфраструктури закладу вищої освіти із застосуванням бездротових mesh-технологій.

Метою роботи є проєктування та моделювання сучасної кампусної мережі закладу вищої освіти з використанням технології Wi-Fi Mesh для забезпечення надійного бездротового покриття, централізованого управління мережею та високої відмовостійкості в межах чотирьох навчальних корпусів. Предметом дослідження є моделі, методи та технології побудови бездротових mesh-мереж на базі обладнання Cisco та їх моделювання у середовищі GNS3.

Для реалізації мережі застосовано сучасні мережеві технології: VLAN для логічної сегментації мережі, зокрема IEEE 802.1Q для підтримки транкових з'єднань; Gigabit Ethernet для організації високошвидкісних дротових з'єднань. Для маршрутизації та мережевих сервісів реалізована робота протоколів OSPF, DHCP, DNS, NAT/PAT та механізми автентифікації на базі RADIUS.

Мережеве обладнання: маршрутизатор Cisco ISR 4331; комутатори Cisco Catalyst 9300 та Cisco Catalyst 9200L; внутрішні точки доступу Cisco Catalyst 9120AXI; зовнішні mesh-вузли Cisco Catalyst 1562I; контролер бездротової мережі Cisco Catalyst 9800-L; міжмережевий екран Cisco Firepower 1010, а також серверна інфраструктура, яка включає сервер автентифікації AD/RADIUS, файловий сервер та сервер моніторингу мережі.

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

VLAN	–	Virtual Local Area Network, віртуальна локальна мережа
Wi-Fi	–	Wireless Fidelity, технологія бездротового доступу до мережі
MESH	–	бездротова мережа з багатоточковою топологією з'єднань
WLC	–	Wireless LAN Controller, контролер бездротової мережі
AP	–	Access Point, точка бездротового доступу
SSID	–	Service Set Identifier, ідентифікатор бездротової мережі
OSPF	–	Open Shortest Path First, протокол динамічної маршрутизації
DHCP	–	Dynamic Host Configuration Protocol, протокол автоматичної видачі IP-адрес
DNS	–	Domain Name System, система доменних імен
NAT	–	Network Address Translation, трансляція мережевих адрес
PAT	–	Port Address Translation, трансляція адрес із використанням номерів портів
RADIUS	–	Remote Authentication Dial-In User Service, служба централізованої автентифікації користувачів
AAA	–	Authentication, Authorization and Accounting, автентифікація, авторизація та облік
LAN	–	Local Area Network, локальна обчислювальна мережа
WLAN	–	Wireless Local Area Network, бездротова локальна мережа
IP	–	Internet Protocol, міжмережевий протокол
TCP/IP	–	Transmission Control Protocol / Internet Protocol, стек мережевих протоколів
IEEE	–	Institute of Electrical and Electronics Engineers, Інститут інженерів з електротехніки та електроніки
PoE	–	Power over Ethernet, технологія передавання електроживлення через мережевий кабель

ВСТУП

Сучасний розвиток інформаційно-комунікаційних технологій, зокрема мережевих рішень і цифрових освітніх платформ, значно підвищує вимоги до інфраструктури передачі даних у закладах вищої освіти. Особливо це актуально для університетів, де необхідна безперервна обробка та передача значних обсягів інформації, включаючи доступ до електронних навчальних ресурсів, систем дистанційного навчання, внутрішніх інформаційних сервісів, а також забезпечення стабільного зв’язку між адміністративними, навчальними та науковими підрозділами.

Ефективне функціонування сучасного закладу вищої освіти неможливе без надійної, високошвидкісної та масштабованої мережі передачі даних, яка забезпечує стабільний доступ до локальних ресурсів і мережі Інтернет для студентів, викладачів та персоналу. З огляду на значну територію навчальних корпусів, велику кількість користувачів та потребу в мобільності, особливої актуальності набуває застосування сучасних бездротових технологій, зокрема mesh-мереж. Такі мережі забезпечують безперервне покриття, автоматичну маршрутизацію трафіку та здатність до самовідновлення при відмові вузлів.

Проєктування мережі вузу із застосуванням mesh-технологій передбачає визначення оптимальної топології, вибір мережевого обладнання (маршрутизаторів, комутаторів, точок доступу та mesh-вузлів), налаштування IP-адресації, сегментацію мережі, а також забезпечення необхідного рівня безпеки, надійності та можливості подальшого масштабування. Важливим аспектом є забезпечення рівномірного бездротового покриття навчальних аудиторій, лабораторій, бібліотек і адміністративних приміщень.

У першій частині роботи проведено аналіз предметної області та технічного завдання на проєктування мережевої інфраструктури закладу вищої освіти. Розглянуто особливості функціонування сучасних інформаційно-комунікаційних мереж у ЗВО, проаналізовано існуючі підходи до організації

бездротового доступу та застосування Mesh-технологій. Визначено основні вимоги до мережевої інфраструктури та сформульовано завдання, які необхідно вирішити в процесі проєктування.

У другій частині роботи розглянуто технології, стандарти та протоколи, що використовуються під час побудови сучасних комп'ютерних мереж. Проведено аналіз технології Mesh, стандартів сімейства IEEE 802.11, мережевих протоколів та служб. Виконано вибір мережевого обладнання, зокрема маршрутизаторів, комутаторів та бездротових точок доступу, необхідних для реалізації проєкту.

У третій частині роботи розроблено проєкт мережевої інфраструктури закладу вищої освіти, що складається з двох навчальних корпусів. Побудовано функціональну та структурну схеми мережі, виконано проєктування топології мережі, розміщення комутаційного обладнання та бездротових точок доступу. Також розроблено схему організації Mesh-покриття навчальних корпусів та виконано моделювання мережі.

Четверта частина роботи присвячена налаштуванню та адмініструванню мережі. Виконано налаштування маршрутизаторів Cisco, DHCP-сервера, комутаторів та бездротових точок доступу. Розглянуто питання організації маршрутизації мережевого трафіку, забезпечення мережевої безпеки, моніторингу та адміністрування мережі. Проведено тестування працездатності спроєктованої мережі та оцінку її відповідності поставленим вимогам.

Практична цінність роботи полягає у розробці проєкту сучасної мережевої інфраструктури закладу вищої освіти із застосуванням Mesh-технологій, який може бути використаний під час модернізації існуючих або створення нових мереж навчальних закладів. Запропоноване рішення забезпечує стабільне бездротове покриття навчальних корпусів, підтримку мобільності користувачів, централізоване адміністрування мережі та можливість подальшого масштабування інфраструктури.

1 ТЕХНІЧНЕ ЗАВДАННЯ ТА ВИМОГИ ДО МЕРЕЖІ

1.1 Поняття та принципи роботи mesh-технологій

Mesh-технології є сучасним підходом до організації бездротових мереж, за якого вузли взаємодіють між собою без обов’язкового використання централізованого керування. У таких мережах кожен вузол (mesh-вузол) виконує не лише функції приймання та передачі даних, але й бере участь у процесі маршрутизації, забезпечуючи ретрансляцію пакетів для інших вузлів розподіленої мережі [1].

Основною особливістю mesh-мереж є їх децентралізована структура, яка відрізняється від традиційних інфраструктурних мереж із єдиною точкою доступу. У mesh-мережі відсутній єдиний центральний вузол, від якого залежить робота всієї мережі. Це дозволяє значно підвищити надійність і стійкість до відмов, оскільки вихід з ладу окремого вузла не призводить до повної втрати зв’язку [2].

Принцип роботи mesh-мереж базується на динамічній маршрутизації даних. Кожен вузол мережі постійно обмінюється інформацією про стан з’єднань із сусідніми вузлами, що дозволяє визначати оптимальні маршрути передачі даних. У разі зміни топології мережі або відмови одного з вузлів маршрути автоматично перебудовуються, забезпечуючи безперервність передачі інформації [3].

Передача даних у mesh-мережі може здійснюватися через декілька проміжних вузлів, що дозволяє розширювати зону покриття без необхідності прокладання додаткових кабельних ліній. Це особливо актуально для великих територій, таких як університетські кампуси, де необхідно забезпечити стабільний зв’язок у різних будівлях та приміщеннях.

До основних принципів роботи mesh-технологій належать:

– самоорганізація – вузли автоматично виявляють один одного та формують мережу;

– самовідновлення – у разі відмови вузлів мережа автоматично перебудовується;

– багатошляхова маршрутизація – наявність декількох альтернативних маршрутів передачі даних;

– масштабованість – можливість додавання нових вузлів без значної зміни існуючої структури.

Таким чином, використання mesh-технологій дозволяє створювати гнучкі, надійні та масштабовані мережі передачі даних, що є особливо важливим для сучасних закладів вищої освіти, де необхідно забезпечити безперервний доступ до інформаційних ресурсів великої кількості користувачів.

1.2 Класифікація mesh-технологій

Mesh-технології є перспективним підходом до побудови розподілених мережевих інфраструктур і можуть бути класифіковані за низкою ознак, зокрема за способом організації топології, типом фізичного середовища передавання даних, функціональним призначенням вузлів, а також масштабом та межами застосування. Така багатовимірна класифікація дозволяє здійснювати обґрунтований вибір архітектури мережі відповідно до вимог щодо продуктивності, надійності, масштабованості, вартості впровадження та умов експлуатації (рис.1.1).

За способом організації топології мережі розрізняють такі типи mesh-мереж:

– повнозв’язна mesh-топологія (Full Mesh) – характеризується наявністю прямого з’єднання між кожною парою вузлів мережі;

– часткова mesh-топологія (Partial Mesh) – передбачає наявність з’єднань лише між окремими вузлами мережі, як правило, найбільш критичними або територіально наближеними.

Повнозв’язна архітектура забезпечує максимальний рівень відмовостійкості, мінімальні затримки передачі даних та відсутність єдиних точок відмови. Водночас її реалізація супроводжується значними витратами мережевих ресурсів, складністю адміністрування та експоненційним зростанням кількості з’єднань зі збільшенням числа вузлів, що обмежує її практичне застосування у великих мережах.

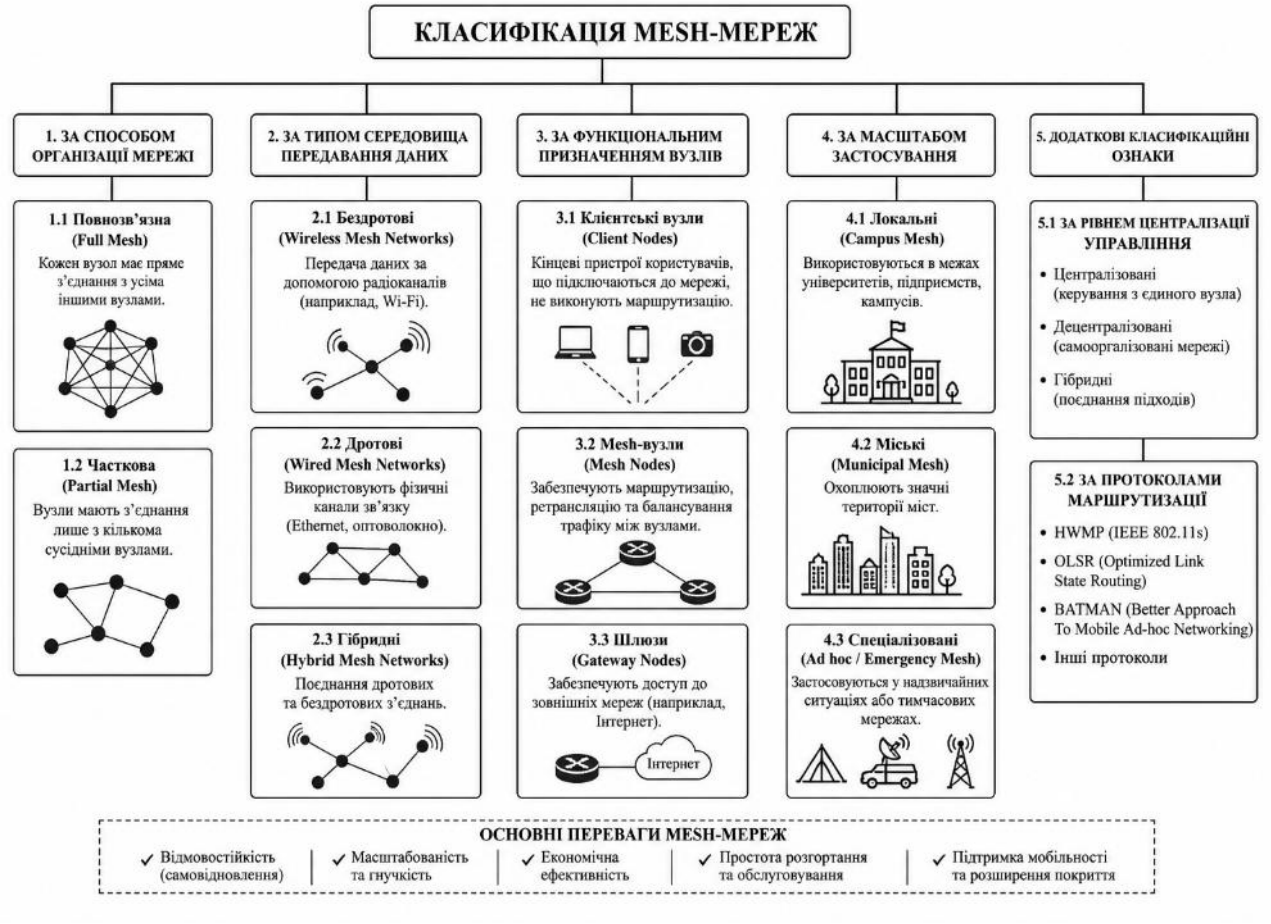


Рисунок 1.1 – Використання mesh-технологій

Підхід із застосуванням часткової mesh-топології дозволяє досягти раціонального компромісу між рівнем надійності функціонування мережі та економічною доцільністю її впровадження і супроводу. На відміну від повнозв’язної топології, де кількість з’єднань зростає експоненційно разом із кількістю вузлів, часткова mesh-архітектура передбачає встановлення з’єднань лише між найбільш важливими або територіально наближеними вузлами. Це

суттєво знижує складність побудови та адміністрування мережевої інфраструктури, а також зменшує витрати на обладнання, прокладання каналів зв’язку та їх обслуговування.

Водночас зберігається достатній рівень відмовостійкості, оскільки наявність альтернативних маршрутів передачі даних забезпечує можливість автоматичного перенаправлення трафіку у разі виходу з ладу окремих вузлів або каналів зв’язку [4]. Таким чином, часткова mesh-топологія забезпечує баланс між ефективністю використання ресурсів, гнучкістю масштабування мережі та надійністю її функціонування, що робить її доцільною для застосування у складних розподілених системах, зокрема в мережах закладів вищої освіти.

За типом фізичного середовища передачі даних mesh-мережі класифікуються як:

– бездротові mesh-мережі (Wireless Mesh Networks, WMN);
– дротові mesh-мережі;
– гібридні mesh-мережі.

Бездротові – використовують радіоканали зв’язку (переважно на базі стандартів IEEE 802.11) для організації взаємодії між вузлами. Вони характеризуються високою гнучкістю розгортання, мобільністю та відносно низькими витратами на інфраструктуру, проте можуть бути чутливими до перешкод, перевантажень ефіру та впливу зовнішніх факторів.

Дротові – базуються на використанні фізичних каналів зв’язку, таких як Ethernet або волоконно-оптичні лінії. Вони забезпечують високу пропускну здатність, стабільність з’єднання та низький рівень затримок, однак характеризуються меншою гнучкістю та вищою вартістю розгортання.

Гібридні mesh-мережі – поєднують переваги дротових і бездротових технологій. У таких мережах дротова інфраструктура зазвичай використовується як магістральний сегмент (backbone), тоді як бездротові вузли забезпечують доступ кінцевих користувачів. Це дозволяє оптимізувати баланс між продуктивністю, надійністю та вартістю.

За функціональним призначенням вузлів у mesh-мережах виділяють: клієнтські вузли (Client Nodes); mesh-вузли (Mesh Nodes або Mesh Routers) та шлюзи (Gateway Nodes) [5].

Клієнтські вузли це кінцеві пристрої користувачів (ноутбуки, смартфони, IoT-пристрої), які здійснюють доступ до мережевих ресурсів, але, як правило, не беруть участі в маршрутизації трафіку. Mesh-вузли є ключовими елементами мережі, які виконують функції маршрутизації, ретрансляції та балансування трафіку між іншими вузлами. Вони формують самоконфігуровану та самовідновлювану мережеву структуру. Шлюзи – спеціалізовані вузли, які забезпечують інтеграцію mesh-мережі із зовнішніми мережами, зокрема з мережею Інтернет або корпоративними сегментами, виконуючи функції трансляції адрес, фільтрації трафіку та забезпечення безпеки [6]. За масштабом застосування mesh-мережі поділяються на: локальні (campus mesh); міські (municipal mesh) та спеціалізовані (ad hoc / emergency mesh).

Локальні розгортаються в межах окремих організацій, зокрема закладів вищої освіти, підприємств або кампусів, забезпечуючи покриття обмеженої території з високою щільністю користувачів. Міські охоплюють значні території населених пунктів і використовуються для організації публічного доступу до мережі, систем відеоспостереження, «розумного міста» тощо. Спеціалізовані застосовуються в умовах надзвичайних ситуацій, військових операцій або тимчасових заходів, де відсутня стаціонарна інфраструктура зв’язку [7].

Додатково доцільно враховувати класифікацію за рівнем централізації управління (централізовані, децентралізовані та гібридні системи), а також за використовуваними протоколами маршрутизації (HWMP, OLSR, BATMAN), які безпосередньо впливає на ефективність функціонування мережі.

Таким чином, різноманіття підходів до класифікації mesh-мереж свідчить про їхню високу адаптивність до різних умов застосування [8]. Для побудови мережевої інфраструктури закладу вищої освіти найбільш доцільним є використання бездротової або гібридної часткової mesh-архітектури, яка забезпечує оптимальне поєднання відмовостійкості, масштабованості, гнучкості

розгортання та економічної ефективності, що є критично важливим в умовах динамічного зростання кількості користувачів і мережевих сервісів [9].

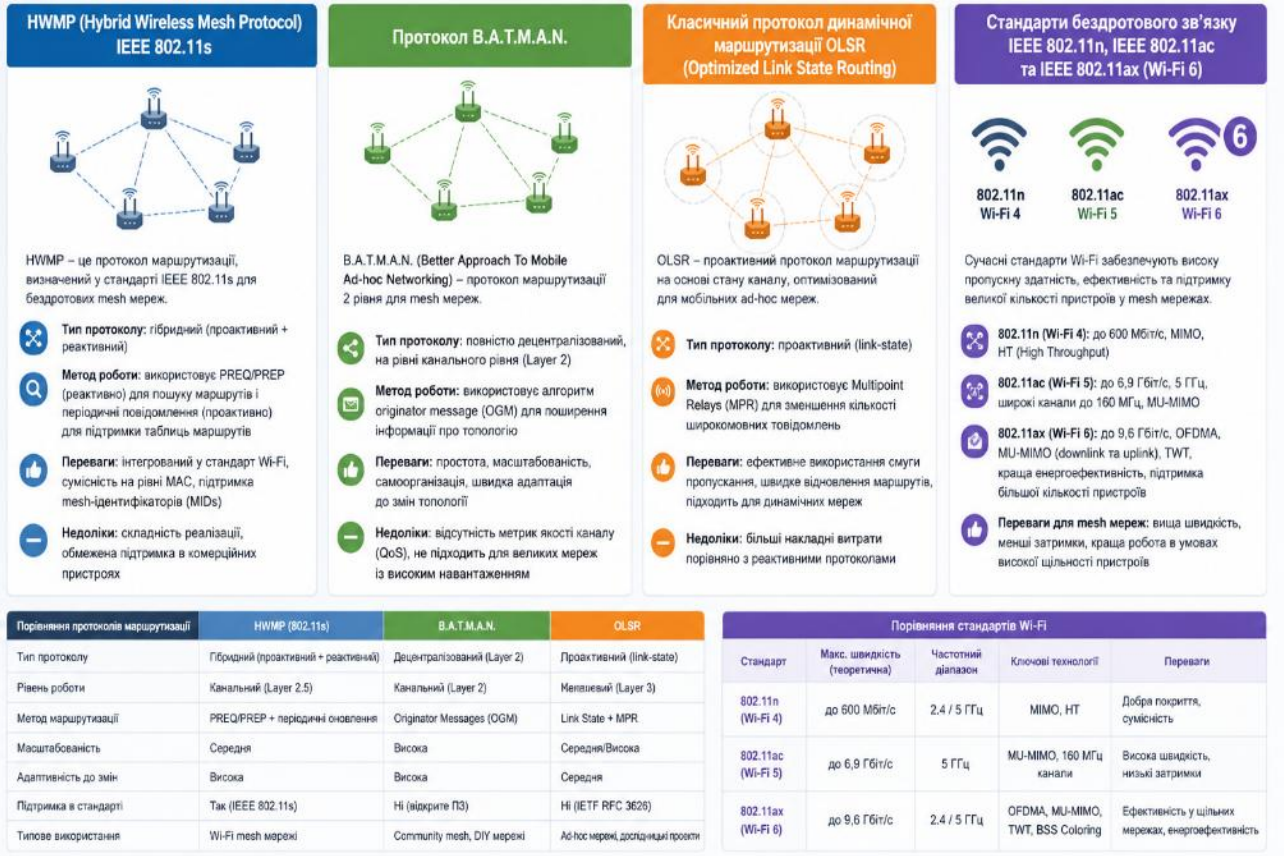
1.3 Аналіз сучасних стандартів mesh-мереж

Сучасні mesh-мережі базуються на стандартах та протоколах, що забезпечують ефективну передачу даних, динамічну маршрутизацію та адаптацію до змін топології мережі. Використання відповідних стандартів є ключовим фактором для забезпечення стабільності, продуктивності та масштабованості мережі, особливо в умовах значної кількості користувачів, як у закладах вищої освіти. Одним із основних стандартів, що регламентує роботу бездротових mesh-мереж, є IEEE 802.11s. Даний стандарт є розширенням сімейства IEEE 802.11 і визначає механізми організації mesh-мереж на канальному рівні. Він забезпечує автоматичне виявлення вузлів, побудову маршрутів та передачу даних між ними без необхідності використання централізованого керування. У межах цього стандарту використовується протокол HWMP (Hybrid Wireless Mesh Protocol), який поєднує проактивні та реактивні методи маршрутизації [10].

Іншим поширеним підходом до організації mesh-мереж є використання протоколу B.A.T.M.A.N. На відміну від традиційних протоколів маршрутизації, B.A.T.M.A.N. не зберігає повну інформацію про всі маршрути в мережі, а визначає лише найкращий напрямок передачі даних. Це дозволяє зменшити навантаження на вузли та підвищити стійкість мережі до змін топології.

Також у mesh-мережах можуть використовуватися класичні протоколи динамічної маршрутизації, такі як OLSR (Optimized Link State Routing). Цей протокол є проактивним і забезпечує постійне оновлення маршрутної інформації між вузлами мережі. Його перевагою є швидка реакція на зміни, однак він може створювати додаткове навантаження на мережу через регулярний обмін

службовими повідомленнями [11]. В ході роботи проведено аналіз основних протоколів маршрутизації Mesh-мереж - HWMP, B.A.T.M.A.N. та OLSR, а також сучасних стандартів бездротового зв’язку IEEE 802.11n, IEEE 802.11ac та IEEE 802.11ax, які відрізняються швидкістю передачі даних, ефективністю використання радіоканалу та підтримкою сучасних технологій (рис. 1.2).



Порівняння протоколів маршрутизації	HWMP (802.11s)	B.A.T.M.A.N.	OLSR
Тип протоколу	Гібридний (проактивний + реактивний)	Децентралізований (Layer 2)	Проактивний (link-state)
Рівень роботи	Канальний (Layer 2.5)	Канальний (Layer 2)	Мережевий (Layer 3)
Метод маршрутизації	PREQ/PREP + періодичні оновлення	Originator Messages (OGM)	Link State + MPR
Масштабованість	Середня	Висока	Середня/Висока
Адаптивність до змін	Висока	Висока	Середня
Підтримка в стандарті	Так (IEEE 802.11s)	Ні (відкрите ПЗ)	Ні (IETF RFC 3626)
Типове використання	Wi-Fi mesh мережі	Community mesh, DIY мережі	Ad-hoc мережі, дослідницькі проекти

Порівняння стандартів Wi-Fi				
Стандарт	Макс. швидкість (теоретична)	Частотний діапазон	Ключові технології	Переваги
802.11n (Wi-Fi 4)	до 600 Мбіт/с	2.4 / 5 ГГц	MIMO, HT	Добра покриття, сумісність
802.11ac (Wi-Fi 5)	до 6,9 Гбіт/с	5 ГГц	MU-MIMO, 160 МГц канали	Висока швидкість, низькі затримки
802.11ax (Wi-Fi 6)	до 9,6 Гбіт/с	2.4 / 5 ГГц	OFDMA, MU-MIMO, TWT, BSS Coloring	Ефективність у щільних мережах, енергоефективність

Рисунок 1.2 – Аналіз основних протоколів

Окрім спеціалізованих mesh-протоколів, суттєве значення мають сучасні стандарти бездротового зв’язку, зокрема IEEE 802.11n, IEEE 802.11ac та IEEE 802.11ax (Wi-Fi 6), які регламентують роботу фізичного та канального рівнів передачі даних. Їх застосування забезпечує підвищену пропускну здатність, зменшення затримок, а також стабільну роботу мережі за умов великої кількості одночасно підключених пристроїв.

Порівняльний аналіз сучасних рішень свідчить, що кожен зі стандартів і протоколів має власні переваги та певні обмеження. Так, IEEE 802.11s виступає

як базовий стандарт для побудови бездротових mesh-мереж, тоді як протокол B.A.T.M.A.N. характеризується високою адаптивністю та ефективністю функціонування в умовах динамічної зміни топології мережі. У свою чергу, протокол OLSR є більш доцільним для використання в мережах зі стабільною або малозмінною структурою.

Отже, вибір конкретного стандарту бездротового зв'язку та протоколу маршрутизації для mesh-мережі визначається умовами її експлуатації та вимогами до продуктивності. Для інформаційної інфраструктури закладу вищої освіти найбільш обґрунтованим є застосування IEEE 802.11s у поєднанні із сучасними технологіями Wi-Fi, що дозволяє забезпечити надійність, масштабованість і високу ефективність функціонування мережі.

1.4 Особливості застосування mesh-мереж у закладі вищої освіти

Використання mesh-технологій у закладах вищої освіти обумовлене сукупністю специфічних вимог до мережевої інфраструктури, що формуються під впливом значної кількості одночасно підключених користувачів, великої території покриття, а також необхідності забезпечення гарантованого, безперервного та високошвидкісного доступу до освітніх, наукових і адміністративних ресурсів (рис.1.3).

Сучасні університетські кампуси, як правило, мають розподілену структуру та включають навчальні корпуси, науково-дослідні лабораторії, бібліотеки, адміністративні будівлі, гуртожитки та інші об'єкти інфраструктури, що потребує впровадження гнучких, масштабованих і надійних мережевих рішень [12].

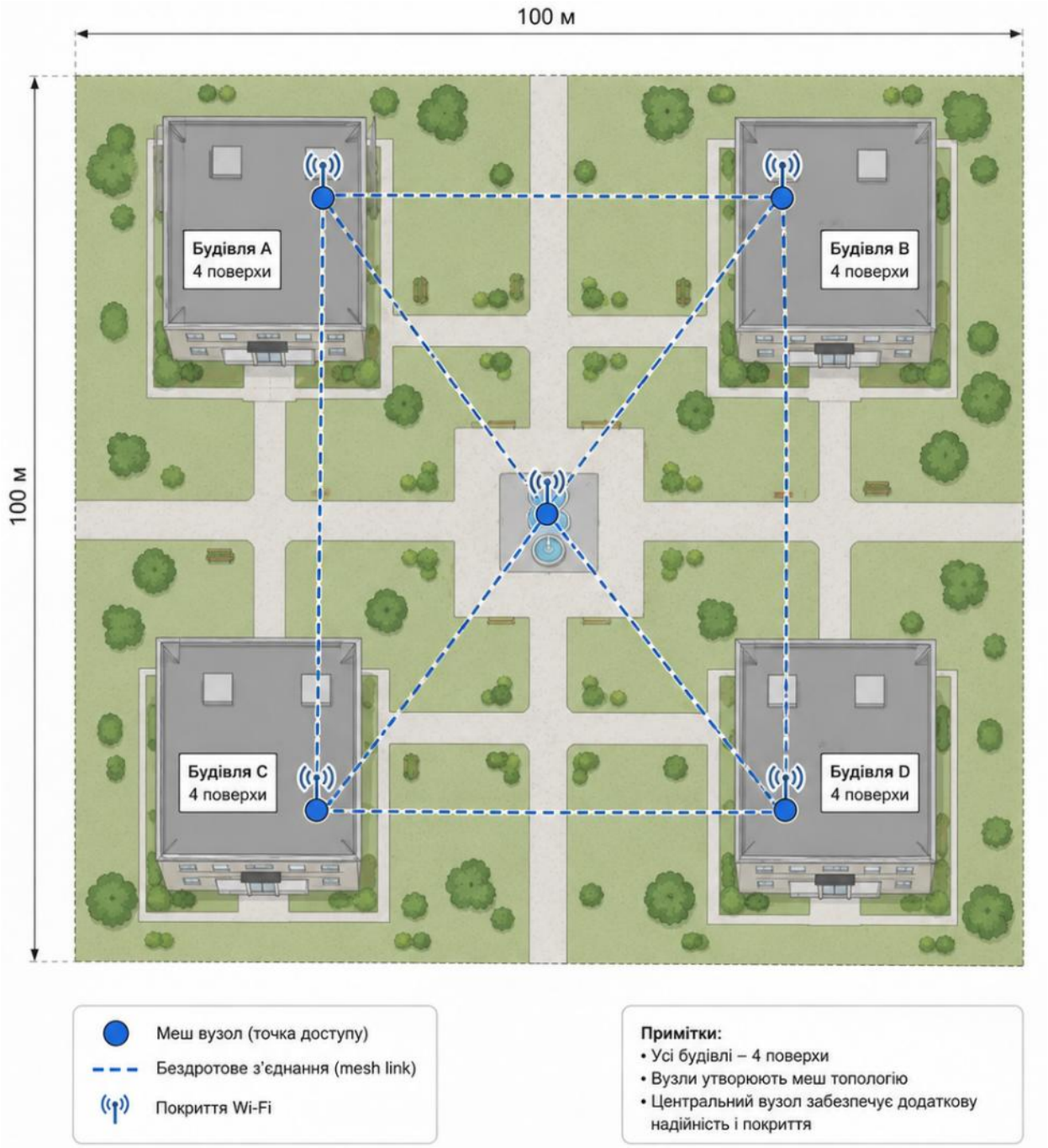


Рисунок 1.3 – Модель mesh-мережі ЗВО

Однією з ключових особливостей застосування mesh-мереж у закладах вищої освіти є можливість забезпечення суцільного бездротового покриття всієї території кампусу. На відміну від традиційних інфраструктурних підходів, де кожна точка доступу жорстко прив'язана до дротової мережі, mesh-архітектура дозволяє розширювати зону покриття шляхом поступового додавання нових вузлів, які автоматично інтегруються в існуючу мережу. Це суттєво спрощує

процес розгортання та модернізації інфраструктури, особливо в умовах обмежень, пов’язаних із прокладанням кабельних ліній, зокрема у будівлях зі складною архітектурою або в тимчасових навчальних приміщеннях.

Не менш важливою характеристикою є підвищена відмовостійкість мережі. У mesh-архітектурі відсутня централізована точка відмови, оскільки кожен вузол здатний виконувати функції маршрутизації та ретрансляції трафіку. У разі виходу з ладу окремого вузла, каналу зв’язку або сегмента мережі, система автоматично здійснює перебудову маршрутів передавання даних, використовуючи альтернативні шляхи.

Це забезпечує високу надійність функціонування мережі та безперервність доступу до освітніх сервісів, що є критично важливим для підтримки навчального процесу.

Важливою перевагою mesh-мереж є їх масштабованість. Архітектура таких мереж передбачає можливість поступового нарощування інфраструктури без необхідності суттєвої реконфігурації або перебудови вже існуючих сегментів. Додавання нових вузлів здійснюється з мінімальними витратами часу та ресурсів, що особливо актуально для закладів вищої освіти, де спостерігається постійне зростання кількості користувачів, підключених пристроїв та обсягів даних, які передаються.

Суттєвим напрямом є підтримка мобільності користувачів. Освітній процес передбачає активне переміщення студентів, викладачів та адміністративного персоналу між аудиторіями, корпусами та іншими об’єктами кампусу. Mesh-мережі забезпечують безшовне підключення до мережі завдяки автоматичному перемиканню між вузлами доступу без розриву сеансу зв’язку, що підвищує зручність користування мережевими сервісами та ефективність навчальної діяльності.

Важливим є питання ефективного розподілу мережевого навантаження. У сучасних університетах значна частка трафіку формується за рахунок використання систем дистанційного навчання, платформ відеоконференцій, хмарних сервісів, а також мультимедійного контенту. Mesh-мережі дозволяють

реалізувати динамічний розподіл трафіку між вузлами з урахуванням їх поточного завантаження та якості каналів зв’язку. Це сприяє зниженню перевантаження окремих сегментів мережі, підвищенню загальної продуктивності та покращенню якості обслуговування користувачів [13].

Також, важливою є можливість інтеграції механізмів забезпечення інформаційної безпеки, включаючи аутентифікацію користувачів, шифрування трафіку та сегментацію мережі. Це дозволяє забезпечити належний рівень захисту даних у відкритому бездротовому середовищі, що є особливо актуальним для освітніх установ.

Виходячи з цього, застосування mesh-технологій у закладах вищої освіти дозволяє створити високонадійну, гнучку, масштабовану та ефективну мережеву інфраструктуру, здатну задовольнити сучасні вимоги до якості та доступності освітніх і наукових сервісів.

Разом з тим використання mesh-мереж у вузах має певні особливості, які

- необхідно враховувати при проєктуванні:
- можливе зростання затримок при передачі даних через декілька вузлів;
- необхідність оптимального розміщення вузлів для уникнення
- перевантаження каналів;
- вплив радіоперешкод у щільно забудованих приміщеннях;
- потреба у забезпеченні належного рівня інформаційної безпеки.

Враховуючи особливості функціонування mesh-мереж, можна стверджувати, що їх використання у закладах вищої освіти сприяє створенню гнучкої, надійної та масштабованої мережевої інфраструктури.

Така інфраструктура забезпечує стабільний доступ до інформаційних ресурсів для всіх учасників освітнього процесу та підтримує безперервну роботу сучасних цифрових сервісів навіть за умов підвищеного мережевого навантаження або часткових відмов окремих вузлів мережі [14].

1.5 Постановка завдань проєктування мережі ЗВО

У зв’язку з підвищеними вимогами до якості та надійності мережевої інфраструктури закладів вищої освіти виникає необхідність розробки сучасної мережі передачі даних, здатної забезпечити стабільний доступ до інформаційних ресурсів для великої кількості користувачів.

Виходячи з мети роботи, об’єкта та предмета розробки сформулюємо ряд завдань, які необхідно вирішити для досягнення поставленої мети:

– здійснити аналіз принципів побудови та функціонування бездротових мереж, зокрема мереж із топологією mesh;

– розглянути сучасні стандарти та технології, що застосовуються в mesh-мережах (IEEE 802.11s, Wi-Fi 6/6E тощо);

– проаналізувати переваги та обмеження використання mesh-архітектури в інфраструктурі закладів вищої освіти;

– розробити структурну та функціональну архітектуру мережі ЗВО із застосуванням mesh-технологій;

– обґрунтувати вибір мережевого обладнання та програмного забезпечення для реалізації запропонованої мережі;

– виконати адресацію та планування мережевих ресурсів (IP-адресація, сегментація, VLAN тощо);

– реалізувати модель мережі у середовищі моделювання Cisco GNS3;

– провести дослідження функціонування розробленої мережі за різних режимів навантаження;

– здійснити аналіз відмовостійкості та надійності мережі, зокрема в умовах виходу з ладу окремих вузлів;

– оцінити масштабованість та можливості подальшого розширення мережевої інфраструктури.

Результатом виконання роботи є модель сучасної мережевої інфраструктури вузу, яка відповідає вимогам надійності, ефективності та масштабованості.

2 ТЕХНОЛОГІЇ, СТАНДАРТИ, ПРОТОКОЛИ ТА ВИБІР ОБЛАДНАННЯ

2.1 Мережеві технології вибір та застосування

Одним із ключових елементів сучасної бездротової мережевої інфраструктури є точки доступу (Access Point, AP), які забезпечують підключення користувацьких пристроїв до локальної мережі та мережі Internet через бездротовий канал зв’язку [15]. У закладах вищої освіти точки доступу відіграють важливу роль, оскільки повинні забезпечувати стабільне покриття значної території та підтримувати одночасну роботу великої кількості користувачів.

Традиційна архітектура бездротових мереж передбачає використання окремих точок доступу, кожна з яких обслуговує визначену зону покриття та підключається до мережевої інфраструктури через дротовий канал зв’язку. Такий підхід є ефективним для невеликих приміщень, однак у багатоповерхових будівлях та мережах із великою площею покриття виникають труднощі, пов’язані зі складністю масштабування, організацією роумінгу та забезпеченням рівномірного розподілу навантаження [16].

Для вирішення цих проблем використовуються Mesh-технології, які дозволяють створити єдину бездротову мережу з декількох взаємопов’язаних точок доступу. У такій архітектурі точки доступу взаємодіють між собою та можуть передавати дані через сусідні вузли, утворюючи багаторівневу структуру передачі трафіку.

Основним принципом роботи Mesh-мережі є створення множини альтернативних маршрутів передачі даних між вузлами. Якщо один із вузлів виходить з ладу або канал зв’язку стає недоступним, мережа автоматично перебудовує маршрут і продовжує функціонувати без суттєвого впливу на користувачів. Завдяки цьому забезпечується високий рівень відмовостійкості та надійності мережевої інфраструктури. Структурно Mesh-мережа може включати декілька типів вузлів:

– кореневий вузол (Root Node) – має пряме підключення до дротової мережі та забезпечує вихід до мережі Internet;

– проміжний вузол (Mesh Node) – бере участь у маршрутизації та передачі трафіку між іншими вузлами мережі;

– клієнтський вузол (Client Node) – кінцевий пристрій користувача, який підключається до мережі через найближчу точку доступу.

У межах даного проєкту кожен навчальний корпус має чотири поверхи. Для забезпечення якісного покриття на кожному поверсі передбачається використання двох бездротових точок доступу. Таким чином, у кожному корпусі функціонуватиме вісім точок доступу, а загальна кількість вузлів Mesh-мережі становитиме шістнадцять точок доступу для двох корпусів. Таке рішення дозволяє забезпечити:

– повне покриття всіх навчальних приміщень;

– зменшення кількості зон зі слабким сигналом;

– рівномірний розподіл навантаження між точками доступу;

– стабільне підключення великої кількості користувачів;

– безперервний роумінг між поверхами та корпусами.

Особливо важливим для закладу вищої освіти є механізм безшовного роумінгу. Під час переміщення користувача між аудиторіями або поверхами його пристрій автоматично переключається на точку доступу з кращим рівнем сигналу без втрати мережевого з’єднання. Це дозволяє підтримувати безперервну роботу освітніх платформ, сервісів відеоконференцій та інших мережевих застосунків.

Ще однією перевагою Mesh-технологій є простота масштабування мережі. У разі розширення навчального закладу або збільшення кількості приміщень до існуючої мережі можуть бути додані нові точки доступу без необхідності повного перепроєктування інфраструктури. Новий вузол автоматично інтегрується в мережу та починає взаємодіяти з іншими елементами системи.

Для моделювання роботи Mesh-мережі у даній роботі використовується середовище GNS3. У процесі моделювання реалізується логічна структура

мережі, яка відображає взаємодію між маршрутизаторами, комутаторами та бездротовими точками доступу. Це дозволяє оцінити ефективність запропонованої архітектури та перевірити її працездатність у різних сценаріях навантаження [17].

Таким чином, застосування Mesh-технологій є доцільним рішенням для побудови сучасної мережевої інфраструктури закладу вищої освіти, оскільки забезпечує високу масштабованість, відмовостійкість, ефективне покриття території та стабільний доступ користувачів до мережевих ресурсів.

2.2 Вибір обладнання та його функціональні характеристики

Для реалізації mesh-мережі університетського кампусу загальною площею близько 10 тисяч квадратних метрів необхідно сформувати комплексну багаторівневу бездротову інфраструктуру, здатну забезпечити безперервне та надійне покриття на всій території навчального закладу [18]. Така мережа повинна охоплювати не лише внутрішні приміщення навчальних корпусів, лабораторій, бібліотек, адміністративних приміщень та аудиторій, але й відкриті простори між будівлями, включаючи внутрішні двори, пішохідні зони, місця відпочинку студентів та інші ділянки кампусу (рис. 2.1).

Побудова подібної мережевої інфраструктури потребує ретельного планування розміщення мережевого обладнання, визначення зон покриття та врахування особливостей архітектури будівель. Значна кількість стін, перекриттів, металевих конструкцій та інших фізичних перешкод може негативно впливати на якість поширення радіосигналу, тому при проєктуванні необхідно забезпечити оптимальне розташування точок доступу та mesh-вузлів. Особлива увага повинна приділятися місцям із високою концентрацією користувачів, таким як лекційні аудиторії, конференц-зали, читальні зали

бібліотек та комп’ютерні класи, де мережа повинна підтримувати одночасне підключення великої кількості пристроїв без втрати продуктивності [19].

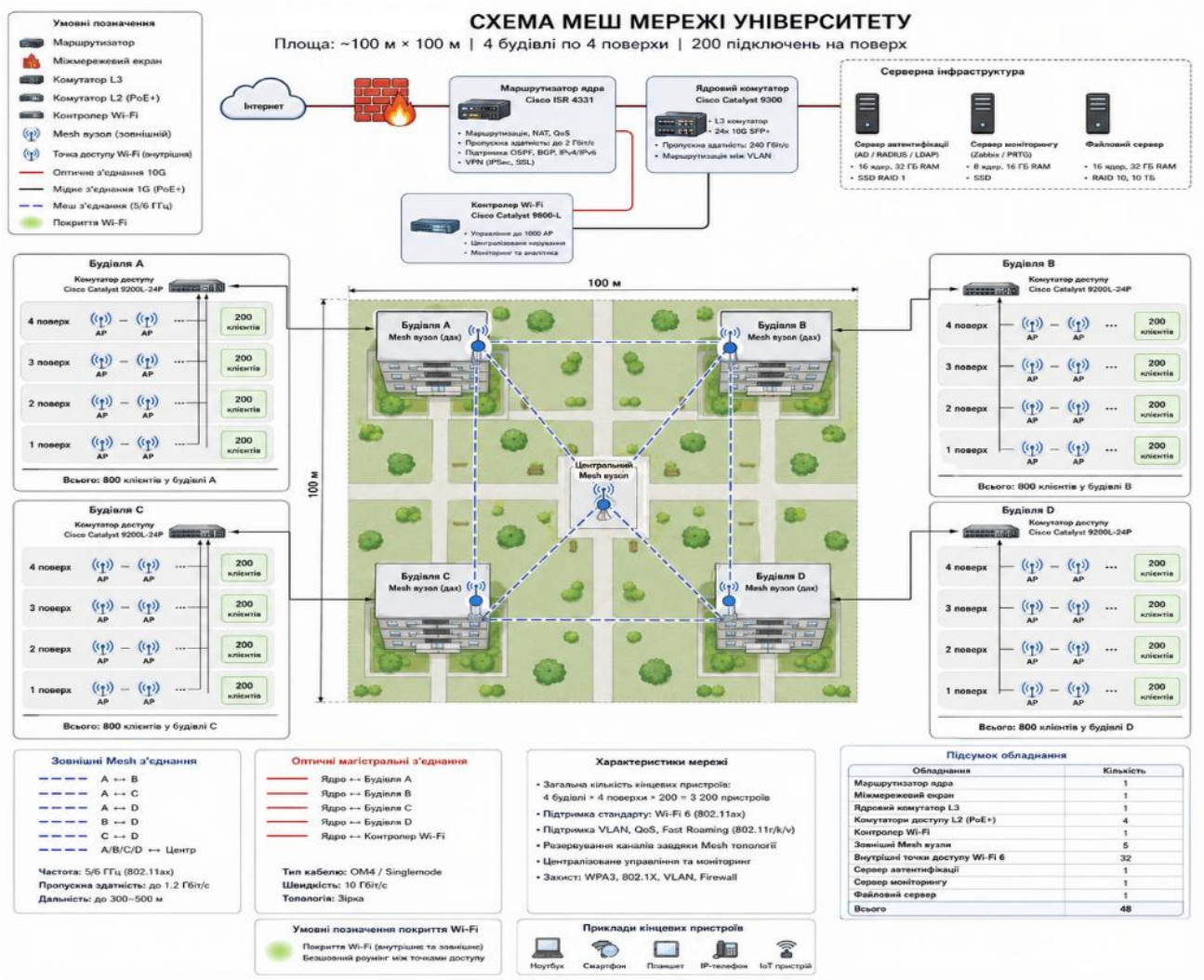


Рисунок 2.1 – Функціональна схема mesh-мережі ЗВО

Для забезпечення стабільного зв’язку між окремими корпусами доцільно використовувати зовнішні mesh-вузли, які формуватимуть магістральну бездротову мережу та забезпечуватимуть передачу даних між різними сегментами інфраструктури. Внутрішнє покриття будівель реалізується за допомогою точок доступу, інтегрованих у єдину систему керування [20]. Такий підхід дозволяє створити масштабовану, відмовостійку та гнучку мережу, здатну адаптуватися до змін кількості користувачів, розширення території кампусу та впровадження нових інформаційних сервісів. У результаті формується сучасне

мережеве середовище, яке забезпечує стабільний доступ до освітніх ресурсів, електронних платформ навчання та інформаційних систем університету незалежно від місця перебування користувача на території кампусу [21].

Основу мережі складатимуть вузли Mesh Wi-Fi, комутатори доступу, маршрутизатор ядра мережі та серверна інфраструктура (табл. 2.1).

Таблиця 2.1 – Орієнтовна підсумкова специфікація

Обладнання	Кількість
Маршрутизатор ядра	1
Комутатори L2/L3	4
Внутрішні точки доступу Wi-Fi 6	32
Зовнішні Mesh-вузли	5
Контролер Wi-Fi	1
Сервер AD/RADIUS	1
Сервер моніторингу	1
Файловий сервер	1
Firewall	1
Оптичні лінії між корпусами	4

2.2.1 Центральний маршрутизатор Cisco ISR 4331

Центральний маршрутизатор є одним із ключових елементів мережевої інфраструктури університетської меш-мережі, оскільки саме він забезпечує взаємодію між усіма сегментами мережі, виконує маршрутизацію трафіку між VLAN, організовує доступ до мережі Інтернет, а також реалізує механізми інформаційної безпеки та віддаленого доступу [22].

В умовах сучасного розвитку інформаційно-комунікаційних технологій, збільшення кількості мережевих сервісів, хмарних платформ, систем дистанційного навчання та мобільних користувачів вимоги до продуктивності та надійності маршрутизатора постійно зростають. Саме тому для побудови мережі університетського кампусу доцільним є використання високопродуктивних маршрутизаторів корпоративного класу, таких як Cisco ISR 4331 або MikroTik CCR2004. Дані пристрої зображені на рисунках 2.2 та 2.3.

Рисунок 2.2 – Пристрій Cisco ISR 4331

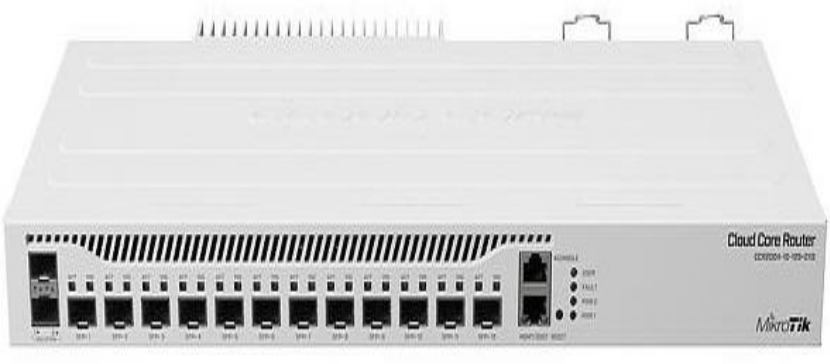


Рисунок 2.3 – Пристрій MikroTik CCR2004

Призначення:

- маршрутизація трафіку між VLAN;
- підключення до мережі Інтернет;
- реалізація VPN-з'єднань;
- підтримка QoS та політик безпеки.

Основні характеристики:

- пропускна здатність до 1–2 Гбіт/с;
- підтримка IPv4/IPv6;
- підтримка OSPF, BGP, RIP;
- IPSec VPN;
- NAT, ACL, Firewall.

Актуальність застосування даного обладнання обумовлена необхідністю забезпечення стабільної роботи великої кількості користувачів та пристроїв, які одночасно використовують мережеві ресурси. З урахуванням того, що в

проєктованій мережі функціонує чотири навчальні корпуси по чотири поверхи кожний із можливістю підключення до 200 користувачів на поверх, загальна кількість потенційно активних клієнтів може перевищувати 3200 пристроїв. У таких умовах центральний маршрутизатор повинен забезпечувати ефективну обробку значних обсягів мережевого трафіку, підтримувати балансування навантаження та гарантувати високу швидкодію мережевих сервісів.

Функціонально маршрутизатор виконує роль центрального вузла мережі, через який проходить весь міжмережевий трафік [23]. Він здійснює маршрутизацію пакетів між віртуальними локальними мережами (VLAN), що дозволяє логічно розділити користувачів за категоріями, наприклад студентів, викладачів, адміністративний персонал, серверне обладнання та гостьові пристрої. Таке сегментування підвищує рівень інформаційної безпеки, зменшує широкомовний трафік та спрощує адміністрування мережі.

Додатково маршрутизатор забезпечує підключення мережі університету до провайдера Інтернет-послуг та реалізує механізми трансляції мережевих адрес NAT, що дозволяє використовувати приватну адресацію всередині мережі та ефективно керувати зовнішніми підключеннями. Важливою функцією є підтримка сучасних мережевих протоколів IPv4 та IPv6, що забезпечує сумісність мережі з сучасними телекомунікаційними стандартами та створює основу для подальшого розвитку інфраструктури.

Для забезпечення надійного функціонування розподіленої мережі підтримуються протоколи динамічної маршрутизації OSPF, BGP та RIP. Використання OSPF дозволяє автоматично визначати оптимальні маршрути всередині мережі університету, а BGP може застосовуватися при взаємодії з декількома зовнішніми провайдерами або іншими автономними системами. Завдяки цьому мережа отримує можливість швидкого відновлення після аварій та ефективного використання резервних каналів зв’язку. Особливе значення має підтримка технології IPSec VPN, яка дозволяє створювати захищені тунелі між віддаленими підрозділами університету, філіями, дата-центрами або користувачами, що працюють дистанційно [24]. Використання VPN забезпечує

конфіденційність, цілісність та автентичність переданих даних навіть при передачі через незахищені мережі загального користування.

Для забезпечення належного рівня кібербезпеки маршрутизатор підтримує механізми списків контролю доступу (ACL), міжмережевого екранування (Firewall), фільтрації пакетів та контролю мережевих потоків. Це дозволяє обмежувати несанкціонований доступ до ресурсів мережі, запобігати поширенню шкідливого програмного забезпечення та мінімізувати ризики мережевих атак. Важливим компонентом функціональності є підтримка механізмів QoS (Quality of Service), які забезпечують пріоритизацію критично важливого трафіку [25]. Завдяки цьому мережеві сервіси дистанційного навчання, відеоконференції, IP-телефонія та інформаційні системи університету отримують гарантовану пропускну здатність навіть за умов значного навантаження мережі.

Маршрутизатори Cisco ISR 4331 та MikroTik CCR2004 характеризуються високою продуктивністю та надійністю. Вони підтримують пропускну здатність на рівні 1–2 Гбіт/с і більше залежно від конфігурації, мають сучасні багатоядерні процесори, апаратне прискорення криптографічних операцій та можливість подальшого масштабування мережі без суттєвої модернізації обладнання.

Отже, використання одного центрального маршрутизатора корпоративного класу є обґрунтованим рішенням для побудови університетської меш-мережі [26]. Його функціональні можливості забезпечують ефективну маршрутизацію, сегментацію мережі, підтримку VPN-технологій, захист інформаційних ресурсів та стабільний доступ до мережевих сервісів. Завдяки високій продуктивності, підтримці сучасних протоколів і механізмів безпеки центральний маршрутизатор формує основу надійної, масштабованої та захищеної мережевої інфраструктури університету, здатної забезпечити потреби кількох тисяч одночасно підключених користувачів.

2.2.2 Комутатори доступу – Cisco Catalyst 9200L або Aruba 6100

Комутатори доступу є основою локальної мережевої інфраструктури університету та виконують одну з найважливіших функцій у побудові сучасної багаторівневої мережі. Саме через комутатори здійснюється підключення кінцевих пристроїв користувачів, бездротових точок доступу, серверного обладнання та інших мережевих компонентів до єдиного інформаційного середовища університету. В умовах впровадження меш-мережі на території кампусу площею близько 100×100 метрів із чотирма чотириповерховими навчальними корпусами використання керованих комутаторів корпоративного класу є необхідною умовою забезпечення стабільної, масштабованої та безпечної роботи всієї мережі. У кожному корпусі необхідно встановити один або декілька комутаторів.

Призначення:

- підключення точок доступу;
- підключення серверів і робочих станцій;
- підтримка VLAN.

Характеристики:

- 24 або 48 портів Gigabit Ethernet;
- PoE+ живлення для точок доступу;
- підтримка IEEE 802.1Q;
- підтримка STP/RSTP;
- DHCP Snooping;
- Port Security.

Кількість**:** по 1 комутатору на будівлю; разом 4 шт.

Актуальність застосування комутаторів Cisco Catalyst 9200L або Aruba 6100 обумовлена постійним зростанням кількості мережевих пристроїв, розвитком бездротових технологій Wi-Fi 6, використанням хмарних сервісів, систем дистанційного навчання, відеоконференцій та електронного документообігу [27]. Враховуючи, що кожен поверх проєктованої будівлі розрахований на підключення до 200 користувачів, а загальна кількість

потенційних клієнтів у чотирьох корпусах становить близько 3200 пристроїв, комутаційне обладнання повинно забезпечувати високу продуктивність, надійність та підтримку сучасних технологій управління мережею. Дані пристрої зображені на рисунках 2.4 та 2.5.

Рисунок 2.4 – Комутатор доступу Cisco Catalyst 9200L

У структурі проєктованої мережі комутатори доступу розміщуються в кожному навчальному корпусі та виконують функцію концентрації локального мережевого трафіку. До них підключаються внутрішні точки доступу Wi-Fi, персональні комп’ютери, ноутбуки, IP-телефони, принтери, мультимедійне обладнання аудиторій, системи відеоспостереження та інші мережеві пристрої. Через висхідні магістральні канали комутатори з’єднуються з ядром мережі та забезпечують передачу даних між усіма сегментами інформаційної системи університету.

Рисунок 2.5 – Комутатор доступу Aruba 6100

Однією з ключових функцій комутаторів є підтримка технології VLAN відповідно до стандарту IEEE 802.1Q. Завдяки цьому стає можливим логічний поділ мережі на окремі сегменти незалежно від фізичного розташування користувачів [28]. Наприклад, можна створити окремі VLAN для студентів,

викладачів, адміністрації, серверної інфраструктури, систем відеоспостереження та гостьового доступу. Такий підхід підвищує рівень інформаційної безпеки, зменшує широкомовний трафік та спрощує централізоване адміністрування мережі.

Для забезпечення підключення великої кількості обладнання комутатори Cisco Catalyst 9200L та Aruba 6100 оснащуються 24 або 48 портами Gigabit Ethernet, що дозволяє організувати швидкісне дротове підключення користувачів і мережевих пристроїв. Гігабітна швидкість передачі даних є достатньою для роботи сучасних інформаційних систем, передачі мультимедійного контенту високої якості та підтримки хмарних сервісів.

Особливо важливою для реалізації бездротової інфраструктури є підтримка технології PoE+ (Power over Ethernet), яка дозволяє передавати живлення та дані одним мережевим кабелем. Завдяки цьому точки доступу Wi-Fi можуть встановлюватися в оптимальних місцях без необхідності прокладання окремих ліній електроживлення, що значно спрощує монтажні роботи, знижує вартість розгортання мережі та підвищує її надійність.

Для забезпечення стабільності роботи мережі комутатори підтримують протоколи STP (Spanning Tree Protocol) та RSTP (Rapid Spanning Tree Protocol), які запобігають виникненню петель у мережевій інфраструктурі. Наявність резервних з’єднань між мережевими вузлами є необхідною умовою забезпечення відмовостійкості, проте без використання даних протоколів це може призвести до широкомовних штормів та порушення функціонування мережі. Використання STP і RSTP дозволяє автоматично контролювати резервні канали та забезпечувати швидке відновлення зв’язку у випадку аварійних ситуацій.

Значна увага приділяється також питанням мережевої безпеки. Для захисту від атак на канальному рівні комутатори підтримують технологію DHCP Snooping, яка здійснює контроль процесу видачі IP-адрес та блокує роботу несанкціонованих DHCP-серверів. Це дозволяє запобігти перехопленню мережевого трафіку та несанкціонованому перенаправленню користувачів на фальшиві мережеві ресурси.

Додатковий рівень захисту забезпечується механізмом Port Security, який дозволяє контролювати кількість та тип пристроїв, що можуть підключатися до конкретного порту комутатора. У випадку спроби підключення невідомого або неавторизованого пристрою порт може бути автоматично заблокований, що суттєво знижує ризик несанкціонованого доступу до корпоративної мережі університету.

Для реалізації мережі передбачається встановлення щонайменше одного комутатора доступу в кожному корпусі. Загальна кількість комутаторів становить чотири одиниці. Однак з огляду на значну кількість користувачів та мережевого обладнання, доцільним є встановлення додаткових комутаторів на окремих поверхах або використання моделей із 48 портами та можливістю стекування. Такий підхід забезпечить подальше масштабування мережі без необхідності кардинальної модернізації існуючої інфраструктури.

Отже, комутатори доступу Cisco Catalyst 9200L або Aruba 6100 є важливими компонентами мережевої інфраструктури університету, які забезпечують підключення користувачів та обладнання до інформаційної системи, підтримують сегментацію мережі за допомогою VLAN, реалізують сучасні механізми безпеки та гарантують високу швидкість передачі даних. Їх використання дозволяє створити надійну, масштабовану та захищену мережу, здатну ефективно обслуговувати кілька тисяч одночасно підключених пристроїв і забезпечувати безперебійну роботу всіх інформаційних сервісів університету.

2.2.3 Внутрішні точки доступу Wi-Fi

Функціонально внутрішні точки доступу Wi-Fi є базовими елементами бездротової інфраструктури університетської mesh-мережі. Для чотириповерхової будівлі площею орієнтовно 1500–2500 м² кожного корпусу передбачається повне радіопокриття кожного поверху шляхом розміщення щонайменше двох точок доступу на поверх. Як технічну основу доцільно використовувати сучасні моделі, такі як Cisco Catalyst 9120AXI або Ubiquiti UniFi U6 Enterprise, які підтримують стандарт IEEE 802.11ax (Wi-Fi 6) та забезпечують пропускну здатність до 5–6 Гбіт/с.

Для чотириповерхової будівлі площею приблизно 1500–2500 м² необхідно забезпечити покриття кожного поверху. Тому для цього використовуємо Cisco Catalyst 9120AXI або Ubiquiti UniFi U6 Enterprise. Дані пристрої зображені на риснуках 2.6 та 2.7.

Рисунок 2.6 –Точка доступу Cisco Catalyst 9120AXI

Рисунок 2.7 –Точка доступу Ubiquiti UniFi U6 Enterprise

Характеристики:

- стандарт IEEE 802.11ax (Wi-Fi 6);
- до 5–6 Гбіт/с;
- MU-MIMO;

- OFDMA;
- підтримка до 300–500 клієнтів;
- живлення PoE+.

Рекомендоване розміщення: 2 точки доступу на поверх. Для одного корпусу: 4 поверхи × 2 AP = 8 AP. Для чотирьох корпусів: 8 × 4 = 32 AP.

Завдяки застосуванню технологій MU-MIMO та OFDMA такі точки доступу ефективно обробляють велику кількість одночасних підключень (до 300–500 клієнтів на один пристрій), що є особливо важливим для університетського середовища, де одночасно працюють студенти, викладачі та адміністративний персонал. Використання живлення PoE+ спрощує інсталяцію обладнання, зменшує витрати на електромонтажні роботи та підвищує гнучкість розміщення точок доступу.

З точки зору масштабування мережі, для одного навчального корпусу необхідно 4 поверхи × 2 точки доступу = 8 AP, а для чотирьох корпусів загальна кількість становитиме 32 точки доступу. Така структура дозволяє забезпечити рівномірне покриття всієї території університету, а також створити основу для інтеграції з mesh-архітектурою, де вузли можуть автоматично оптимізувати маршрутизацію трафіку та забезпечувати резервування каналів зв’язку.

Отже, впровадження внутрішніх точок доступу Wi-Fi у поєднанні з mesh-архітектурою є доцільним та ефективним рішенням для університетської мережі. Воно забезпечує високу пропускну здатність, масштабованість, стійкість до відмов та стабільний доступ до мережевих сервісів у всіх навчальних корпусах, що підвищує якість інформаційного середовища закладу вищої освіти.

2.2.4 Зовнішні Mesh-вузли

Функціонально зовнішні Mesh-вузли формують базовий рівень бездротової взаємодії між корпусами університету, забезпечуючи автоматичну побудову маршрутів передачі даних, резервування каналів зв’язку та динамічну адаптацію до змін у мережевій топології. Вони виконують функцію транзитних і маршрутизуючих елементів, через які передається трафік між окремими

будівлями університетського кампусу, а також забезпечують повне покриття відкритих територій.

Як технічну основу для побудови mesh-мережі доцільно використовувати сучасні високопродуктивні рішення, зокрема мережеві пристрої Cisco Catalyst 1562I або Ubiquiti UniFi U6 Mesh, які підтримують стандарт Wi-Fi 6 та оснащені вбудованими механізмами організації mesh-топології (рис. 2.8, 2.9). Застосування такого обладнання дозволяє забезпечити високу швидкість передавання даних, ефективне використання радіочастотного спектра та стабільне підключення великої кількості користувачів одночасно.

Рисунок 2.8 – Пристрій Cisco Catalyst 1562I

Крім того, зазначені пристрої характеризуються високою надійністю, можливістю централізованого керування та підтримкою сучасних засобів мережевої безпеки, що є важливим для функціонування університетської мережевої інфраструктури.

Рисунок 2.9 – Пристрій Ubiquiti UniFi U6 Mesh

Функції:

– автоматична побудова маршрутів;
– резервування каналів зв'язку;
– передача трафіку між корпусами;
– покриття території кампусу.

Характеристики:

– Wi-Fi 6;
– дальність до 300–500 м;
– підтримка Mesh;
– захист IP67;
– робота при температурі від -40 до +65 °C.

Кількість. По одному вузлу на даху кожної будівлі: 4 вузли. Додатковий центральний вузол: 1 вузол. Разом: 5 зовнішніх Mesh-вузлів.

Завдяки технічним характеристикам, зокрема дальності дії до 300–500 метрів, підтримці високошвидкісного бездротового зв’язку, захисту корпусу IP67 та стійкості до екстремальних температурних умов (від -40 до +65 °C), такі пристрої є оптимальними для зовнішнього розгортання в умовах кампусу. Їх використання дозволяє забезпечити стабільну передачу даних між корпусами навіть за несприятливих погодних умов, що підвищує загальну надійність мережевої інфраструктури.

У межах запропонованої архітектури передбачається розгортання п’яти зовнішніх Mesh-вузлів: по одному на даху кожної з чотирьох будівель та додаткового центрального вузла, який виконує роль ядра бездротової mesh-топології.

Така конфігурація забезпечує багатошляхову маршрутизацію, резервування з'єднань та рівномірний розподіл навантаження між каналами зв'язку, що є критично важливим для підтримки великої кількості одночасних користувачів.

Отже, впровадження зовнішніх Mesh-вузлів у мережеву інфраструктуру університету є технічно обґрунтованим і стратегічно доцільним рішенням. Воно забезпечує високу відмовостійкість, гнучкість масштабування та стабільність міжкорпусного зв'язку, що в сукупності формує сучасну, ефективну та надійну бездротову мережу кампусного типу.

2.2.5 Контролер бездротової мережі

У межах проєктування університетської mesh-мережі доцільним є застосування контролера бездротової мережі рівня enterprise, зокрема Cisco Systems Cisco Catalyst 9800-L або альтернативного рішення Ubiquiti Inc. UniFi Cloud Key Gen2 Plus, які забезпечують централізоване адміністрування точок доступу та інтеграцію в єдину керовану бездротову інфраструктуру. Ці пристрої зображені на рисунках 2.10 та 2.11.

Рисунок 2.10 – Контролер Cisco System Cisco Catalyst 9800-l

Рисунок 2.11 – Контролер Ubiquiti Inc. UniFi Cloud Key Gen2 Plus

Актуальність впровадження такого контролера зумовлена зростанням кількості мобільних пристроїв у навчальному середовищі, підвищенням вимог до безперервності доступу до мережевих сервісів, а також необхідністю ефективного управління розподіленою mesh-топологією між корпусами університету.

У великих кампусних мережах ручне налаштування точок доступу є неефективним і підвищує ризики конфігураційних помилок, тоді як централізований контролер дозволяє уніфікувати політики безпеки, балансування навантаження та параметри радіодоступу.

Призначення:

– централізоване управління AP;
– моніторинг;
– автоматичне оновлення;
– керування роумінгом користувачів.

Характеристики:

– підтримка сотень точок доступу;
– веб-інтерфейс;
– аналітика мережі.

Функціонально контролер бездротової мережі виконує низку критично важливих завдань. По-перше, забезпечується централізоване управління

точками доступу (AP), що дозволяє адміністратору конфігурувати всю мережу з єдиної консолі. По-друге, реалізується безперервний моніторинг стану радіомережі, включаючи завантаження каналів, рівень сигналу та активність користувачів.

По-третє, підтримується автоматичне оновлення прошивок і конфігурацій, що підвищує рівень безпеки та зменшує експлуатаційні витрати. Окремо слід виділити механізми керування роумінгом користувачів, які забезпечують безперервне переключення між точками доступу без розриву з'єднання, що є особливо важливим у mesh-мережах кампусу. Додатково сучасні контролери надають аналітичні інструменти для оцінки продуктивності мережі, прогнозування навантаження та оптимізації радіоресурсів.

З точки зору технічних характеристик, такі рішення підтримують керування сотнями точок доступу, що робить їх придатними для масштабних університетських інфраструктур, мають зручний веб-інтерфейс адміністрування, а також інтегровані засоби аналітики та логування подій. Це дозволяє не лише підтримувати стабільну роботу мережі, але й здійснювати її постійне вдосконалення на основі зібраних даних.

Отже, впровадження централізованого контролера бездротової мережі в архітектуру університетської mesh-мережі є ключовим елементом побудови сучасної, масштабованої та відмовостійкої інфраструктури. Такий підхід забезпечує підвищення керованості, безпеки та ефективності використання мережевих ресурсів, що сприяє підвищенню якості цифрового освітнього середовища та підтримці безперервного доступу до університетських сервісів.

2.2.6 Серверне обладнання

У проєктованій архітектурі університетської mesh-мережі серверне обладнання відіграє ключову роль у забезпеченні централізованого управління, безпеки, моніторингу та зберігання даних, формуючи базовий рівень інформаційної інфраструктури кампусу. Актуальність впровадження серверного кластера зумовлена необхідністю підтримки великої кількості одночасних користувачів, забезпечення безперервного доступу до освітніх ресурсів, а також

підвищенням вимог до інформаційної безпеки та відмовостійкості мережевих сервісів у сучасному університетському середовищі.

Сервер автентифікації є критично важливим елементом безпекової архітектури мережі та виконує функції централізованого контролю доступу користувачів до ресурсів університетської інфраструктури. Його робота базується на інтеграції служб каталогів і протоколів автентифікації, зокрема Microsoft Active Directory, а також використанні протоколів RADIUS і LDAP. Такий підхід дозволяє реалізувати єдину систему облікових записів, політик доступу та ролей користувачів (студенти, викладачі, адміністрація), забезпечуючи при цьому високий рівень безпеки та контроль підключень до Wi-Fi мережі. Рекомендовані апаратні характеристики (8–16 ядер CPU, 32–64 ГБ RAM та SSD у RAID-конфігурації) забезпечують стабільну обробку великої кількості запитів автентифікації в умовах пікового навантаження.

Сервер моніторингу виконує функції безперервного контролю стану мережевої інфраструктури та аналізу її продуктивності. У межах запропонованої архітектури використовується комплекс програмних рішень, зокрема Zabbix для збору та аналізу метрик, PRTG Network Monitor для візуалізації стану мережевих пристроїв, а також Grafana для побудови аналітичних дашбордів. Така інтеграція дозволяє здійснювати контроль навантаження каналів зв’язку, моніторинг стану mesh-вузлів, аналіз якості Wi-Fi сигналу та виявлення потенційних збоїв у режимі реального часу. Це є особливо актуальним для розподіленої університетської мережі, де стабільність з’єднання безпосередньо впливає на якість освітнього процесу.

Файловий сервер забезпечує централізоване зберігання навчальних матеріалів, наукових даних, методичних ресурсів та резервних копій критично важливої інформації. Його впровадження дозволяє реалізувати єдиний інформаційний простір університету з контрольованим доступом та можливістю швидкого відновлення даних у разі збоїв або втрати інформації. Це також сприяє підвищенню ефективності обміну навчальними матеріалами між підрозділами університету та зменшує залежність від локальних носіїв інформації.

Узагальнюючи, серверне обладнання в запропонованій архітектурі університетської mesh-мережі формує інтегровану платформу для управління і захисту даних, моніторингу мережевої інфраструктури та забезпечення безперервного доступу до освітніх сервісів. Такий підхід підвищує надійність, масштабованість і безпеку інформаційної системи університету, створюючи основу для подальшого розвитку цифрового освітнього середовища та впровадження сучасних IT-сервісів.

2.2.7 Система безпеки та структурована кабельна система

В університетській mesh-мережі система безпеки та структурована кабельна система (СКС) є ключовими складовими мережевої інфраструктури, які забезпечують логічний і фізичний захист інформаційних ресурсів, стабільність функціонування мережі та гарантовану пропускну здатність каналів зв’язку. Актуальність впровадження комплексного підходу до побудови системи безпеки та СКС обумовлена постійним зростанням кількості кіберзагроз, збільшенням обсягів передавання даних у цифровому освітньому середовищі та необхідністю забезпечення безперервного функціонування університетських сервісів у межах розподіленої багатокорпусної мережі.

Для захисту мережевої інфраструктури доцільно використовувати міжмережеві екрани корпоративного класу, зокрема Fortinet FortiGate 100F або Cisco Firepower 1010. Дані пристрої реалізують комплексний підхід до мережевої безпеки та підтримують функції глибокого аналізу мережевого трафіку (IDS/IPS), фільтрації пакетів, контролю доступу, захисту від DDoS-атак, виявлення шкідливої активності та організації захищених VPN-з’єднань для віддаленого доступу до ресурсів університету. Використання таких рішень дозволяє централізовано керувати політиками безпеки, здійснювати сегментацію мережі за допомогою VLAN та забезпечувати захист як дротового, так і бездротового сегментів mesh-інфраструктури.

Фізичний рівень мережі базується на сучасній СКС, яка забезпечує високу продуктивність, надійність та можливість подальшого масштабування телекомунікаційної інфраструктури. У межах окремих корпусів

використовується мідна кабельна система категорії Cat6A, що підтримує передачу даних зі швидкістю до 10 Гбіт/с та забезпечує стабільну роботу робочих станцій, серверів, комутаторів доступу та бездротових точок доступу.

Для організації магістральних каналів між корпусами університету використовується оптичне волокно, яке забезпечує високу пропускну здатність, низький рівень загасання сигналу та стійкість до електромагнітних завад. Під час побудови міжкорпусних з'єднань доцільно застосовувати стандарт 1000Base-LX, який працює на довжині хвилі 1310 нм та забезпечує передачу даних зі швидкістю 1 Гбіт/с на відстань до 5 км по одномодовому оптичному волокну. Використання стандарту 1000Base-LX дозволяє створити надійні канали зв'язку між будівлями кампусу без втрати якості передачі даних та забезпечити резервування важливих мережевих сегментів. Для подальшого збільшення пропускної здатності можливе використання сучасних стандартів 10GBase-LR та 10GBase-SR, що забезпечують передачу даних зі швидкістю 10 Гбіт/с.

Додатковими компонентами СКС є патч-панелі, оптичні кроси, організатори кабелю та серверні шафи формату 42U, які забезпечують впорядковане розміщення активного й пасивного мережевого обладнання. Такий підхід спрощує адміністрування мережі, проведення модернізації, технічного обслуговування та пошуку несправностей. Правильна організація кабельної частини сприяє зменшенню ризику фізичних пошкоджень кабельних ліній та підвищує загальну надійність функціонування мережевої інфраструктури.

Отже, поєднання сучасних засобів мережевої безпеки із якісно спроєктованою СКС створює надійний фундамент для функціонування університетської mesh-мережі. Запропонований підхід забезпечує високий рівень інформаційної безпеки, відмовостійкості та продуктивності мережі, створює умови для розвитку цифрової інфраструктури ЗВО, впровадження нових освітніх сервісів та розширення бездротового покриття кампусу.

3 ПРОЄКТУВАННЯ МЕРЕЖІ ЗВО ІЗ ЗАСТОСУВАННЯМ MESH ТЕХНОЛОГІЙ

3.1 Логічна структура мережі

Логічна структура проєктованої кампусної мережі закладу вищої освіти побудована за ієрархічним принципом, який відповідає рекомендаціям Cisco Enterprise Architecture. Дана модель передбачає розділення мережі на три основні рівні: рівень доступу, рівень розподілу та рівень ядра, що забезпечує ефективну організацію трафіку, масштабованість та відмовостійкість інфраструктури.

На рівні доступу маємо безпосереднє підключення кінцевих пристроїв користувачів до мережі з використанням комутаторів Cisco Catalyst 9200L, бездротових точок доступу Cisco Catalyst 9120AXI, а також зовнішніх mesh-вузлів Cisco Catalyst 1562I. На даному рівні реалізовано підключення:

- персональних комп’ютерів користувачів;
- серверного обладнання;
- бездротових клієнтських пристроїв (ноутбуків, смартфонів);
- IoT та мобільних пристроїв через Wi-Fi 6 інфраструктуру.

Сегментація трафіку виконується за допомогою VLAN, що дозволяє логічно розділити різні категорії користувачів та сервісів. Рівень розподілу виконує функції агрегації трафіку та міжвіртуальної маршрутизації. У межах проєктованої мережі ці функції реалізуються на комутаторах Cisco Catalyst 9200L, які підтримують можливості Layer 3. Основні функції рівня розподілу:

- маршрутизація між VLAN (Inter-VLAN Routing);
- застосування політик доступу;
- агрегація трафіку з кількох сегментів доступу;
- забезпечення резервування маршрутів у межах кампусу.

Ядро мережі реалізовано на базі маршрутизатора Cisco ISR 4331 та міжмережевого екрана Cisco Firepower 1010. Основні функції ядра: маршрутизація між

внутрішньою мережею та зовнішніми мережами; реалізація NAT/PAT для доступу до Internet; забезпечення політик безпеки на периметрі мережі; фільтрація та контроль трафіку між внутрішніми та зовнішніми сегментами.

Бездротова частина мережі побудована на основі централізованої архітектури з використанням контролера Cisco Catalyst 9800-L, який керує всіма точками доступу Cisco Catalyst 9120AXI. Крім того, для забезпечення зв'язності між корпусами використовується часткова mesh-топологія на базі зовнішніх вузлів Cisco Catalyst 1562I, що підвищує відмовостійкість мережі та забезпечує альтернативні маршрути передачі даних. Логічна структура мережі передбачає використання VLAN для розділення трафіку за функціональним призначенням:

- VLAN 10 – користувачі (навчальні та адміністративні ПК);
- VLAN 20 – бездротовий доступ (Wi-Fi та mesh-пристрої);
- VLAN 30 – серверна інфраструктура;
- VLAN 99 – службове та адміністративне керування.

Топологія мережі представляє собою багаторівневу гібридну мережу, яка поєднує класичну ієрархічну архітектуру з елементами mesh-структури для забезпечення підвищеної відмовостійкості та гнучкості (рис. 3.1). На верхньому рівні знаходиться підключення до Internet, яке проходить через міжмережевий екран для забезпечення базового захисту зовнішнього трафіку. Далі трафік передається на маршрутизатор R1, який виконує функції маршрутизації між зовнішньою та внутрішньою частинами мережі.

До маршрутизатора підключено комутатор ядра SWC, який забезпечує розподіл трафіку до серверного сегмента мережі, зокрема до Server, що виконує роль центрального ресурсу зберігання та надання сервісів. Також у верхній частині схеми присутній контролер бездротової мережі (WLC), який централізовано керує точками доступу та політиками Wi-Fi інфраструктури.

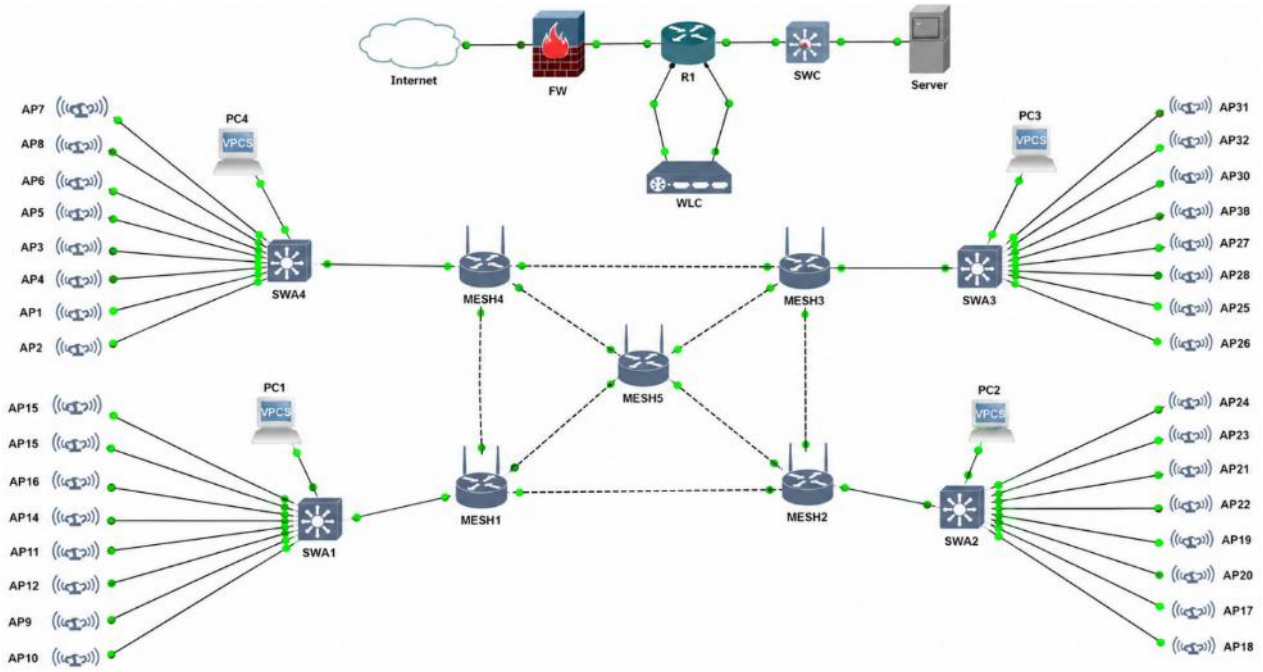


Рисунок 3.1 – Логічна структура мережі

Основну частину мережі формують mesh-вузли (MESH1–MESH5), які з’єднані між собою у вигляді частково повнозв’язної mesh-топології. Така структура забезпечує альтернативні маршрути передавання даних між вузлами, що підвищує надійність мережі та мінімізує вплив відмов окремих каналів зв’язку. Центральний вузол MESH5 виконує роль ядра бездротового сегмента та забезпечує додаткову маршрутизацію між периферійними mesh-вузлами. До кожного mesh-вузла підключені комутатори доступу (SWA1–SWA4), які забезпечують інтеграцію кінцевих пристроїв у мережу. До них під’єднані клієнтські комп’ютери (PC1–PC4) та велика кількість точок доступу (AP1–AP32), що формують бездротове покриття кампусу. Точки доступу організовані таким чином, щоб забезпечити рівномірне покриття навчальних корпусів та прилеглих територій.

Запропонована модель у GNS3 дозволяє імітувати реальну роботу університетської мережі, перевіряти маршрутизацію, відмовостійкість mesh-структури, а також взаємодію між дротовими та бездротовими сегментами. Загалом, архітектура забезпечує масштабованість, централізоване керування та високу надійність, що відповідає вимогам сучасних освітніх інформаційних систем. Далі розглянемо монтаж мережі з підключенням обладнання.

3.2 Мережеве обладнання та апаратна інфраструктура

Реалізація запропонованої університетської mesh-мережі передбачає розгортання багаторівневої інфраструктури, яка включає периметровий захист, ядро мережі, розподілений рівень доступу та бездротову mesh-топологію, яка об’єднує всі навчальні корпуси в єдиний інформаційний простір. На верхньому рівні підключення до глобальної мережі Інтернет здійснюється через міжмережевий екран, який використовує рішення класу enterprise, зокрема Fortinet FortiGate 100F або Cisco Firepower 1010, що забезпечують фільтрацію трафіку, IDS/IPS-захист, VPN-концентрацію та контроль прикладного рівня. Далі трафік передається на центральний маршрутизатор Cisco ISR 4331, який виконує міжвланову маршрутизацію, NAT, політики QoS, підтримку протоколів OSPF/BGP та організацію захищених IPSec VPN-тунелів для віддалених сегментів мережі. Маршрутизатор з’єднаний із ядром мережі через високошвидкісний комутатор, після чого трафік спрямовується до серверної інфраструктури, яка включає сервер автентифікації (Active Directory/RADIUS), сервер моніторингу та файловий сервер, розміщені у захищеній серверній зоні з резервуванням живлення та RAID-масивами для підвищення відмовостійкості.

Рівень керування бездротовою інфраструктурою реалізується через контролер Wi-Fi Cisco Catalyst 9800-L або Ubiquiti UniFi Cloud Key Gen2 Plus, який забезпечує централізовану конфігурацію точок доступу, роумінг користувачів, балансування навантаження та аналітику радіоефіру. Під його управлінням функціонують внутрішні точки доступу стандарту Wi-Fi 6, зокрема Cisco Catalyst 9120AXI або Ubiquiti UniFi U6 Enterprise, які підключаються до комутаторів доступу через PoE+ живлення, що дозволяє мінімізувати кількість окремих електричних підключень і спростити монтаж у стельовому просторі аудиторій та коридорів. На рівні доступу в кожному навчальному корпусі встановлюються керовані комутатори Cisco Catalyst 9200L або Aruba 6100, які забезпечують підключення кінцевих пристроїв, серверів локального рівня, IP-

телефонії та точок доступу, а також реалізують VLAN-сегментацію, STP/RSTP-захист від петель, DHCP Snooping і Port Security для запобігання несанкціонованому доступу.

Міжкорпусна взаємодія реалізується за допомогою зовнішніх mesh-вузлів, розміщених на дахах будівель та ключових відкритих майданчиках кампусу. Ці вузли формують бездротову магістральну топологію типу mesh, у якій кожен вузол має декілька сусідніх з'єднань, що забезпечує резервування маршрутів і автоматичну перебудову трафіку у разі відмови одного з каналів. Логічна структура mesh включає центральний вузол та розподілені вузли між корпусами, які утворюють стійку багатошляхову топологію з динамічною маршрутизацією. У якості обладнання використовуються Cisco Catalyst 1562I або Ubiquiti UniFi U6 Mesh, які встановлено на щоглах або дахових конструкціях із забезпеченням захисту від погодних умов (IP67) та живлення через PoE.

Фізичне з'єднання між активними компонентами всередині корпусів реалізується через структуровану кабельну систему на основі витої пари Cat6A, тоді як між будівлями використовуються оптичні канали зв'язку, що забезпечують високу пропускну здатність і мінімальні затримки. Комутатори ядра та розподілу розміщено у серверних шафах 42U з організованою системою патч-панелей, системою охолодження та резервним електроживленням (UPS). Усі активні компоненти інтегруються в єдину систему моніторингу, що дозволяє відслідковувати стан mesh-вузлів, завантаження каналів, якість радіосигналу та мережеві затримки в режимі реального часу.

Монтаж обладнання виконано з урахуванням зон радіопокриття та фізичних перешкод: внутрішні точки доступу встановлюються на стелі аудиторій та коридорів для рівномірного розподілу сигналу, комутатори розміщуються у телекомунікаційних шафах кожного поверху або корпусу, серверне обладнання – у захищеному дата-центрі, а зовнішні mesh-вузли – на дахах будівель із забезпеченням прямої видимості між корпусами. Підключення організорване за принципом ієрархічної зірки з елементами mesh-резервування: кінцеві пристрої підключаються до access-рівня, який агрегує трафік і передає

його на ядро, а міжкорпусний обмін даними виконується через бездротову mesh-магістраль. У результаті формується масштабована, відмовостійка та централізовано керована мережа кампусного типу, здатна забезпечити стабільний доступ до освітніх сервісів для кількох тисяч одночасних користувачів і підтримувати подальше розширення інфраструктури без суттєвої модернізації базового обладнання.

Рівень розподілу та доступу реалізовано на базі комутаторів Cisco Catalyst 9200L, які забезпечують високошвидкісну комутацію та підтримку функцій третього рівня (Layer 3). Дані пристрої виконують:

- міжвіртуальну маршрутизацію (Inter-VLAN Routing);
- агрегацію трафіку з рівня доступу;
- забезпечення логічної сегментації мережі;
- реалізацію політик доступу до ресурсів.

Бездротовий сегмент мережі побудований на основі сучасних технологій Wi-Fi 6 та централізованого управління. Внутрішній бездротовий доступ забезпечується точками доступу Cisco Catalyst 9120AXI, які підтримують стандарт 802.11ax та забезпечують високу пропускну здатність і ефективне використання радіочастотного спектра. Зовнішня бездротова інфраструктура реалізується за допомогою mesh-вузлів Cisco Catalyst 1562I, які формують часткову mesh-топологію для забезпечення альтернативних каналів зв’язку між корпусами закладу освіти.

Централізоване керування бездротовою мережею здійснюється через контролер Cisco Catalyst 9800-L, який виконує автоматичне налаштування точок доступу, керування SSID, оптимізацію радіоресурсів та забезпечення безшовного роумінгу користувачів. Серверний сегмент мережі включає набір спеціалізованих серверів, які забезпечують функціонування ключових мережевих сервісів:

- сервер автентифікації (RADIUS/AAA);
- сервер доменних служб (AD);
- файловий сервер для зберігання даних;

– сервер моніторингу та управління мережею.

Дані сервери підключаються до мережі через комутатори рівня доступу та ізольовані в окремій логічній VLAN-сегментації. Фізична інфраструктура мережі побудована на основі структурованої кабельної системи (СКС), яка забезпечує з’єднання між корпусами, комутаторами та кінцевими пристроями.

Між будівлями передбачено використання оптичних каналів зв’язку, що забезпечують високу пропускну здатність, низьку затримку та стійкість до електромагнітних завад. До рівня кінцевих пристроїв належать:

– робочі станції користувачів;

– ноутбуки та мобільні пристрої;

– сервери;

– бездротові клієнти, що підключаються через Wi-Fi 6 інфраструктуру.

Підключення здійснюється через комутатори доступу та бездротові точки доступу відповідно до логічної VLAN-сегментації.

Запропонована апаратна інфраструктура базується на сучасному мережевому обладнанні Cisco корпоративного класу та забезпечує реалізацію багаторівневої архітектури кампусної мережі. Використання маршрутизатора ISR 4331, комутаторів Catalyst 9200L, бездротових рішень Wi-Fi 6, mesh-технології та системи безпеки Firepower 1010 дозволяє створити масштабовану, відмовостійку та безпечну мережеву інфраструктуру закладу вищої освіти.

3.3 Структурна схема мережі

Структурна схема проєктованої мережі закладу вищої освіти відображає взаємозв’язки між основними компонентами мережевої інфраструктури та демонструє організацію обміну даними між її сегментами. Побудова мережі здійснюється відповідно до ієрархічної моделі, що передбачає розподіл функцій між рівнями ядра, розподілу та доступу.

У центрі мережевої інфраструктури розташовується маршрутизатор Cisco ISR 4331, який виконує функції ядра мережі та забезпечує маршрутизацію трафіку між внутрішніми сегментами та зовнішніми мережами. Передача даних до мережі Internet здійснюється через міжмережевий екран Cisco Firepower 1010, який реалізує механізми фільтрації та захисту мережевого периметра.

До маршрутизатора ядра підключаються комутатори Cisco Catalyst 9200L, які формують рівень розподілу мережі. Вони забезпечують агрегацію трафіку від окремих корпусів закладу освіти, реалізують міжвіртуальну маршрутизацію та підтримують функціонування VLAN-сегментації.

Кожен корпус закладу освіти обладнується комутатором доступу Cisco Catalyst 9200L, до якого підключаються робочі станції користувачів, серверне обладнання, бездротові точки доступу та зовнішні mesh-вузли. Такий підхід дозволяє локалізувати трафік у межах окремих сегментів мережі та спростити подальше масштабування інфраструктури.

Бездротова мережа реалізується за допомогою точок доступу Cisco Catalyst 9120AXI, які забезпечують покриття внутрішніх приміщень корпусів та підтримують стандарт Wi-Fi 6. Централізоване управління точками доступу здійснюється контролером Cisco Catalyst 9800-L, що дозволяє автоматизувати процес налаштування бездротової мережі та забезпечити безшовний роумінг користувачів між зонами покриття.

Для організації зв’язку між корпусами та забезпечення резервування каналів передачі даних передбачається використання зовнішніх mesh-вузлів Cisco Catalyst 1562I. Вузли формують часткову mesh-топологію, у межах якої кожен вузол має декілька альтернативних маршрутів передачі трафіку. Такий підхід підвищує відмовостійкість мережі та дозволяє підтримувати зв’язок навіть у разі виходу з ладу окремих каналів або пристроїв.

Серверна інфраструктура мережі включає сервер автентифікації та авторизації (RADIUS/AAA), сервер доменних служб Active Directory, файловий сервер та сервер моніторингу. Усі сервери розміщуються в окремому сегменті мережі та взаємодіють із користувачами через комутаційну інфраструктуру

кампусу. Передача даних між корпусами здійснюється через оптичні канали зв’язку, які забезпечують високу пропускну здатність та надійність з’єднання. Поєднання оптичних каналів та mesh-інфраструктури дозволяє реалізувати резервування мережевих ресурсів і підвищити загальну доступність сервісів.

Структурну схему проєктованої мережі наведено на рисунку 3.2.

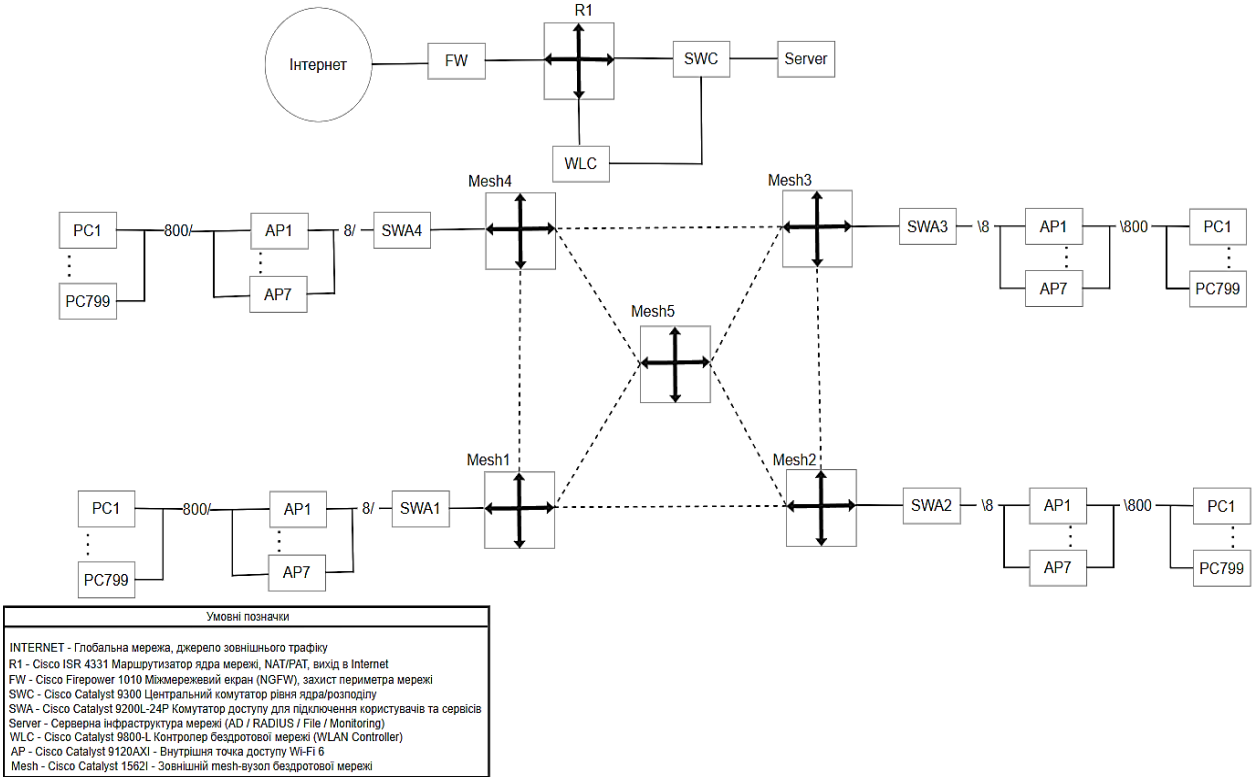


Рисунок 3.2 - Структурна схема мережі

Наведена структурна схема мережі відображає багаторівневу гібридну архітектуру, яка поєднує класичну ієрархічну модель локальної мережі з бездротовою mesh-топологією для забезпечення зв’язності між корпусами університетського кампусу. На граничному рівні мережі розташовано підключення до глобальної мережі Internet, через яке зовнішній трафік потрапляє до міжмережевого екрану (FW). Далі трафік спрямовується до маршрутизатора R1, який виконує функції основного вузла маршрутизації та розподілу потоків даних між сегментами мережі. До нього підключено центральний комутатор SWC, що забезпечує агрегацію внутрішнього трафіку, а також серверну інфраструктуру, яка реалізує сервіси зберігання даних і прикладні сервіси.

Паралельно інтегровано контролер бездротової мережі (WLC), який централізовано керує точками доступу Wi-Fi, забезпечуючи їхню конфігурацію, безпеку та балансування навантаження.

Рівень доступу представлений комутаторами доступу SWA1–SWA4, які забезпечують підключення кінцевих пристроїв, зокрема робочих станцій (PC1–PC799) та точок доступу (AP1–AP7) у кожному корпусі. Точки доступу формують бездротове покриття локальних сегментів мережі та передають трафік до комутаторів доступу. Між будівлями реалізовано mesh-структуру, утворену вузлами Mesh1–Mesh5, які забезпечують бездротову магістральну взаємодію між корпусами. Mesh-вузли формують резервовані канали зв’язку у вигляді частково з’єднаної топології, що підвищує відмовостійкість і забезпечує автоматичну перебудову маршрутів у разі втрати окремих лінків.

Таким чином, запропонована архітектура поєднує централізоване керування (WLC, FW, R1, SWC) з розподіленою бездротовою mesh-топологією між корпусами, що забезпечує масштабованість, відмовостійкість, ефективне керування трафіком та стабільне покриття території університетського кампусу.

3.4 Технології та протоколи маршрутизації

У межах проєкту використовується сучасна багаторівнева ієрархічна архітектура, яка відповідає рекомендаціям Cisco Enterprise Campus Architecture. Проєктована мережа розподілена на рівні доступу, розподілу та ядра, що дозволить забезпечити масштабованість, відмовостійкість та централізоване керування мережевими ресурсами. Функції ядра мережі реалізовано на базі маршрутизатора Cisco ISR 4331, який виконує агрегацію трафіку з внутрішніх сегментів та забезпечує взаємодію із зовнішніми мережами, включаючи Internet. На даному пристрої передбачається використання статичної маршрутизації та

технології трансляції мережевих адрес (NAT/PAT), що дозволяє забезпечити доступ користувачів приватної мережі до глобальних ресурсів.

Рівень розподілу та доступу реалізується на основі комутаторів Cisco Catalyst 9200L, які забезпечують високошвидкісну комутацію та підтримку функцій Layer 3. На цих пристроях реалізовано міжвіртуальну маршрутизацію (Inter-VLAN Routing) із використанням SVI-інтерфейсів, що дозволяє забезпечувати логічну сегментацію мережі та ізоляцію трафіку різних груп користувачів і сервісів.

Бездротовий доступ забезпечено внутрішніми точками доступу Cisco Catalyst 9120AXI, які підтримують стандарт Wi-Fi 6 (802.11ax). Вони забезпечує високу пропускну здатність, низьку затримку та ефективне використання радіочастотного спектра. Зовнішня бездротова інфраструктура реалізована на основі mesh-вузлів Cisco Catalyst 1562I, які формують часткову mesh-топологію. Це дозволяє забезпечити резервні канали передачі даних між корпусами та підвищувати відмовостійкість мережі при виході з ладу окремих з’єднань.

Централізоване керування бездротовою інфраструктурою здійснюється за допомогою контролера Cisco Catalyst 9800-L, який забезпечує автоматичне налаштування точок доступу, керування політиками безпеки та оптимізацію радіоресурсів бездротової мережі. Функції мережевої безпеки реалізуються на базі міжмережевого екрану Cisco Firepower 1010. Він забезпечує фільтрацію трафіку, контроль доступу, виявлення загроз та захист внутрішньої мережі від несанкціонованих підключень.

Для побудови логічної структури мережі передбачається використання VLAN-сегментації, яка дозволяє розділити трафік за функціональним призначенням (користувачі, бездротова мережа, серверна інфраструктура, адміністративне керування). Міжвіртуальна маршрутизація реалізована на комутаторах Cisco Catalyst 9200L за допомогою SVI-інтерфейсів, що забезпечить обмін трафіком між VLAN без необхідності використання маршрутизатора ядра.

На маршрутизаторі Cisco ISR 4331 застосовується налаштування статичних маршрутів і маршруту за замовчуванням, який визначає напрямок

передачі зовнішнього трафіку до мережі Internet через міжмережевий екран Cisco Firepower 1010. Такий підхід дозволяє централізовано контролювати вихідний трафік та спрощує структуру маршрутної таблиці ядра мережі.

Для забезпечення доступу внутрішніх вузлів із приватною адресацією до зовнішніх мереж використано технологію трансляції мережевих адрес (NAT/PAT), яка реалізується на маршрутизаторі Cisco ISR 4331. Це дозволяє великій кількості внутрішніх пристроїв використовувати обмежену кількість публічних IP-адрес для доступу до зовнішніх ресурсів.

Для підвищення масштабованості та автоматизації обміну маршрутною інформацією в межах кампусної мережі застосовано протокол динамічної маршрутизації OSPF (Open Shortest Path First), який забезпечує швидку конвергенцію мережі та оптимальний вибір маршрутів між її сегментами. При цьому бездротова частина мережі побудована з використанням часткової mesh-топології на базі зовнішніх вузлів Cisco Catalyst 1562I. Така архітектура дозволяє організувати альтернативні маршрути передачі даних між корпусами, що підвищує відмовостійкість мережі та її стійкість до відмов. Управління підключеннями здійснюється через контролер Cisco Catalyst 9800-L.

3.5 Додаткові протоколи та сервіси

При проєктуванні мережі застсовуються додаткові мережеві протоколи і сервіси, які забезпечують централізоване керування інфраструктурою, підвищення рівня інформаційної безпеки, контроль доступу користувачів та моніторинг стану мережевих ресурсів. Застосування цих технологій спрямоване на підвищення надійності, масштабованості та захищеності мережевого середовища. Для централізованої автентифікації користувачів у мережі передбачається використання сервера RADIUS, інтегрованого з системою AAA (Authentication, Authorization, Accounting). Застосування сервісу забезпечує:

– перевірку облікових даних користувачів при підключенні до мережі;

– централізоване управління правами доступу;

– ведення журналів підключень та дій користувачів;

– реалізацію політик безпеки корпоративного рівня.

Автентифікація застосовується як для доступу до Wi-Fi мережі, так і для доступу до внутрішніх корпоративних сегментів. Централізоване керування бездротовою мережею передбачається здійснювати за допомогою контролера Cisco Catalyst 9800-L, який виконує функції Wireless LAN Controller (WLC).

До основних функцій контролера належать:

– автоматичне налаштування точок доступу Cisco Catalyst 9120AXI;

– централізоване управління SSID та політиками безпеки;

– оптимізація радіочастотного середовища (Radio Resource Management, RRM);

– балансування навантаження між точками доступу;

– забезпечення безшовного роумінгу користувачів у межах кампусу.

Зовнішня бездротова інфраструктура проєктується на основі вузлів Cisco Catalyst 1562I, які підтримують технологію часткової mesh-топології.

Використання mesh-архітектури дозволяє:

– організувати альтернативні маршрути передачі даних між корпусами;

– забезпечити підключення без необхідності повного кабельного з’єднання між будівлями;

– підвищити відмовостійкість мережі;

– автоматично змінювати маршрути передачі трафіку у разі виходу з ладу

– окремих вузлів або каналів зв’язку.

Захист периметру проєктованої мережі реалізуємо на базі міжмережевого екрана Cisco Firepower 1010, що працює як Next Generation Firewall (NGFW).

Пристрій забезпечує:

– stateful inspection мережевих пакетів;

– політико-орієнтовану фільтрацію трафіку;

– систему виявлення та запобігання вторгненням (IPS);
– контроль застосунків і мережевих сервісів;
– сегментацію внутрішнього та зовнішнього трафіку.

У мережі використовуємо службу DHCP для автоматичного призначення конфігураційних параметрів кінцевим пристроям у відповідних VLAN.

Застосування DHCP забезпечує:

– зменшення обсягу ручного налаштування мережевих пристроїв;
– централізоване управління IP-адресним простором;
– зниження ймовірності конфігураційних помилок;
– спрощення масштабування мережі.

Для контролю стану та працездатності мережевої інфраструктури застосовуємо сервер моніторингу, який забезпечує:

– збір статистичних даних щодо навантаження мережі;
– моніторинг доступності мережевих пристроїв;
– аналіз продуктивності каналів зв’язку;
– виявлення та фіксацію аварійних ситуацій.

У складі серверної інфраструктури маємо файловий сервер, що забезпечує:

– централізоване зберігання навчальних та службових даних;
– контроль доступу користувачів до ресурсів;
– резервування та захист критично важливої інформації.

Впровадження додаткових мережевих сервісів, зокрема RADIUS/AAA, DHCP, системи моніторингу, централізованого контролера бездротової мережі та міжмережевого екрана Cisco Firepower 1010, дозволяє сформувати комплексну, безпечну та керовану кампусну інфраструктуру. Інтеграція зазначених технологій забезпечує високу відмовостійкість, масштабованість та централізоване адміністрування мережі закладу вищої освіти.

4 НАЛАШТУВАННЯ МЕРЕЖ І МІЖМЕРЕЖЕВИХ З'ЄДНАНЬ

4.1 Поетапне впровадження VLAN у мережі

Виходячи з розробленої та впровадженої структури мережі, наведемо поетапне впровадження логічної сегментації мережі закладу вищої освіти за допомогою технології VLAN. Реалізація VLAN здійснюється на комутаторах Cisco Catalyst 9200L із подальшою інтеграцією міжвіртуальної маршрутизації та налаштуванням міжмережевих з'єднань.

Описані нижче конфігураційні команди демонструють практичну реалізацію створеної логічної структури мережі, включаючи розподіл трафіку між сегментами, налаштування транкових з'єднань та забезпечення взаємодії між VLAN (рис. 4.1). Це дозволяє перейти від теоретичної моделі до її безпосередньої технічної реалізації в середовищі Cisco.

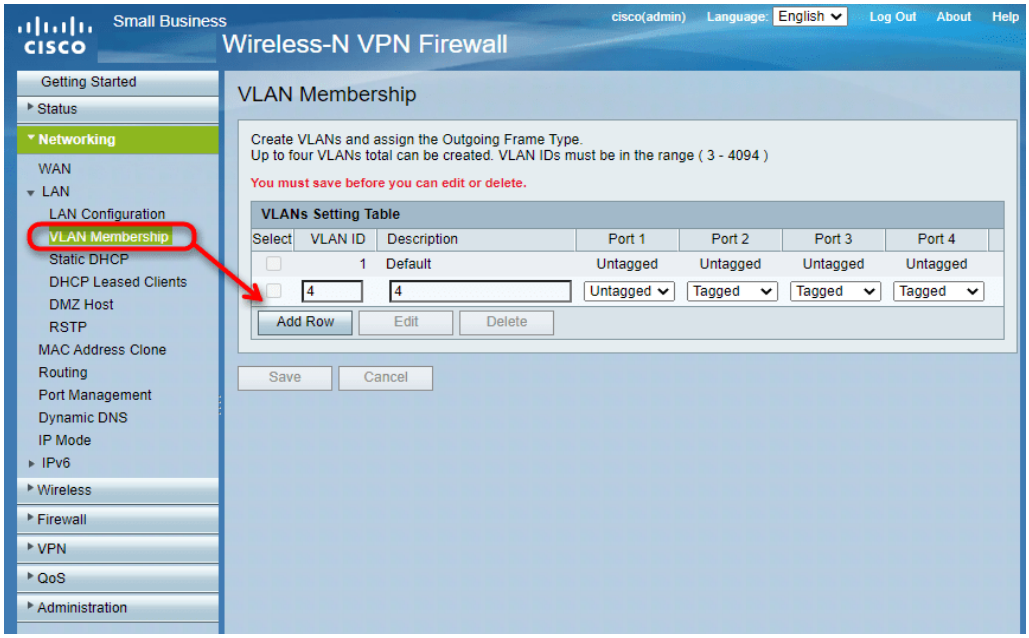


Рисунок 4.1 – Налаштування VLAN

Наводимо конфігурацію Core / Distribution Switch (Cisco Catalyst 9200L). Спочатку здійснюється перехід до привілейованого режиму та режиму глобальної конфігурації:

```
enable
configure terminal
```

Після цього створюються віртуальні локальні мережі (VLAN), які забезпечують логічну сегментацію мережі за функціональним призначенням:

```
vlan 10
name USERS
vlan 20
name WIFI
vlan 30
name SERVERS
vlan 99
name MGMT
```

Для VLAN 10 (користувачі):

```
interface vlan 10
ip address 192.168.10.1 255.255.255.0
 no shutdown
```

Для VLAN 20 (бездротова мережа):

```
interface vlan 20
ip address 192.168.20.1 255.255.255.0
no shutdown
```

Для VLAN 30 (серверна інфраструктура):

```
interface vlan 30
ip address 192.168.30.1 255.255.255.0
no shutdown
```

Для VLAN 99 (адміністративне управління):

```
interface vlan 99
ip address 192.168.99.1 255.255.255.0
no shutdown
```

Наступним етапом виконується налаштування інтерфейсу, який забезпечує зв’язок із маршрутизатором Cisco ISR 4331:

```
ip routing
interface gigabitEthernet1/1/1
description TO_ISR4331
no switchport
```

```
ip address 10.0.0.2 255.255.255.252
no shutdown
ip route 0.0.0.0 0.0.0.0 10.0.0.1
write memory
```

У результаті виконаного налаштування комутатора Cisco Catalyst 9200L реалізовано логічну сегментацію мережі шляхом створення окремих VLAN для користувачів, бездротової мережі, серверної інфраструктури та адміністративного управління, що забезпечує підвищення рівня безпеки та ефективності використання мережевих ресурсів. Додатково налаштовано міжмережеву маршрутизацію та підключення до маршрутизатора Cisco ISR 4331, що дозволяє забезпечити взаємодію між усіма сегментами мережі та доступ до зовнішніх мережевих ресурсів.

4.2 Налаштування комутатора доступу

При налаштуванні комутатора доступу спочатку виконується перехід до привілейованого режиму та режиму глобальної конфігурації:

```
enable
configure terminal
```

На даному етапі створюються віртуальні локальні мережі, які використовуються для логічної сегментації трафіку:

```
vlan 10
vlan 20
vlan 30
vlan 99
```

Порти, які використовуються для підключення робочих станцій користувачів, налаштовуються як access-порти (рис. 4.2) та призначаються до VLAN 10:

```
interface range gigabitEthernet1/0/1-10
switchport mode access
switchport access vlan 10
```

```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/23, Gig0/1, Gig0/2
10   USERS                            active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10
20   WIFI                             active    Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20
30   SERVERS                          active    Fa0/21, Fa0/22, Fa0/24
99   MGMT                             active
```

Рисунок 4.2 – Налаштування access-портів

Порти, до яких підключаються бездротові точки доступу Cisco Catalyst 9120AXI, налаштовуються у VLAN 20:

```
interface range gigabitEthernet1/0/11-20
switchport mode access
switchport access vlan 20
```

Окремий порт виділяється для підключення серверів (AD/RADIUS, File Server, Monitoring):

```
interface gigabitEthernet1/0/24
switchport mode access
switchport access vlan 30
```

Для передачі трафіку між комутаторами використовується trunk-порт, який дозволяє передавати декілька VLAN одночасно:

```
interface gigabitEthernet1/0/48
switchport mode trunk
switchport trunk allowed vlan 10,20,30,99
```

Після завершення налаштувань конфігурація зберігається в пам’яті:

```
end
write memory
```

У результаті налаштування Cisco Catalyst 9200L реалізовано логічний розподіл мережевого трафіку між окремими VLAN, що дозволяє ізолювати кінцеві пристрої, бездротову інфраструктуру, серверні ресурси та мережу управління. Використання access-портів для кінцевих пристроїв і trunk-з’єднання між комутаторами забезпечує ефективну передачу даних, централізоване керування мережею та можливість подальшого масштабування мережевої інфраструктури закладу.

4.3 Налаштування маршрутизатора Cisco ISR 4331

При налаштуванні маршрутизатору на першому етапі виконується перехід до привілейованого режиму та режиму глобальної конфігурації маршрутизатора:

```
enable
configure terminal
```

Інтерфейс GigabitEthernet0/0/0 використовується для підключення маршрутизатора до міжмережевого екрана Cisco Firepower 1010. Для нього призначається IP-адреса та визначається роль зовнішнього інтерфейсу NAT:

```
interface gigabitEthernet0/0/0
description TO_FIREWALL
ip address 200.0.0.2 255.255.255.252
ip nat outside
no shutdown
```

Інтерфейс GigabitEthernet0/0/1 використовується для з'єднання маршрутизатора з центральним комутатором мережі. Для нього призначається IP-адреса та визначається роль внутрішнього інтерфейсу NAT:

```
interface gigabitEthernet0/0/1
description TO_CORE_SWITCH
ip address 10.0.0.1 255.255.255.252
ip nat inside
no shutdown
```

Для автоматичного обміну маршрутною інформацією між мережевими пристроями налаштовується протокол маршрутизації OSPF. Також задається ідентифікатор маршрутизатора та мережі, які братимуть участь у процесі маршрутизації:

```
router ospf 1
router-id 1.1.1.1
network 10.0.0.0 0.0.0.3 area 0
network 192.168.0.0 0.0.255.255 area 0
```

Для забезпечення доступу до зовнішніх мереж створюється маршрут за замовчуванням, який спрямовує весь невідомий трафік до міжмережевого екрана Cisco Firepower 1010:

```
ip route 0.0.0.0 0.0.0.0 200.0.0.1
```

Для забезпечення доступу внутрішніх користувачів до мережі Internet налаштовується механізм трансляції мережевих адрес. Спочатку створюється список доступу, який визначає внутрішні мережі, що підлягають трансляції:

```
access-list 1 permit 192.168.0.0 0.0.255.255
```

Після цього активується перевантаження NAT (PAT), що дозволяє всім внутрішнім вузлам використовувати одну зовнішню IP-адресу для доступу до зовнішніх ресурсів: `ip nat inside source list 1 interface gigabitEthernet0/0/0 overload`

Після завершення налаштування конфігурація зберігається в енергонезалежній пам'яті маршрутизатора:

```
end
write memory
```

У результаті виконаних налаштувань маршрутизатор Cisco ISR 4331 забезпечує маршрутизацію трафіку між внутрішніми сегментами мережі, підтримує обмін маршрутною інформацією за допомогою протоколу OSPF, виконує трансляцію мережевих адрес та забезпечує доступ користувачів до зовнішніх мереж через міжмережевий екран Cisco Firepower 1010.

4.4 Налаштування Firewall Cisco Firepower 1010 і DHCP

Для забезпечення захисту периметра мережі виконується базове налаштування міжмережевого екрана Cisco Firepower 1010. На першому етапі конфігурується внутрішній інтерфейс, який забезпечує взаємодію з маршрутизатором Cisco ISR 4331 та внутрішньою мережею закладу.

Внутрішньому інтерфейсу присвоюється ім'я inside, встановлюється максимальний рівень довіри та призначається IP-адреса:

```
interface inside
nameif inside
security-level 100
ip address 200.0.0.1 255.255.255.252
```

Наступним кроком налаштовується зовнішній інтерфейс міжмережевого екрана, який забезпечує підключення до мережі провайдера або мережі Internet.

Для даного інтерфейсу задається ім'я outside, встановлюється мінімальний рівень довіри та активується автоматичне отримання IP-адреси через DHCP:

```
interface outside
 nameif outside
 security-level 0
 ip address dhcp
```

У даній конфігурації інтерфейс inside представляє довірену внутрішню мережу та має рівень безпеки 100, тоді як інтерфейс outside використовується для взаємодії із зовнішніми мережами та має рівень безпеки 0. Такий підхід відповідає класичній архітектурі міжмережевого екрана та забезпечує базовий контроль доступу між внутрішнім і зовнішнім сегментами мережі.

Для автоматичного призначення IP-адрес кінцевим пристроям у мережі налаштовується служба динамічної конфігурації хостів (DHCP). Використання DHCP дозволяє централізувати управління адресним простором та зменшити кількість помилок, пов’язаних із ручним налаштуванням мережевих параметрів.

На першому етапі визначається діапазон IP-адрес, які не будуть видаватися клієнтським пристроям. Зарезервовані адреси використовуються для мережевого обладнання, серверів та інших пристроїв, яким необхідно призначити статичні IP-адреси:

```
ip dhcp excluded-address 192.168.10.1 192.168.10.20
```

Для користувацького сегмента мережі створюється DHCP-пул VLAN10. У конфігурації визначається мережева адреса підмережі, шлюз за замовчуванням та DNS-сервер:

```
ip dhcp pool VLAN10
network 192.168.10.0 255.255.255.0
default-router 192.168.10.1
dns-server 8.8.8.8
```

У даному випадку клієнтські пристрої VLAN 10 автоматично отримуватимуть IP-адресу з підмережі 192.168.10.0/24, а також параметри шлюзу та DNS-сервера. Аналогічним чином створюється DHCP-пул для бездротового сегмента мережі VLAN 20:

```
ip dhcp pool VLAN20
 network 192.168.20.0 255.255.255.0
 default-router 192.168.20.1
 dns-server 8.8.8.8
```

Клієнти бездротової мережі автоматично отримуватимуть IP-адреси з підмережі 192.168.20.0/24 та необхідні параметри мережевого підключення.

Після виконання наведених налаштувань служба DHCP забезпечує автоматичне призначення мережевих параметрів користувацьким і бездротовим пристроям. Це спрощує процес підключення нових вузлів до мережі, зменшує навантаження на адміністратора та забезпечує централізоване управління IP-адресним простором кампусної мережі.

4.5 Забезпечення відмовостійкості та надійності мережі

Виходячи із завдання щодо побудови бездротової мережі університетського кампусу площею близько 10 тис. м², одним із ключових критеріїв проєктування є забезпечення високої відмовостійкості мережевої інфраструктури та безперервного доступу користувачів до інформаційних ресурсів. Особливої актуальності це набуває в умовах функціонування розподіленого кампусу, де мережеве обладнання розташовується у декількох навчальних корпусах і між ними необхідно підтримувати стабільний зв’язок навіть у разі виникнення аварійних

ситуацій. З цією метою в проєкті використовується часткова mesh-топологія на базі зовнішніх вузлів Cisco Catalyst 1562I, яка забезпечує автоматичне резервування маршрутів передачі даних та усунення єдиної точки відмови в бездротовому сегменті мережі (рис. 4.3).

На відміну від традиційної схеми типу «точка-точка», де пошкодження одного каналу призводить до втрати зв’язку між сегментами мережі, mesh-архітектура передбачає наявність декількох альтернативних маршрутів між вузлами. Кожен mesh-вузол Cisco Catalyst 1562I може одночасно підтримувати декілька бездротових з’єднань із сусідніми вузлами, формуючи резервні шляхи передачі даних. У разі виходу з ладу одного з вузлів через технічну несправність, відсутність електроживлення, механічне пошкодження або погіршення радіочастотних умов мережа автоматично виконує перебудову маршрутів і перенаправляє трафік через інші доступні вузли без необхідності втручання адміністратора.

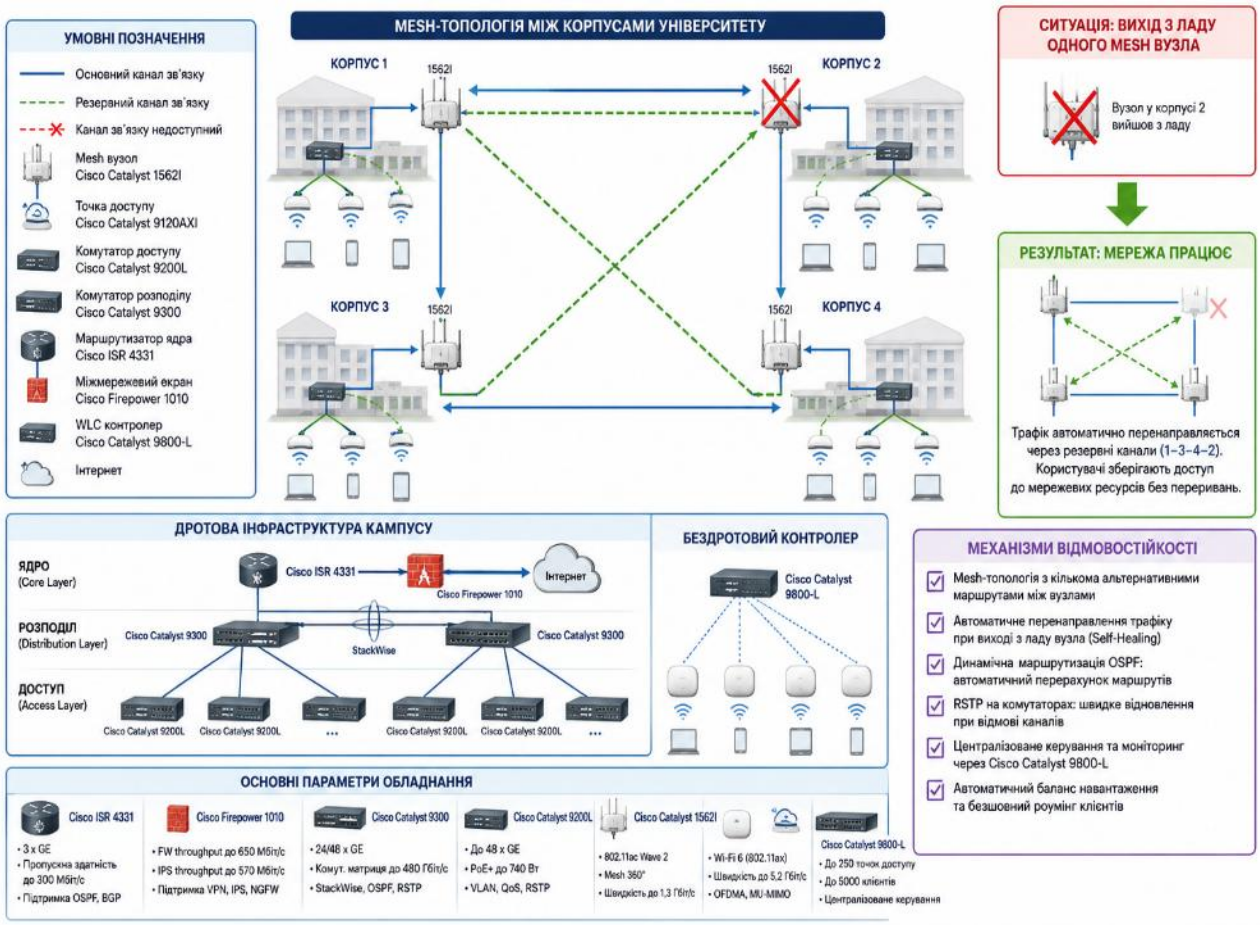


Рисунок 4.3 – Забезпечення відмовостійкості

Якщо один із зовнішніх mesh-вузлів, розташований між двома корпусами університету, припиняє функціонування, система автоматично знаходить альтернативний маршрут через сусідній вузол, який залишається працездатним. У результаті користувачі продовжують отримувати доступ до серверів, навчальних платформ, хмарних сервісів та мережі Інтернет без суттєвого переривання сеансів зв'язку. Такий механізм самовідновлення є однією з основних переваг технології mesh та суттєво підвищує надійність мережевої інфраструктури.

Для додаткового забезпечення відмовостійкості маршрутизація між мережевими сегментами реалізована за допомогою протоколу OSPF. У випадку втрати окремого маршруту або вузла протокол автоматично оновлює таблиці маршрутизації та обирає новий оптимальний шлях передачі пакетів. Час реакції системи на зміну топології становить лише декілька секунд, що дозволяє мінімізувати вплив аварійних ситуацій на роботу користувачів.

Дротова частина мережі також спроєктована з урахуванням вимог високої доступності. Рівень ядра побудований на базі маршрутизатора Cisco ISR 4331 з пропускною здатністю до 300 Мбіт/с, а рівні розподілу та доступу реалізовані на комутаторах Cisco Catalyst 9300 і Cisco Catalyst 9200L відповідно. Для запобігання утворенню мережевих петель та забезпечення коректної роботи резервних з'єднань використовується протокол Rapid Spanning Tree Protocol (RSTP), який автоматично активує резервні канали у разі відмови основних.

Бездротовий доступ користувачів забезпечується точками доступу Cisco Catalyst 9120AXI стандарту Wi-Fi 6 із максимальною швидкістю передачі даних до 5,2 Гбіт/с. Їх робота координується контролером Cisco Catalyst 9800-L, який виконує централізоване керування мережею, моніторинг стану обладнання та автоматичний розподіл навантаження між точками доступу. У випадку відмови окремої точки доступу контролер перенаправляє клієнтські пристрої до сусідніх точок із достатнім рівнем сигналу, що дозволяє зберігати безперервність бездротового доступу. Таким чином, основою забезпечення відмовостійкості мережі є саме використання mesh-топології, здатної автоматично адаптуватися до змін топології та функціонувати навіть при виході з ладу окремих вузлів або каналів

зв’язку. Завдяки наявності декількох альтернативних маршрутів, механізмам самовідновлення мережі, динамічній маршрутизації OSPF, резервуванню каналів та централізованому керуванню бездротовою інфраструктурою забезпечується висока доступність мережевих сервісів і безперервна робота інформаційно-комунікаційної системи університету навіть в умовах часткових відмов обладнання.

4.6 Безпека роботи мережі

Мережа університету передбачає реалізацію комплексу заходів інформаційної безпеки, спрямованих на захист мережевих ресурсів, контроль доступу користувачів та логічну сегментацію трафіку. Основним елементом захисту периметра виступає міжмережевий екран Cisco Firepower 1010, який забезпечує фільтрацію вхідного та вихідного мережевого трафіку, а також контроль політик доступу між внутрішньою корпоративною мережею та зовнішніми мережевими сегментами. На пристрої реалізовано розподіл на зони безпеки inside та outside, що дозволяє відокремити довірену внутрішню інфраструктуру від недовірених зовнішніх підключень і підвищити рівень захищеності мережі (рис. 4.4).

```
ciscoasa(config)#interface vlan 1
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 200.0.0.1 255.255.255.252
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)#interface vlan 2
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address dhcp
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)#interface vlan 2
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address dhcp
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)#interface ethernet0/1
ciscoasa(config-if)# switchport access vlan 1
ciscoasa(config-if)#
ciscoasa(config-if)#interface ethernet0/0
ciscoasa(config-if)# switchport access vlan 2
ciscoasa(config-if)#route outside 0.0.0.0 0.0.0.0 200.0.0.2
ciscoasa(config)#exit
```

Рисунок 4.4 – Налаштування інтерфейсів та зон безпеки

Додатковим рівнем підвищення безпеки є використання VLAN-сегментації, яка забезпечує логічне розділення користувацького, бездротового та серверного трафіку. Такий підхід зменшує ймовірність несанкціонованого доступу між різними групами користувачів і підвищує рівень ізоляції мережевих сегментів.

Для централізованої автентифікації користувачів бездротової мережі застосовується сервер AD/RADIUS, який функціонує у складі системи AAA. Це дозволяє реалізувати контроль доступу до мережі на основі унікальних облікових даних користувачів, забезпечує облік і аудит їх мережевої активності.

Також у мережі використовується окремий VLAN для керування мережевим обладнанням, що обмежує доступ до комутаторів та маршрутизатора лише адміністративним пристроям. Це підвищує рівень безпеки керування інфраструктурою та мінімізує ризики несанкціонованого втручання в конфігурацію мережевого обладнання.

Після завершення налаштування мережевої інфраструктури університету виконується комплексне тестування, яке включає перевірку працездатності VLAN, маршрутизації, бездротового доступу та політик безпеки. Спочатку перевіряється коректність сегментації мережі. Для цього до портів різних VLAN підключаються тестові клієнти, після чого виконується перевірка ізоляції між сегментами за допомогою команди ping. Пристрій у VLAN 10 (мережа користувачів) не повинен мати можливості отримати відповідь від пристрою у VLAN 20 (серверний сегмент). Це підтверджує правильність реалізації міжвланової ізоляції або політик доступу.

Далі перевіряється робота міжмережевої взаємодії через маршрутизатор або L3-комутатор шляхом тестування доступу до шлюзів кожного VLAN та перевірки таблиці маршрутизації командою show ip route. Окремо виконується тестування бездротової мережі. Клієнтський пристрій підключається до Wi-Fi з автентифікацією через AD/RADIUS. У процесі перевіряється успішність проходження AAA-аутентифікації, отримання IP-адреси через DHCP та доступ до дозволених ресурсів внутрішньої мережі.

Також перевіряється робота міжмережевого екрану Cisco Firepower 1010. Для цього виконуються спроби доступу до заборонених ресурсів із внутрішньої мережі у зовнішню та навпаки. У разі коректного налаштування такі з'єднання повинні блокуватися згідно з політиками безпеки. Завершальним етапом є тестування керованості мережевого обладнання через окремий management VLAN. Перевіряється доступ адміністратора до комутаторів і маршрутизаторів та відсутність доступу до цього сегмента з мереж користувачів.

4.7 Додаткові налаштування безпечних підключень і результати

Після завершення налаштування мережевого обладнання виконано перевірку коректності конфігурації за допомогою службових команд Cisco IOS.

Для перегляду створених VLAN використовується команда:

```
show vlan brief
```

Очікуваний результат:

```
VLAN Name                              Status    Ports
1    default                           active
10   USERS                             active    Gi1/0/1-10
20   WIFI                              active    Gi1/0/11-20
30   SERVERS                           active    Gi1/0/24
99   MGMT                              active
```

Результат підтверджує успішне створення VLAN та призначення відповідних портів. Для перевірки стану фізичних і логічних інтерфейсів використовується команда:

```
show ip interface brief
```

Очікуваний результат:

```
Interface              IP-Address      Status      Protocol
Vlan10                 192.168.10.1    up          up
Vlan20                 192.168.20.1    up          up
Vlan30                 192.168.30.1    up          up
```

```
Vlan99                 192.168.99.1    up          up
Gi1/1/1                10.0.0.2        up          up
```

Отримані дані свідчать про коректну роботу інтерфейсів та активність мережевих з'єднань. Для перегляду маршрутів використовується команда:

```
show ip route
```

Очікуваний результат:

```
Gateway of last resort is 10.0.0.1

C    192.168.10.0/24 is directly connected, Vlan10
C    192.168.20.0/24 is directly connected, Vlan20
C    192.168.30.0/24 is directly connected, Vlan30
C    192.168.99.0/24 is directly connected, Vlan99
S*   0.0.0.0/0 [1/0] via 10.0.0.1
```

Наявність маршруту за замовчуванням підтверджує можливість передачі трафіку до зовнішніх мереж. Для перевірки трансляції мережевих адрес використовується команда:

```
show ip nat translations
```

Після генерації трафіку очікується поява записів такого типу:

```
Pro    Inside global  Inside local    Outside local    Outside global
icmp   200.0.0.2      192.168.10.100       8.8.8.8         8.8.8.8
tcp    200.0.0.2:1025 192.168.10.100:1025  8.8.8.8:80     8.8.8.8:80
```

Поява записів у таблиці підтверджує коректну роботу механізму трансляції адрес NAT/PAT. Для проведення перевірки доступності зовнішніх ресурсів використовується команда:

```
ping 8.8.8.8
```

Очікуваний результат:

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5)
```

Успішне проходження всіх пакетів підтверджує працездатність маршрутизації, NAT та з'єднання з мережею Internet.

На рисунку 4.5 представлено узагальнену багаторівневу архітектуру mesh-мережі університету, яка поєднує елементи маршрутизації, бездротового доступу, серверної інфраструктури та комплексної системи інформаційної безпеки. На верхньому рівні знаходиться підключення до глобальної мережі Інтернет, яке є зовнішнім каналом взаємодії університетської інформаційної системи з зовнішніми ресурсами, хмарними сервісами та віддаленими користувачами. Безпосередньо перед входом у внутрішню мережу розташовано міжмережевий екран, який виконує функції первинного контролю трафіку, забезпечує NAT-трансляцію адрес, фільтрацію пакетів та захист від зовнішніх кібератак, включаючи DDoS-подібні навантаження.

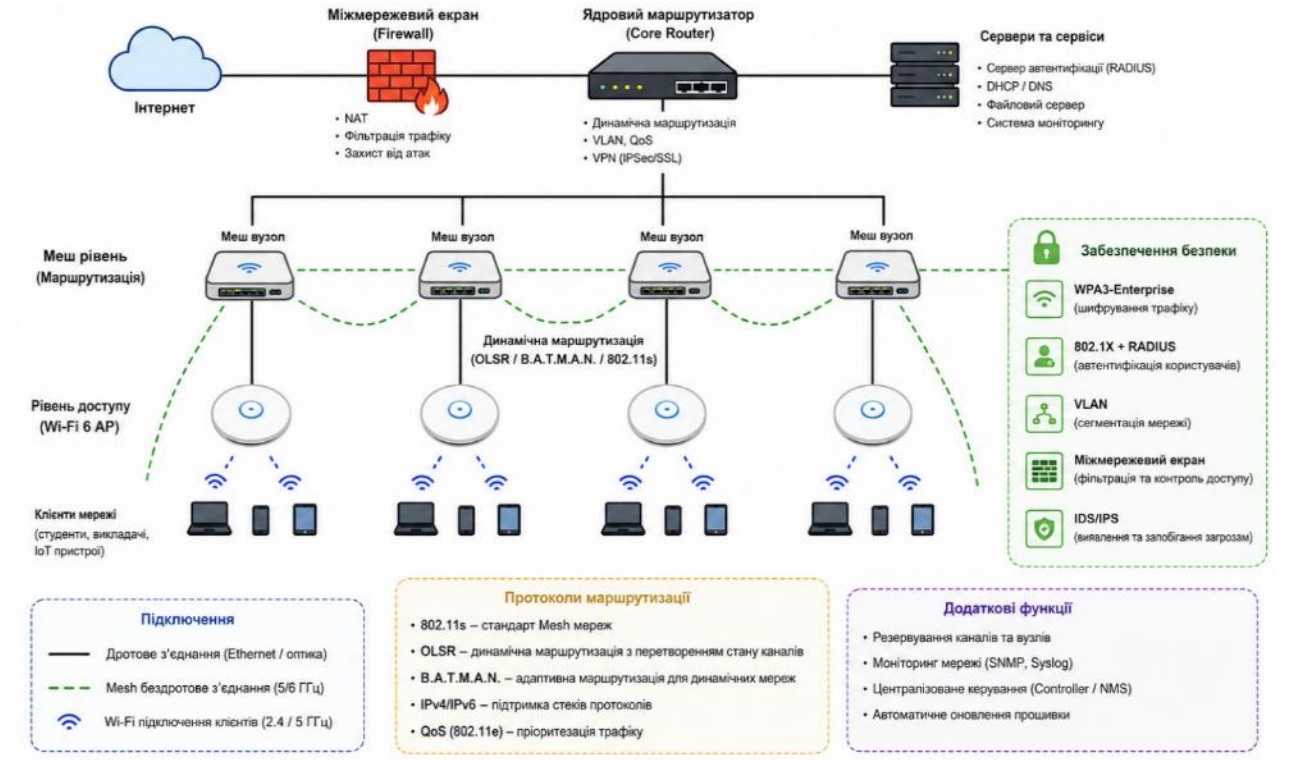


Рисунок 4.5 – Підключення, маршрутизація та безпека

Наступним елементом архітектури є маршрутизатор ядра, який виступає центральним вузлом обробки мережевого трафіку. Він забезпечує маршрутизацію між VLAN-сегментами, реалізацію політик QoS для пріоритезації навчального та службового трафіку, а також підтримку VPN-з'єднань на основі IPsec або SSL для безпечного віддаленого доступу до внутрішніх ресурсів університету.

Саме цей рівень формує логічну основу всієї мережевої інфраструктури та забезпечує її масштабованість.

Далі представлено серверний сегмент, який включає ключові сервіси університетської мережі. Сервер автентифікації забезпечує централізоване управління користувачами та доступом через інтеграцію з RADIUS, DHCP та DNS-сервісами, що дозволяє реалізувати єдину політику ідентифікації. Файлові сервери використовуються для зберігання навчальних матеріалів, методичних ресурсів і резервних копій, забезпечуючи доступність та цілісність даних. Окремо функціонує система моніторингу, яка здійснює контроль стану мережі, серверів та каналів зв’язку в режимі реального часу, що дозволяє оперативно виявляти та усувати збої.

Середній рівень архітектури представлений mesh-вузлами, які формують розподілену бездротову топологію між корпусами університету. Ці вузли взаємодіють між собою через бездротові канали зв’язку та забезпечують динамічне перенаправлення трафіку у випадку відмови окремих вузлів. Для реалізації маршрутизації в mesh-сегменті застосовуються адаптивні протоколи OLSR та BATMAN, а також стандарт IEEE 802.11s, що забезпечує сумісність і автоматичне формування mesh-структури. Такий підхід підвищує відмовостійкість мережі та дозволяє забезпечити безперервність зв’язку між корпусами навіть у випадку часткових пошкоджень інфраструктури.

Нижній рівень архітектури включає точки доступу Wi-Fi 6, які забезпечують підключення кінцевих користувачів до мережі університету. До клієнтських пристроїв належать ноутбуки, смартфони, планшети та IoT-пристрої, що активно використовуються в освітньому процесі. Підключення здійснюється у діапазонах 2.4 та 5 ГГц, що дозволяє оптимізувати баланс між покриттям і швидкістю передачі даних.

Окремий блок схеми присвячено механізмам забезпечення безпеки інформаційної системи. Використання WPA3-Enterprise забезпечує сучасне шифрування бездротового трафіку та захист від перехоплення даних. Автентифікація користувачів реалізується на основі 802.1X із використанням RADIUS-серверів,

що дозволяє централізовано керувати доступом до мережі. Сегментація мережі здійснюється за допомогою VLAN, що розділяє трафік різних категорій користувачів та сервісів. Додатково впроваджуються системи IDS/IPS, які забезпечують виявлення та блокування потенційних мережевих атак у реальному часі.

У нижній частині схеми наведено протоколи маршрутизації та технології, що використовуються в mesh-мережі. Серед них 802.11s як базовий стандарт бездротових mesh-мереж, OLSR як протокол із обчисленням оптимальних маршрутів, BATMAN як адаптивний алгоритм для динамічних топологій, а також підтримка IPv4/IPv6 для забезпечення сумісності з сучасними мережевими стандартами. Додатково застосовується QoS (802.11e), що дозволяє пріоритезувати критичний трафік, зокрема відеолекції та сервіси дистанційного навчання.

Окремо виділено додаткові функції, які забезпечують стабільність та керованість мережі. До них належать резервування каналів та вузлів, що підвищує відмовостійкість системи, а також централізоване керування через контролери або NMS-системи. Моніторинг здійснюється за допомогою SNMP та Syslog, що дозволяє збирати діагностичні дані з усіх елементів інфраструктури. Також передбачено автоматичне оновлення прошивок мережевого обладнання, що підвищує рівень безпеки та зменшує адміністративне навантаження.

Узагальнюючи, представлена схема демонструє комплексну архітектуру університетської mesh-мережі, яка поєднує багаторівневу маршрутизацію, централізоване управління, сучасні механізми кібербезпеки та високопродуктивну бездротову інфраструктуру. Такий підхід забезпечує масштабованість, відмовостійкість і високий рівень захисту даних, що є критично важливим для функціонування сучасного цифрового освітнього середовища університету.

ВИСНОВКИ

У результаті виконання дипломної роботи здійснено проєктування та моделювання сучасної мережевої інфраструктури закладу вищої освіти з використанням технології Wi-Fi Mesh, що забезпечує безперервне, масштабоване та відмовостійке бездротове покриття в межах чотирьох навчальних корпусів. Розроблена архітектура мережі відповідає сучасним вимогам до продуктивності, безпеки та централізованого управління кампусними інформаційно-комунікаційними системами.

У межах роботи реалізовано комплекс сучасних мережевих технологій, зокрема VLAN із підтримкою IEEE 802.1Q для логічної сегментації трафіку, Gigabit Ethernet для високошвидкісних з’єднань, а також протоколи динамічної маршрутизації OSPF, сервіси DHCP, DNS, NAT/PAT і механізми автентифікації на основі RADIUS, що забезпечує безпечний доступ до мережевих ресурсів.

Побудована мережа базується на сучасному обладнанні Cisco, зокрема маршрутизаторі ISR 4331, комутаторах Catalyst 9300 та 9200L, точках доступу Catalyst 9120AXI, зовнішніх mesh-вузлах Catalyst 1562I, контролері бездротової мережі Catalyst 9800-L та міжмережевому екрані Firepower 1010. Також передбачено серверну інфраструктуру, яка включає сервери автентифікації AD/RADIUS, файловий сервер та сервер моніторингу мережі, що забезпечує комплексне адміністрування та контроль роботи мережі.

Моделювання запропонованої архітектури у середовищі GNS3 підтвердило її коректність, працездатність і відповідність заданим вимогам. Таким чином, розроблена мережева інфраструктура є ефективним рішенням для закладу вищої освіти, забезпечує високий рівень надійності, безпеки та масштабованості, а також може бути рекомендована як базова модель для впровадження сучасних кампусних мереж на основі Wi-Fi Mesh технологій.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Киричек Г.Г., Зайцев О.В., Литовченко М.С. Сучасна мережа вузу із застосуванням mesh технології. Міжнародна науково-практична конференція «*Проблеми та перспективи науки, освіти і суспільства в сучасних умовах*». (Полтава, 25 лют. 2026). Полтава, Україна, 2026. С.109-113. URL: https://drive.google.com/file/d/1gNEQPxMNIMhDjSjWvonI12VB4RYx0ix1/view (дата звернення: 23.04.2026).

2. Heinzelman W. R., Chandrakasan A., Balakrishnan H. Energy-efficient communication protocol for wireless microsensor networks. Proceedings of the 33rd Hawaii International Conference on System Sciences (HICSS). IEEE. 2000. P. 1–10. DOI: 10.1109/HICSS.2000.926982.

3. Winter T., Thubert P., Brandt A., Hui J., Kelsey R., Levis P., Pister K., Struik R., Vasseur J., Alexander R. RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks. RFC 6550. IETF. 2012. DOI: 10.17487/RFC6550.

4. Del-Valle-Soto C., Rodríguez A., Ascencio-Piña C. R. A survey of energy-efficient clustering routing protocols for wireless sensor networks based on metaheuristic approaches. Artificial Intelligence Review. 2023. Vol. 56(9). P. 9699–9770. DOI: 10.1007/s10462-023-10402-w.

5. Киричек Г.Г., Зайцев О.В., Тягунова М.Ю. Основні підходи до побудови mesh-мереж IoT. Міжнародна наук.-практ. конференція «*Розвиток науки, освіти та технологій як основа соціально-економічних змін: проблеми та перспективи*». (Остін, 5 бер. 2026). Остін, США, 2026. С.116-121. URL: https://drive.google.com/file/d/1iCKMp0m2MaIbVFHgaJfQurn55wsTM57c/view (дата звернення: 20.04.2026).

6. Зайцев О. В., Киричек Г. Г. Адаптивна бездротова mesh-мережа // Тиждень науки–2026. Факультет комп'ютерних наук і технологій : тези доповідей наук.-практ. конф., м. Запоріжжя, 13–17 квіт. 2026 р. / редкол.: В. Шаломєєв (відп. ред.). Запоріжжя : НУ «Запорізька політехніка», 2026.

7. Kaur L., Kaur R. A survey on energy efficient routing techniques in WSNs focusing IoT applications and enhancing fog computing paradigm. Global Transitions Proceedings. 2021. Vol. 2(2). P. 520–529. DOI: 10.1016/j. gltp.2021.08.001.

8. Behera T. M., Samal U. C., Mohapatra S. K., Khan M. S., Appasani B., Bizon N. Thounthong P. Energy- Efficient Routing Protocols for Wireless Sensor Networks: Architectures, Strategies, and Performance. Electronics. 2022. Vol. 11(15). Art. 2282. DOI: 10.3390/electronics11152282.

9. Darabkh K. A., Al-Akhras M., Zomot J. N., Atiquzzaman M. RPL routing protocol over IoT: A comprehensive survey, recent advances, insights, bibliometric analysis, recommendations, and future directions. Journal of Network and Computer Applications. 2022. Vol. 207. Art. 103476. DOI: 10.1016/j.jnca.2022.103476.

10. Tournier J., Lesueur F., Le Mouël F., Guyon L., Ben-Hassine H. A survey of IoT protocols and their security issues through the lens of a generic IoT stack. Internet of Things. 2020. Vol. 16. Art. 100264. DOI: 10.1016/j.iot.2020.100264.

11. Киричек Г.Г., Тягунова М.Ю., Братчиков В.В. Система кешування даних в розгалуженій мікросервісній архітектурі *Вчені записки ТНУ імені В.І. Вернадського. Серія: Технічні науки.* 2024. Том 35 (74) №1. Ч.1. С.141-146. DOI: 10.32782/2663-5941/2024.1.1/21.

12. Wood, M. J. Study of Network Design Considerations for Small Businesses. IOARP Journal of Communication and Networks (IOARP JCN), 2023, 3.1. pp.38-56.

13. Kaur L., Kaur R. A survey on energy efficient routing techniques in WSNs focusing IoT applications and enhancing fog computing paradigm. Global Transitions Proceedings. 2021. Vol. 2(2). P. 520–529. DOI: 10.1016/j. gltp.2021.08.001.

14. Ruaya E. P., Buladaco M. V. M. Virtual local area network (vlan) network design for nemsu-administration building. International Journal, 2022, 11.6. pp. 294-298.

15. Forbacha S. C., Agwu M. J. A. Design and implementation of a secure virtual private network over an open network (Internet). American Journal of Technology, 2023, 2.1: pp. 1-36.

16. Ogunyanda K., Ogunyanda O. O., Familua A. D., Shongwe T., Swart T. G., Cheng L. Wi-Fi 6 Data Transmission over a Low-Voltage Power Line Channel: Implementation and Analysis. Journal of Communications, 2025, 20.3: 315-323. DOI: 10.12720/jcm.20.3.315-323.

17. Дира В. В. Огляд взаємодії технологій ethernet і wifi у корпоративних телекомунікаційних мережах. Вчені записки ТНУ імені В.І. Вернадського. Серія: Технічні науки, 2024. 35 (74). № 3. С. 37-44. DOI: 10.32782/2663-5941/2024.3.2/05.

18. Wu X., O'Brien D. C. Parallel transmission LiFi. IEEE Transactions on Wireless Communications. 2020. № 19 (10). P. 6268–6276. DOI: 1010.1109/TWC.2020.3001983.

19. Киричек Г.Г., Школовий В.В. Забезпечення відмовостійкості та надійності мереж передачі даних. Вчені записки ТНУ імені В.І. Вернадського. Серія: Технічні науки. 2026. Том 37 (76) №1. Ч.2. С.128-134. DOI: 10.32782/2663-5941/2026.1.2/17.

20. Kumar S., Singh M., Gupta A., Tiwari M., Shadab A. Designing a Secure Campus Area Network with an Advanced DNS System. In: 2025 7th International Conference on Signal Processing, Computing and Control (ISPCC). IEEE, 2025. P. 1051-1056.

21. Zhong M., Xie W., Yang L. The Optimization and Improvement of Campus Network Based on MSTP. In: 2023 4th International Conference on Computers and Artificial Intelligence Technology (CAIT). IEEE, 2023. P. 212-216.

22. Киричек Г.Г., Живогляд В.А., Тягунова М.Ю. Система моніторингу мереж із підтримкою передачі повідомлень. Таврійський науковий вісник. Серія: Технічні науки. 2026. №1. Ч.1. С.122-130. DOI: 10.32782/tnv-tech.2026.1.1.14.

23. Prajapati D., Bowman J., Suvarna N. Designing Real-World Multi-domain Networks. Cisco Press, 2024. 456 p.

24. Tiahunova M., Kyrychek H., Bohatyrova T., Moshynets D. System and method of automatic collection of objects in the room. Paper presented at the *CEUR Workshop Proceedings*, 2021. Vol-3077. P. 174-186. URL: https://ceur-ws.org/Vol-3077/paper10.pdf (дата звернення: 23.04.2026).

25. Connectivity Standards Alliance. Zigbee Specification. Revision 23. 15 March 2023. URL: https://csa-iot.org/wp-content/uploads/2023/04/05-3474-23-csg-zigbee-specification-compressed.pdf (дата звернення: 28.04.2026).

26. Zhang Y., Luo J., Hu H. (Eds.). Wireless Mesh Networking: Architectures, Protocols and Standards. CRC Press, 2007.

27. Thread Group. Thread 1.3.0 Public Specification. 2023. URL: https://www.threadgroup.org/ThreadSpec

28. Ogundile O. O., Alfa A. S. A survey on an energy-efficient and energy-balanced routing protocol for wireless sensor networks. Sensors. 2017. Vol. 17(5). Art. 1084. DOI: 10.3390/s17051084.

ДОДАТОК А
СХЕМА МЕРЕЖІ

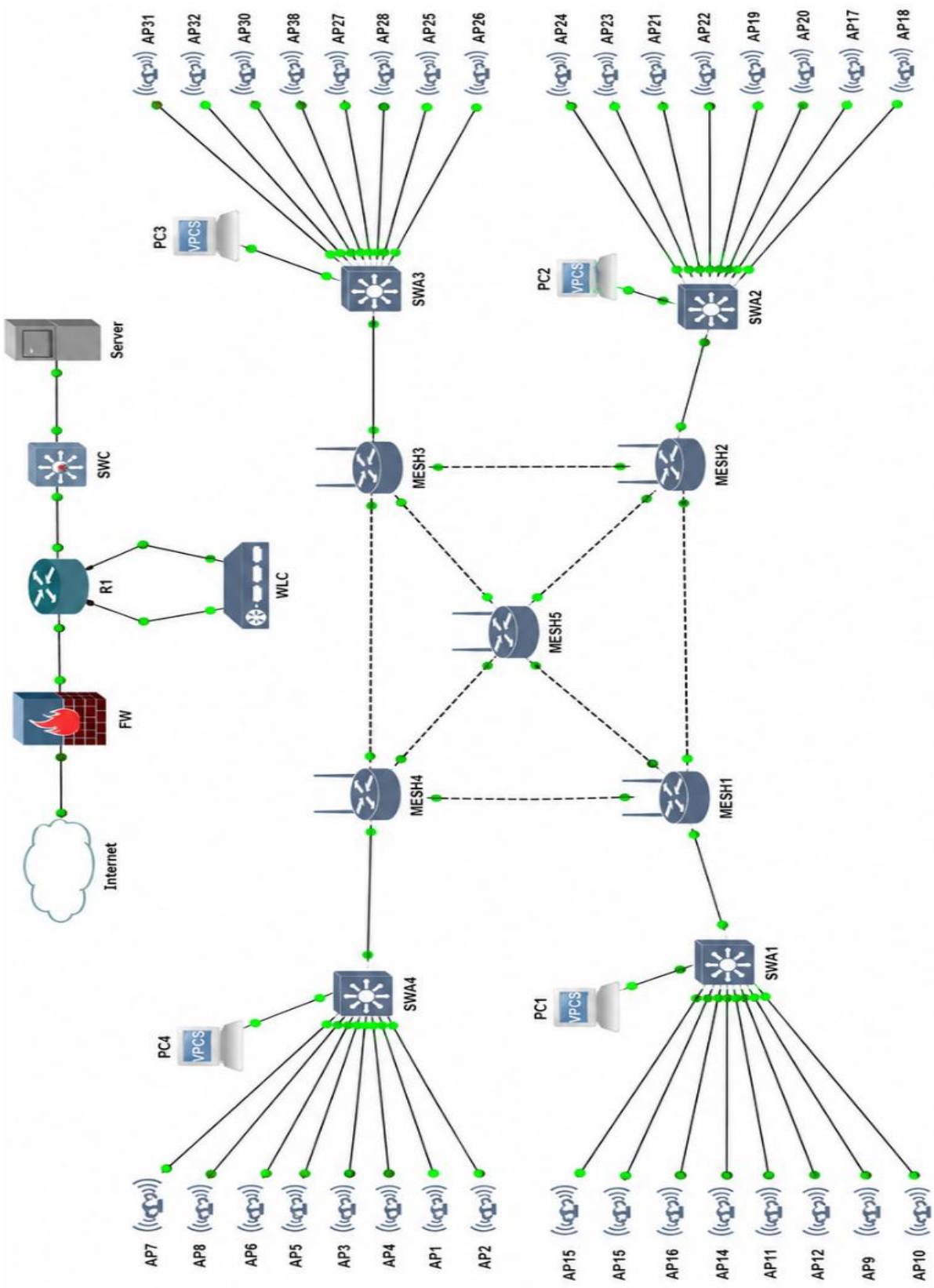


Рисунок А.1 – Логічна схема мережі

ДОДАТОК Б
СЛАЙДИ ПРЕЗЕНТАЦІЇ

Рисунок Б.1 – Слайд 1

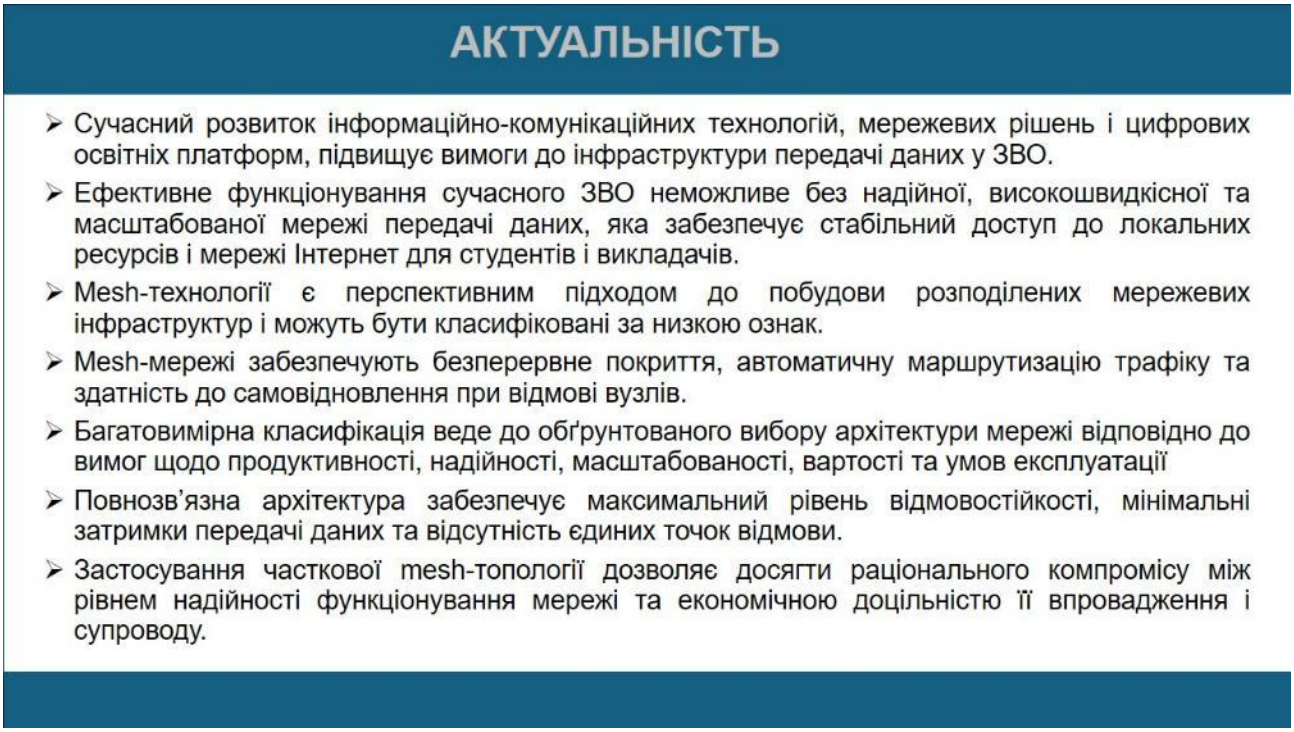


Рисунок Б.2 – Слайд 2

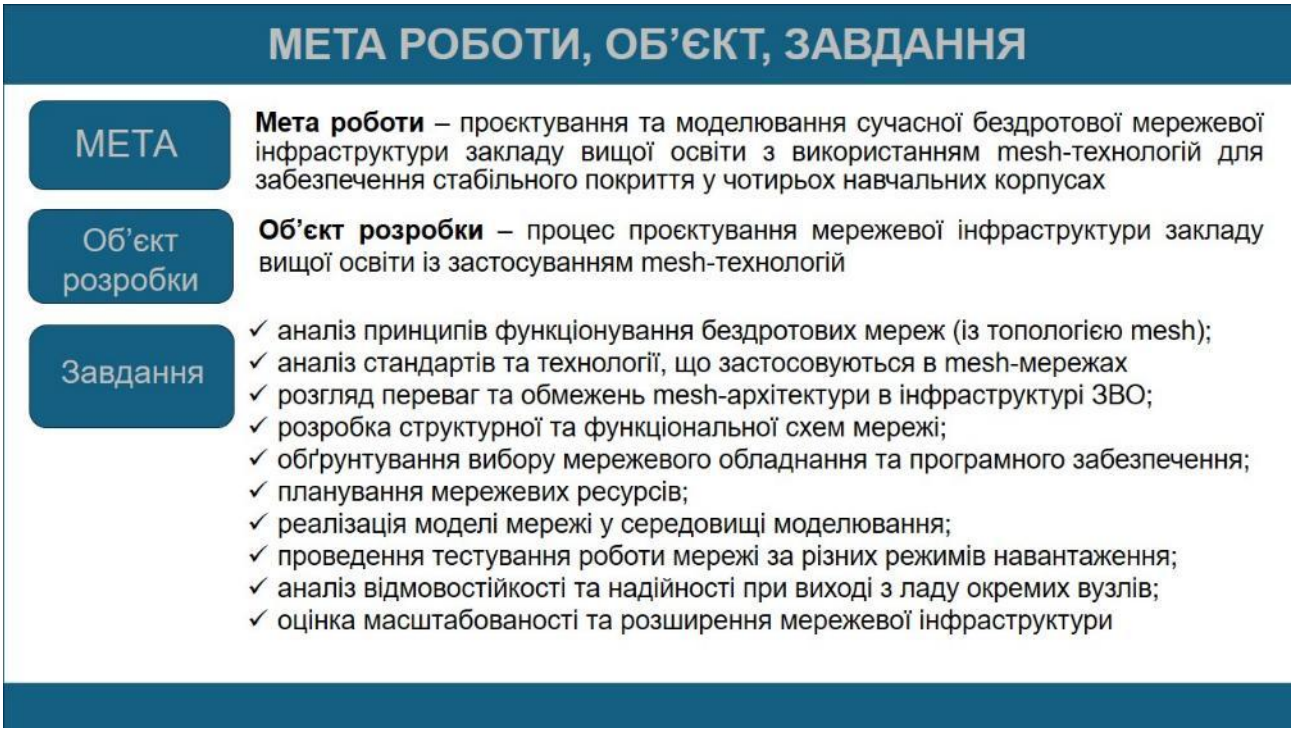


Рисунок Б.3 – Слайд 3

Рисунок Б.4 – Слайд 4

Рисунок Б.5 – Слайд 5

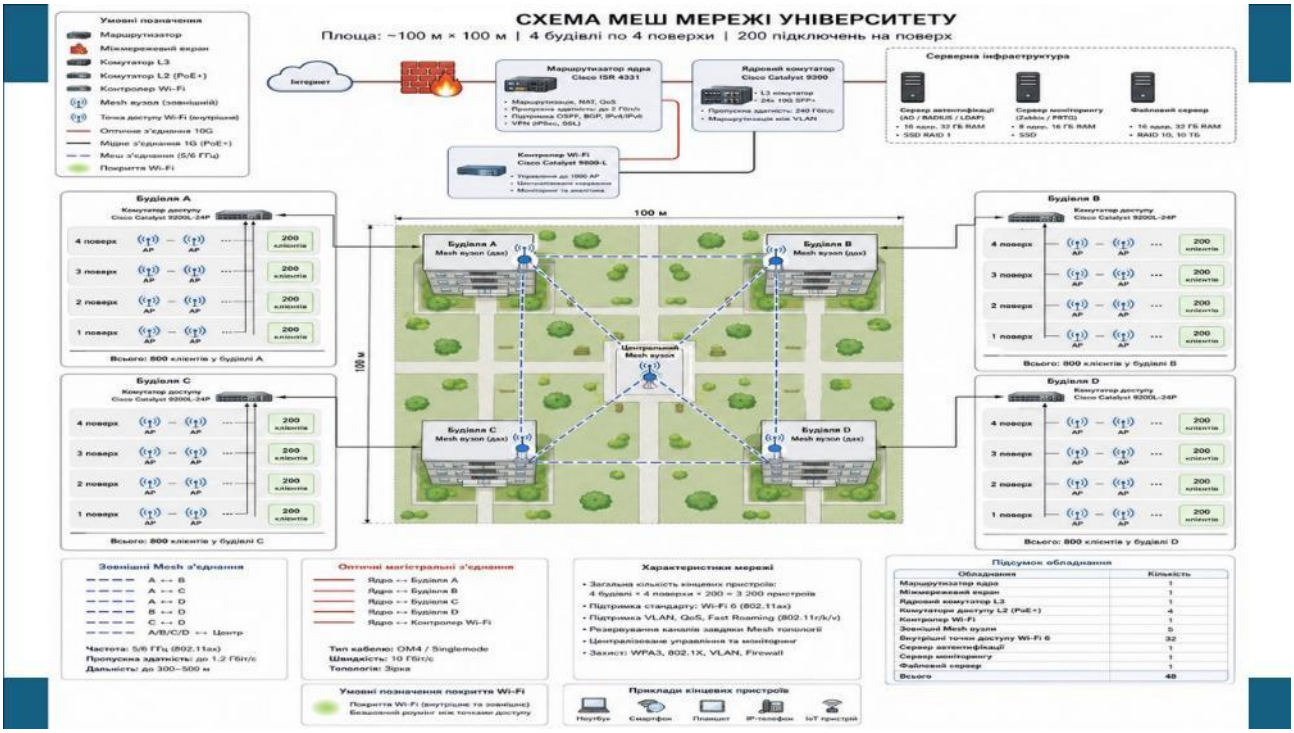


Рисунок Б.6 – Слайд 6

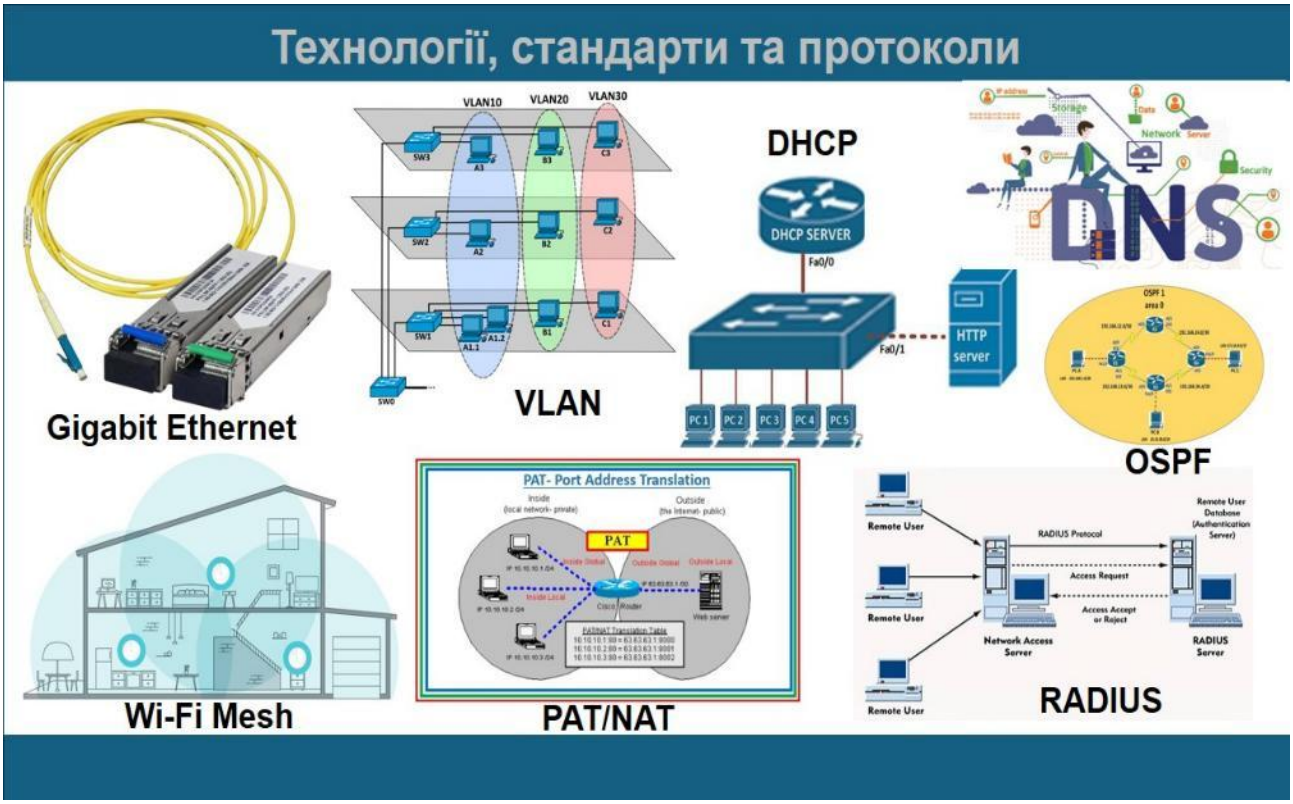


Рисунок Б.7 – Слайд 7

Обладнання	Кількість
Маршрутизатор ядра	1
Комутатори L2/L3	4
Внутрішні точки доступу Wi-Fi 6	32
Зовнішні Mesh-вузли	5
Контролер Wi-Fi	1
Сервер AD/RADIUS	1
Сервер моніторингу	1
Файловий сервер	1
Firewall	1
Оптичні лінії між корпусами	4

Рисунок Б.8 – Слайд 8

Рисунок Б.9 – Слайд 9

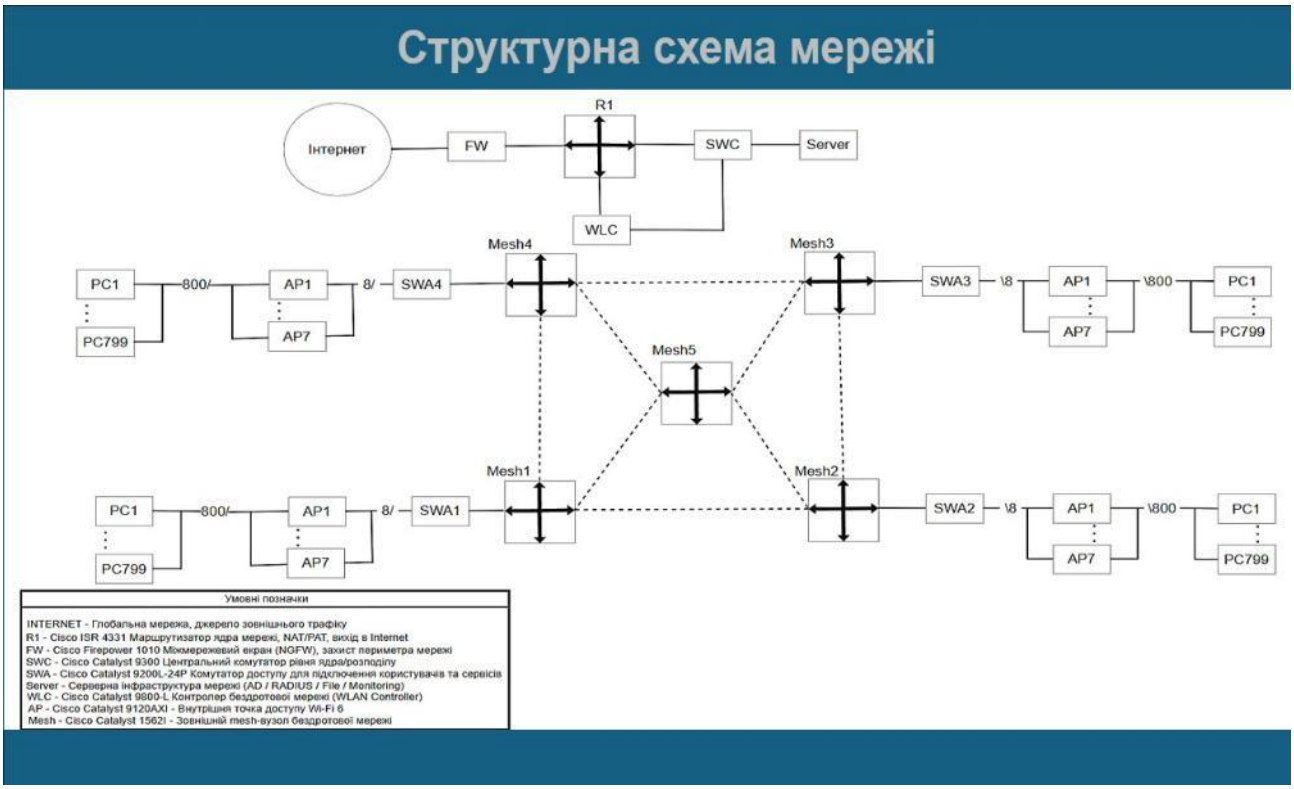


Рисунок Б.10 – Слайд 10

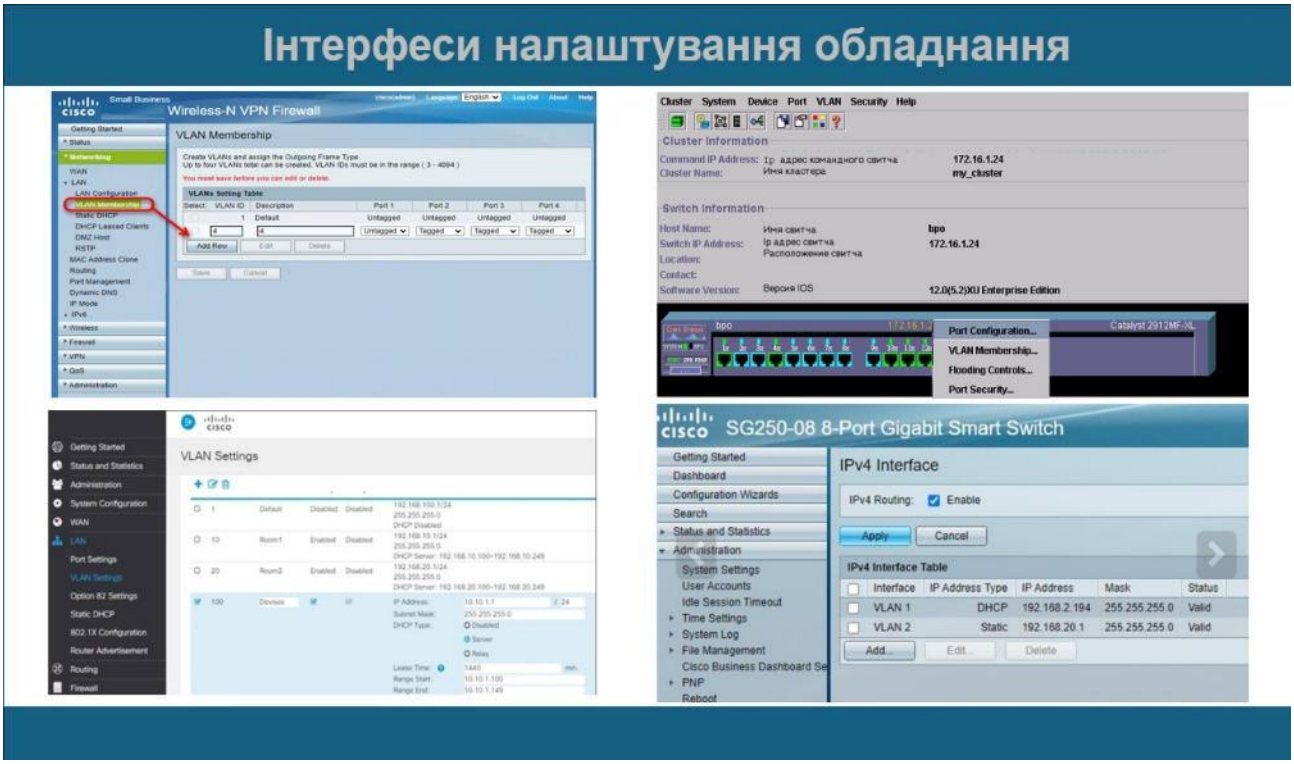


Рисунок Б.11 – Слайд 11

Рисунок Б.12 – Слайд 12

ВИСНОВКИ

- розглянуто актуальне завдання проєктування сучасної мережевої інфраструктури закладу вищої освіти з використанням mesh-технологій;
- проаналізовано особливості побудови бездротових та mesh-мереж, переваги та обмеження, сучасні стандарти, протоколи та технології;
- здійснено проєктування та моделювання сучасної мережевої інфраструктури закладу вищої освіти з використанням технології Wi-Fi Mesh;
- реалізовано комплекс сучасних мережевих технологій: VLAN із підтримкою IEEE 802.1Q; Gigabit Ethernet для високошвидкісних з'єднань; протокол динамічної маршрутизації OSPF; сервіси DHCP, DNS, NAT/PAT і механізми автентифікації на основі RADIUS;
- застосоване сучасне обладнання Cisco: маршрутизатор ISR 4331; комутатори Catalyst 9300 та 9200L; точки доступу Catalyst 9120AXI; mesh-вузли Catalyst 1562I; контролер бездротової мережі Catalyst 9800-L та міжмережевий екран Firepower 1010.

Рисунок Б.13 – Слайд 13

Публікації за темою роботи

1. *Киричек Г.Г.,* ***Зайцев О.В.****, Литовченко М.С.* ***Сучасна мережа вузу із застосуванням mesh технології****. Міжнародна науково-практична конференція «Проблеми та перспективи науки, освіти і суспільства в сучасних умовах». (Полтава, 25 лют. 2026). Полтава, Україна, 2026. С.109-113. URL: https://drive.google.com/file/d/1gNEQPxMNIMhDjSjWvonI12VB4RYx0ix1/view*

2. *Зайцев О. В**. , Киричек Г. Г.* ***Адаптивна бездротова mesh-мережа*** *// Тиждень науки–2026. Факультет комп'ютерних наук і технологій : тези доповідей наук.-практ. конф., м. Запоріжжя, 13–17 квіт. 2026 р. / редкол.: В. Шаломєєв (відп. ред.). Запоріжжя : НУ «Запорізька політехніка», 2026.*

3. Киричек Г.Г., ***Зайцев О.В.****, Тягунова М.Ю.* ***Основні підходи до побудови mesh-мереж IoT****. Міжнародна наук.-практ. конференція «Розвиток науки, освіти та технологій як основа соціально-економічних змін: проблеми та перспективи». (Остін, 5 бер. 2026). Остін, США, 2026. С.116-121. URL: https://drive.google.com/file/d/1iCKMp0m2MaIbVFHgaJfQurn55wsTM57c/view*

Рисунок Б.14 – Слайд 14