

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: ПРОЄКТУВАННЯ КОРПОРАТИВНОЇ МЕРЕЖІ З  
ВИКОРИСТАННЯМ ТЕХНОЛОГІЙ ETHERNET ТА  
ЦЕНТРАЛІЗОВАНОЇ АРХІТЕКТУРИ WLAN

Виконав(ла): студент(ка) 4 курсу,  
групи КНТ-522

Спеціальності  
123 Комп'ютерна інженерія  
(код і найменування спеціальності)

Освітня програма (спеціалізація)  
Комп'ютерна інженерія  
(назва освітньої програми (спеціалізації))

ЛИТОВЧЕНКО М.С.  
(ПРІЗВИЩЕ та ініціали)

Керівник КИРИЧЕК Г.Г.  
(ПРІЗВИЩЕ та ініціали)

Рецензент РОМАНОВСЬКИЙ О.В.  
(ПРІЗВИЩЕ та ініціали)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ  
Національний університет «Запорізька політехніка»

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)**

ЛИТОВЧЕНКА Максима Сергійовича

(ПРІЗВИЩЕ, ім'я, по батькові)

1. Тема проєкту (роботи) Проектування корпоративної мережі з використанням технологій Ethernet та централізованої архітектури WLAN  
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) Архітектурний план промислового кампусу з чотирма окремими корпусами для розміщення адміністрації, логістики, лабораторії та виробництва. Технічне завдання на розгортання єдиної корпоративної мережі з підтримкою дротового та бездротового сегментів зв'язку. Специфікації мережевого обладнання Cisco для побудови згорнутого ядра та рівня доступу. Вимоги щодо забезпечення відмовостійкості магістральних каналів та впровадження стандартів безпеки для ідентифікації користувачів. Програмне середовище для проведення імітаційного моделювання та перевірки проєктних рішень.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) 1) Опис предметної області: аналіз організаційної структури підприємства та характеристика мережевих інформаційних потоків між підрозділами;

2) Розробка вимог до мережевого та програмного забезпечення: вибір стандартів передачі даних та обґрунтування апаратної специфікації активного обладнання;

3) Моделювання мережевого та програмного забезпечення: розробка логічної структури віртуальних мереж та створення плану адресації вузлів;

4) Проектування архітектури мережевого та програмного забезпечення: розробка топології згорнутого ядра та конфігурація протоколів комутації і маршрутизації;

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

Функціональна схема мережі; Схема при'єднування мережі; Структурна схема мережі; Слайди презентації.

## 6. Консультанти розділів проєкту (роботи)

| Розділ        | ПРИЗВИЩЕ, 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 проєкту (роботи)                                | Строк виконання етапів проєкту ( роботи ) | Примітка |
|-------|-------------------------------------------------------------------------|-------------------------------------------|----------|
| 1     | Аналіз предметної області                                               | до 18.04.2026                             |          |
| 2     | Обґрунтування вибору апаратного забезпечення                            | до 22.04.2026                             |          |
| 3     | Проектування логічної структури та розподіл віртуальних локальних мереж | до 26.04.2026                             |          |
| 4     | Конфігурація протоколів комутації та міждоменної маршрутизації ядра     | до 30.04.2026                             |          |
| 5     | Розгортання бездротової інфраструктури та налаштування контролера       | до 03.05.2026                             |          |
| 6     | Інтеграція сервісів безпеки та служби автентифікації користувачів       | до 06.05.2026                             |          |
| 7     | Імітаційне моделювання інфраструктури та верифікація мережевих сервісів | до 12.05.2026                             |          |
| 8     | Розробка комплексу інженерних графічних креслень проєкту                | до 20.05.2026                             |          |
| 9     | Оформлення пояснювальної записки                                        | до 26.05.2026                             |          |
| 10    | Проходження нормоконтролю                                               | до 01.06.2026                             |          |
| 11    | Перевірка на наявність академічного плагіату                            | до 03.06.2026                             |          |
| 12    | Проходження рецензування                                                | до 10.06.2026                             |          |
|       |                                                                         |                                           |          |

Студент(ка)

( підпис )

Максим ЛИТОВЧЕНКО

(Ім'я ПРИЗВИЩЕ)

Керівник проєкту (роботи)

( підпис )

Галина КИРИЧЕК

(Ім'я ПРИЗВИЩЕ)

## РЕФЕРАТ

Пояснювальна записка до дипломної кваліфікаційної роботи бакалавра:  
76 с., 9 табл., 13 рис., 4 дод., 11 джерел.

ВІРТУАЛЬНА ЛОКАЛЬНА МЕРЕЖА, КОРПОРАТИВНА МЕРЕЖА, КОНТРОЛЕР БЕЗДРОТОВОЇ МЕРЕЖІ, МАРШРУТИЗАЦІЯ, МЕРЕЖЕВА БЕЗПЕКА, ТОЧКА ДОСТУПУ, CAPWAP, ETHERNET, IEEE 802.1X, VLAN, WLC, WLAN.

Об'єкт розробки – корпоративна комп'ютерна мережа підприємства.

Мета роботи – проєктування та розгортання захищеної корпоративної мережевої інфраструктури з використанням технологій Ethernet та централізованої архітектури WLAN для забезпечення високої відмовостійкості, безпеки й централізованого управління інформаційними потоками підприємства.

В ході розробки було проаналізовано технічне завдання та специфіку інформаційних потоків між різними функціональними підрозділами установи. Проведено проєктування логічної структури мережі за допомогою технології віртуальних локальних мереж, що дозволило ізолювати трафік відділів адміністрації, логістики, лабораторії та виробництва. Для усунення єдиної точки відмови впроваджено дворівневу ієрархічну модель Cisco із дубльованим комутаційним центром ядра мережі, на якому реалізовано міждоменну маршрутизацію Inter-VLAN Routing та автоматизовано розподіл IP-адрес через DHCP-пули. Бездротовий сегмент побудовано за централізованою архітектурою на базі апаратного контролера Cisco WLC 3504 та полегшених точок доступу Lightweight AP, що взаємодіють за допомогою тунелювання CAPWAP. Задля реалізації корпоративних стандартів безпеки інтегровано підсистему захисту IEEE 802.1X WPA2-Enterprise з централізованою автентифікацією користувачів на RADIUS-сервері.

В результаті розроблена та верифікована у середовищі симуляції Cisco Packet Tracer комплексна відмовостійка корпоративна мережа підприємства. Впроваджені архітектурні рішення забезпечили безшовний роумінг мобільних клієнтів під час переміщення між антенами та стабільну роботу DHCP-сервісів у межах єдиного ширококомовного домену управління. Створена інфраструктура має високий рівень безпеки завдяки унікальним обліковим даним користувачів, оптимізована для масового підключення нового обладнання та повністю готова до подальшого масштабування бізнесу.

## ЗМІСТ

|                                                                                                                                                                                          |    |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| Скорочення та умовні позначки .....                                                                                                                                                      | 8  |
| Вступ.....                                                                                                                                                                               | 9  |
| 1 Аналіз технічного завдання.....                                                                                                                                                        | 11 |
| 1.1 Структура підприємства з урахуванням наявних апаратних і мережних пристроїв .....                                                                                                    | 11 |
| 1.2 Аналіз інформаційних потоків і особливостей функціонування мережі .....                                                                                                              | 14 |
| 1.3 Постановка завдань, пов'язаних з розробкою та шляхи їх вирішення.....                                                                                                                | 16 |
| 2 Фізична реалізація мережі.....                                                                                                                                                         | 18 |
| 2.1 Вибір LAN технологій для ліній зв'язку між сегментами підприємства .....                                                                                                             | 18 |
| 2.2 Вибір мережних пристроїв з визначенням технічних характеристик для кожного конкретного пристрою або групи ідентичних пристроїв, опис їх призначення та особливості застосування..... | 21 |
| 2.3 Вибір кінцевих пристроїв. Опис технічних характеристик для кожного пристрою або групи пристроїв та особливості застосування.....                                                     | 24 |
| 2.4 Розробка функціональної схеми .....                                                                                                                                                  | 27 |
| 2.5 Розробка схеми при'єднування мережі.....                                                                                                                                             | 30 |
| 2.6 Монтаж мережі .....                                                                                                                                                                  | 32 |
| 2.7 Обґрунтування масштабованості фізичної та апаратної структури мережі .....                                                                                                           | 35 |
| 3 Логічна реалізація мережі .....                                                                                                                                                        | 37 |
| 3.1 Вибір протоколів канального та мережного рівнів .....                                                                                                                                | 37 |
| 3.2 Налаштування конфігураційних параметрів комутаторів .....                                                                                                                            | 39 |
| 3.3 Налаштування маршрутизаторів .....                                                                                                                                                   | 44 |
| 3.4 Налаштування бездротової мережі.....                                                                                                                                                 | 48 |

|                                                                           |    |
|---------------------------------------------------------------------------|----|
| 3.5 Забезпечення безпеки мережі .....                                     | 52 |
| 4 Імітаційне моделювання та тестування мережі .....                       | 57 |
| 4.1 Обґрунтування вибору програмного забезпечення для моделювання .....   | 57 |
| 4.2 Аналіз результатів тестування та верифікація мережевих сервісів ..... | 58 |
| 4.3 Управління трафіком та адміністрування мережі .....                   | 62 |
| 4.4 Надання якості обслуговування .....                                   | 62 |
| 4.5 Резервування модулів критичних для роботи мережі .....                | 63 |
| Висновки .....                                                            | 64 |
| Перелік джерел посилання .....                                            | 66 |
| Додаток А Функціональна схема мережі .....                                | 68 |
| Додаток Б Схема при'єднування мережі .....                                | 69 |
| Додаток В Структурна схема мережі .....                                   | 70 |
| Додаток Г Слайди презентації .....                                        | 71 |

## СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАЧКИ

|        |   |                                                                                                                  |
|--------|---|------------------------------------------------------------------------------------------------------------------|
| KM     | – | Комп'ютерна мережа                                                                                               |
| AAA    | – | Authentication, Authorization, Accounting, автентифікація, авторизація, облік                                    |
| ACL    | – | Access Control List, список контролю доступу                                                                     |
| AP     | – | Access Point, точка доступу                                                                                      |
| BYOD   | – | Bring Your Own Device, концепція використання власних пристроїв                                                  |
| CAPWAP | – | Control and Provisioning of Wireless Access Points, протокол керування та налаштування бездротових точок доступу |
| DHCP   | – | Dynamic Host Configuration Protocol, протокол динамічного налаштування вузла                                     |
| IEEE   | – | Institute of Electrical and Electronics Engineers, Інститут інженерів електротехніки та електроніки              |
| IP     | – | Internet Protocol, міжмережевий протокол                                                                         |
| LAN    | – | Local Area Network, локальна обчислювальна мережа                                                                |
| LAP    | – | Lightweight Access Point, полегшена точка доступу                                                                |
| MAC    | – | Media Access Control, управління доступом до середовища                                                          |
| RADIUS | – | Remote Authentication in Dial-In User Service, служба віддаленої автентифікації користувачів                     |
| SSID   | – | Service Set Identifier, ідентифікатор набору служб                                                               |
| SVI    | – | Switched Virtual Interface, комутований віртуальний інтерфейс                                                    |
| VLAN   | – | Virtual Local Area Network, віртуальна локальна комп'ютерна мережа                                               |
| WLAN   | – | Wireless Local Area Network, бездротова локальна комп'ютерна мережа                                              |
| WLC    | – | Wireless LAN Controller, контролер бездротової мережі                                                            |
| WPA2   | – | Wi-Fi Protected Access 2, захищений доступ до Wi-Fi версії 2                                                     |

## ВСТУП

Стрімкий розвиток інформаційних технологій та глобальна цифровізація бізнес-процесів висувають нові, жорсткіші вимоги до побудови корпоративних мереж зв'язку. Сучасне підприємство не може ефективно функціонувати без надійної, швидкодіючої та безпечної інформаційно-обчислювальної інфраструктури. Зі збільшенням кількості підключених пристроїв, впровадженням хмарних сервісів та концепції BYOD, традиційні підходи до проектування локальних обчислювальних мереж виявляються недостатньо гнучкими та вразливими до сучасних кіберзагроз.

Більшість існуючих корпоративних мереж середнього масштабу історично будувалися за «плоскою» топологією, де всі вузли знаходяться в одному широкомовному домені, а бездротовий доступ забезпечується автономними точками доступу. Такий підхід призводить до надмірного завантаження каналів зв'язку широкомовним трафіком, ускладнює адміністрування та унеможливорює створення єдиної політики безпеки. Окрім того, децентралізовані точки доступу не здатні забезпечити безшовний роумінг для мобільних клієнтів, що критично впливає на якість зв'язку під час переміщення працівників території підприємства.

Вирішення зазначених проблем вимагає переходу до сучасних архітектурних рішень. Розділення мережі на віртуальні локальні мережі за функціональними напрямками дозволяє ізолювати трафік, мінімізувати ризики несанкціонованого доступу та оптимізувати навантаження на комутаційне обладнання. Водночас, використання централізованої архітектури WLAN на базі апаратного контролера бездротового зв'язку та технології інкапсуляції CAPWAP є найбільш актуальним стандартом для побудови масштабованих бездротових мереж. Застосування протоколу 802.1X у зв'язці з RADIUS-сервером дозволяє відмовитися від ненадійних спільних паролів та перейти до персоналізованої автентифікації корпоративного рівня. Тому розробка відмовостійкої

інфраструктури з інтеграцією Ethernet-технологій та централізованого бездротового керування спрямована на комплексне підвищення надійності, продуктивності та безпеки корпоративного середовища.

Для досягнення поставленої інженерної мети у межах дослідження послідовно вирішується низка науково-технічних завдань. Спочатку здійснюється детальний аналіз предметної області, структури типового підприємства та існуючих проблем маршрутизації інформаційних потоків, що дозволяє обґрунтувати вибір оптимального технологічного стеку, мережевого обладнання та протоколів. На наступному етапі проєктується логічна та фізична топологія мережі за дворівневою ієрархічною моделлю з впровадженням технології віртуальних мереж та міждоменої маршрутизації. Особлива увага приділяється розробці архітектури централізованого бездротового покриття на базі контролера та полегшених точок доступу, а також побудові підсистеми безпеки з реалізацією стандарту WPA2-Enterprise та інтеграцією централізованого сервера автентифікації. Завершальним етапом роботи є безпосередня конфігурація обладнання та верифікація розроблених рішень за допомогою імітаційного моделювання у середовищі Cisco Packet Tracer.

Запропоновані в роботі архітектурні рішення, конфігураційні алгоритми та схеми розподілу сегментів становлять готовий інженерний проєкт. Результати дослідження мають суттєве практичне значення, оскільки можуть бути безпосередньо використані підприємствами для модернізації власних ІТ-інфраструктур. Це дозволить суттєво знизити операційні витрати, спростити подальше масштабування мережі та надійно захистити корпоративні дані від внутрішніх і зовнішніх загроз.

## **1 АНАЛІЗ ТЕХНІЧНОГО ЗАВДАННЯ**

### **1.1 Структура підприємства з урахуванням наявних апаратних і мережних пристроїв**

Проектування сучасної мережевої інфраструктури вимагає детального вивчення фізичної та функціональної структури об'єкта автоматизації. Досліджуване підприємство є типовим сучасним комплексом, що складається з кількох територіально розподілених підрозділів, кожен з яких виконує специфічні завдання та має власні вимоги до обміну даними. Фізично інфраструктура розгорнута в межах чотирьох окремих будівель, які необхідно об'єднати в єдиний інформаційний простір: адміністративний корпус, будівля логістики, науково-дослідна лабораторія та виробничий цех.

Центральним вузлом усієї системи є комутаційне ядро, яке забезпечує високу швидкість передачі даних та стійкість до відмов всієї системи. Воно реалізоване на базі двох взаємопов'язаних високопродуктивних комутаторів третього рівня, які дублюють функції один одного. Така архітектура дозволяє уникнути появи єдиної точки відмови: у разі виходу з ладу одного з магістральних пристроїв або пошкодження лінії зв'язку, трафік автоматично перенаправляється через резервний шлях, що гарантує безперервність бізнес-процесів підприємства.

Адміністративний корпус є серцем управління як бізнесом, так і самою комп'ютерною мережею. Тут встановлено комутатор доступу, до якого підключаються стаціонарні персональні комп'ютери співробітників адміністрації, бухгалтерів та керівництва. Окрім робочих станцій, у цьому сегменті зосереджено головне інфраструктурне обладнання компанії. Зокрема, тут функціонує корпоративний сервер, який суміщає обов'язки динамічного налаштування вузлів та централізованої автентифікації користувачів. Також в адміністративній будівлі розміщено апаратний контролер бездротової мережі, який здійснює централізоване керування всіма радіокомпонентами установи.

Будівля логістики забезпечує процеси обліку, приймання та відвантаження продукції. Логістичний підрозділ оснащений власним комутатором доступу, що обслуговує автоматизовані робочі місця операторів та персоналу складу. Для забезпечення мобільності працівників, які використовують бездротові термінали збору даних та смартфони під час переміщення складом, всередині будівлі встановлено полегшену точку доступу, яка знаходиться під безпосереднім управлінням центрального контролера.

Науково-дослідна лабораторія потребує надійної ізоляції свого трафіку через високу конфіденційність розробок та проведення специфічних вимірювань. Локальний комутатор лабораторії об'єднує в мережу спеціалізовані обчислювальні станції та лабораторні комп'ютери. Покриття бездротовим зв'язком у цій зоні забезпечується окремою полегшеною точкою доступу, що дозволяє співробітникам лабораторії безпечно використовувати портативну техніку.

Виробничий цех характеризується найважчими умовами експлуатації мережевого обладнання та високою щільністю клієнтських пристроїв. Комутатор виробничого сегмента з'єднує робочі станції на лініях виготовлення продукції, промислові контролери, а також забезпечує роботу місцевої точки доступу. Бездротовим зв'язком у цьому секторі активно користуються майстри змін та інженери за допомогою корпоративних ноутбуків і смартфонів для оперативного контролю за виробничими циклами.

Таким чином, апаратна структура підприємства побудована за чітким територіально-функціональним принципом. Кожен підрозділ має власний рівень доступу до мережі, але всі вони замикаються на єдине відмовостійке комутаційне ядро. Загальну концептуальну схему розподілу інфраструктурних вимог та зв'язків між функціональними блоками промислового кампусу наведено на рисунку 1.1.

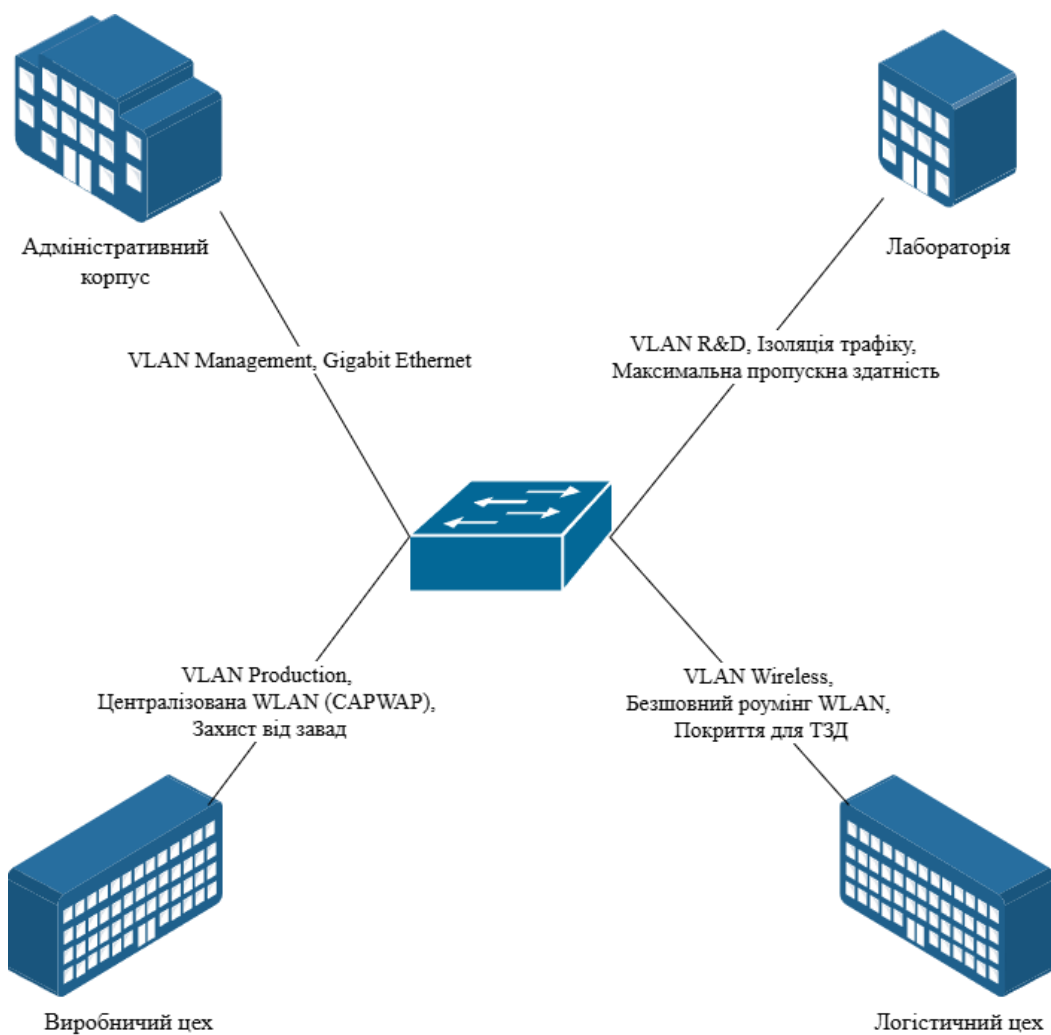


Рисунок 1.1 – Концептуальна схема розподілу інфраструктурних вимог

Як видно з наведеної схеми, територіальна розгалуженість об'єкта та специфічні вимоги кожного підрозділу створюють передумови для впровадження гнучких політик маршрутизації. Це вимагає ретельного підходу до вибору мережевих технологій та протоколів на наступних етапах проєктування інфраструктури.

## 1.2 Аналіз інформаційних потоків і особливостей функціонування мережі

Для забезпечення ефективної роботи підприємства необхідно чітко розуміти характер та обсяги даних, що циркулюють між різними підрозділами. Історично мережа підприємства функціонувала як єдиний широкомовний домен, що призводило до неконтрольованого поширення broadcast-запитів. Це створювало так звані широкомовні шторми, які знижували загальну пропускну здатність каналів зв'язку та викликали затримки у передачі критично важливої інформації.

Інформаційні потоки підприємства можна розділити на кілька ключових категорій відповідно до функціональних зон.

Адміністративний потік: включає обмін документами, роботу з корпоративними БД, ERP-системами та інтернет-трафік. Цей сегмент генерує найбільш інтенсивний, але передбачуваний трафік. Окремо виділяється службовий трафік управління інфраструктурою, який включає запити до DHCP-сервера, обмін ключами шифрування з RADIUS-сервером та керуючі пакети протоколу CAPWAP між WLC та LAP.

Логістичний потік: характеризується високою часткою бездротового трафіку від мобільних терміналів збору даних, що працюють на складі. Дані передаються невеликими пакетами, але вимагають мінімальної затримки для забезпечення роботи систем складського обліку в режимі реального часу.

Лабораторний потік: відрізняється високими вимогами до конфіденційності. Трафік містить результати досліджень та показники з вимірювальних приладів. Цей потік має бути повністю ізольований від інших сегментів мережі задля уникнення витоку даних.

Виробничий потік: складається з телеметричних даних від промислового обладнання та комунікації інженерного персоналу. Характеризується критичністю до втрати пакетів.

Усі внутрішні та зовнішні інформаційні потоки підприємства було

розподілено за територіально-функціональними зонами, детальні інженерні характеристики яких зведено в таблиці 1.1.

Таблиця 1.1 - Характеристика інформаційних потоків підприємства

| Функціональний підрозділ | Основний тип трафіку та сервіси                                    | Інтенсивність трафіку | Вимоги до пропускної здатності | Критерій критичності до затримок | Необхідний рівень безпеки даних |
|--------------------------|--------------------------------------------------------------------|-----------------------|--------------------------------|----------------------------------|---------------------------------|
| Адміністрація            | Документообіг, бази даних, веб-сервіси, електронна пошта           | Середня               | Середня                        | Низький                          | Підвищений                      |
| Логістика                | Бездротовий трафік терміналів обліку, складські програми           | Низька                | Низька                         | Високий                          | Базовий                         |
| Наукова лабораторія      | Результати досліджень, телеметрія вимірювальних приладів           | Середня               | Середня                        | Середній                         | Критичний                       |
| Виробничий цех           | Керуючі сигнали промислових систем, інженерні ноутбуки             | Висока                | Висока                         | Критичний                        | Підвищений                      |
| Службове управління      | Запити адресації, службовий трафік точок доступу та автентифікації | Низька                | Низька                         | Високий                          | Критичний                       |

Аналіз даних, наведених у таблиці 1.1, дозволяє зробити висновок про високу різноманітність корпоративного трафіку підприємства та суттєву відмінність у вимогах до його обслуговування та захисту. Наявність підрозділів із критичним рівнем безпеки, таких як науково-дослідна лабораторія та специфічного інфраструктурного трафіку службового управління повністю виключає можливість використання застарілої «плоскої» топології, де всі

пристрої знаходяться в одному загальному просторі. Окрім того, висока чутливість до затримок у виробничому та логістичному секторах вимагає чіткої ізоляції їхніх інформаційних потоків задля уникнення взаємного впливу та поширення широкомовного шторму. Таким чином, результати аналізу інформаційних потоків безпосередньо обґрунтовують технічну необхідність впровадження технології віртуальних локальних мереж для сегментації ефіру та побудови централізованої бездротової архітектури для контролю мобільних користувачів.

### **1.3 Постановка завдань, пов'язаних з розробкою та шляхи їх вирішення**

На основі проведеного аналізу структури підприємства та характеристик внутрішніх інформаційних потоків було виявлено низку критичних недоліків існуючої мережевої інфраструктури. Головними проблемами є використання застарілої «плоскої» топології без сегментації широкомовних доменів, відсутність апаратного резервування на рівні ядра, а також використання децентралізованих точок доступу з базовим рівнем шифрування. Це не лише знижує загальну пропускну здатність каналів зв'язку через широкомовні шторми, але й створює серйозні загрози інформаційній безпеці компанії.

Для усунення виявлених недоліків та побудови сучасної, захищеної і масштабованої інфраструктури було сформульовано перелік інженерних завдань. Основні проблеми існуючої мережі та пропоновані апаратно-програмні шляхи їх вирішення зведено у таблиці 1.2.

Таблиця 1.2 - Виявлені проблеми мережі та шляхи їх вирішення

| Виявлена проблема інфраструктури                                                      | Поставлене інженерне завдання                                            | Запропоноване технічне рішення                                                                        |
|---------------------------------------------------------------------------------------|--------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|
| Наявність єдиної точки відмови центрального комутаційного вузла                       | Забезпечення апаратного резервування та високої доступності мережі       | Перехід до дворівневої ієрархічної моделі з використанням двох дублюючих комутаторів ядра             |
| Зниження продуктивності через ширококомвні шторми та відсутність ізоляції підрозділів | Логічна сегментація мережі за функціональним призначенням                | Впровадження технології VLAN із виділенням окремих підмереж для кожного відділу та службового трафіку |
| Відсутність зв'язку між ізольованими підрозділами та ручне налаштування IP-адрес      | Організація маршрутизації між сегментами та автоматизація адресації      | Налаштування SVI на комутаторах ядра та розгортання пулів DHCP для кожного VLAN                       |
| Розриви зв'язку мобільних клієнтів при переміщенні, складність управління радіоефіром | Створення єдиного бездротового простору з підтримкою безшовного роумінгу | Впровадження централізованої архітектури WLAN на базі WLC, LAP та протоколу CAPWAP                    |
| Використання вразливих статичних ключів для доступу до корпоративного Wi-Fi           | Підвищення рівня безпеки та персоналізація доступу до мережі             | Інтеграція стандарту IEEE 802.1X (WPA2-Enterprise) з автентифікацією через RADIUS-сервер              |

Як видно з таблиці 1.2, вирішення поставлених завдань вимагає комплексного підходу до модернізації IT-інфраструктури підприємства. Запропоновані технічні шляхи розв'язання базуються на перевірених індустріальних стандартах та рекомендаціях щодо побудови корпоративних мереж. Реалізація цих рішень дозволить не лише усунути поточні вузькі місця у передачі даних, але й закладе міцний фундамент для подальшого масштабування бізнесу без необхідності кардинальної перебудови топології.

Практичне втілення обраних шляхів вирішення, починаючи від вибору конкретних моделей обладнання і закінчуючи розробкою структурної схеми підключення, буде детально розглянуто на етапі фізичної реалізації мережі.

## 2 ФІЗИЧНА РЕАЛІЗАЦІЯ МЕРЕЖІ

### 2.1 Вибір LAN технологій для ліній зв'язку між сегментами підприємства

Побудова надійної та високопродуктивної фізичної інфраструктури корпоративної мережі є фундаментом для забезпечення безперебійного обміну інформацією між територіально розподіленими підрозділами підприємства. Під час проектування кабельної системи промислового кампусу необхідно враховувати довжину магістральних трас, вимоги до пропускної здатності каналів зв'язку, а також стійкість середовища передачі даних до зовнішніх електромагнітних завад, що виникають в умовах сучасного виробництва. Усі основні інженерні параметри та характеристики обраних фізичних середовищ передачі даних для різних ділянок інфраструктури зведено в таблиці 2.1.

Таблиця 2.1 - Технічні характеристики фізичних середовищ передачі даних

| Тип лінії зв'язку                   | Технологія Ethernet | Тип кабелю                   | Максимальна швидкість | Максимальна відстань | Перевага застосування                                           |
|-------------------------------------|---------------------|------------------------------|-----------------------|----------------------|-----------------------------------------------------------------|
| Магістральні канали ядра            | 10GBASE-LX          | Оптичне одномодове волокно   | 10 Гбіт/с             | до 10 км             | Гальванічна ізоляція та абсолютний захист від промислових завад |
| Внутрішня розводка до робочих місць | 1000BASE-T          | Екранована кручена пара Cat6 | 1 Гбіт/с              | до 100 м             | Висока надійність та готовність до подальшого масштабування     |
| Лінії підключення точок доступу     | 1000BASE-T з PoE    | Екранована кручена пара Cat6 | 1 Гбіт/с              | до 100 м             | Дистанційне живлення пристроїв без прокладання силових кабелів  |

Дані, наведені в таблиці 2.1, підтверджують, що обраний комплекс пасивних технологій повністю задовольняє технічні потреби підрозділів щодо швидкодії та надійності зв'язку. Для реалізації провідних ліній зв'язку між

будівлями компанії та всередині робочих зон обрано технології сімейства Ethernet, які регламентуються міжнародними стандартами.

Магістральний рівень мережі, призначений для об'єднання комутаторів доступу окремих будівель із дубльованим комутаційним ядром, реалізується на основі волоконно-оптичних ліній зв'язку (ВОЛЗ). Використання оптичного одномодового волокна (Single Mode Fiber — SMF) для міжбудинкових з'єднань за стандартом IEEE 802.3ae (10GBASE-LX) на довжині хвилі 1310 нм обґрунтовано кількома визначальними інженерними перевагами. По-перше, оптоволоконні кабелі забезпечують повну гальванічну ізоляцію між будівлями, що повністю виключає ризик пошкодження портів активного мережевого обладнання внаслідок виникнення різниці потенціалів систем заземлення різних корпусів або під час грозових розрядів. По-друге, таке діелектричне середовище має абсолютну імунітетність до промислових електромагнітних завад (EMI), що дозволяє прокладати магістральні волоконно-оптичні кабелі у спільних кабельних шахтах та естакадах поруч із силовими кабельними трасами високої напруги без загрози спотворення, згасання чи перехоплення сигналів. Для магістральних каналів ядра проєктується використання стандартів Gigabit Ethernet та 10G Ethernet, що повністю задовольняє поточні вимоги підприємства щодо швидкодії бізнес-процесів та забезпечує високий потенціал для подальшого масштабування інфраструктури при нарощуванні трафіку.

Внутрішня кабельна розводка в межах кожної окремої будівлі від поверхових або центральних розподільчих шаф до кінцевих пристроїв користувачів проєктується на базі мідної крученої пари. Для забезпечення стабільних гігабітних швидкостей передачі даних за стандартом IEEE 802.3ab (1000BASE-T) та мінімізації впливу перехресних наведень усередині монтажних кабельних лотків обрано екрановану кручену пару структури F/UTP категорії Cat6 із частотною смугою пропускання до 250 МГц. Цей тип кабелю підтримує надійну роботу гігабітних технологій на відстанях до 100 метрів (із врахуванням довжини патч-кордів), що повністю покриває архітектурні та планувальні потреби адміністративного корпусу, логістичного складу, наукової лабораторії та

виробничого цеху. Окрім того, використання крученої пари категорії Cat6 є важливим фактором масштабованості: фізичні характеристики кабелю дозволяють за потреби плавно переходити на вищі швидкості до 2.5 Гбіт/с та 5 Гбіт/с (стандарти NBASE-T / IEEE 802.3bz) на рівні доступу без необхідності демонтажу та заміни поточної пасивної кабельної інфраструктури, що значно знижує майбутні експлуатаційні витрати (OPEX).

Окрему увагу при виборі фізичних технологій приділено бездротовому сегменту мережі, який інтегрується у загальну кабельну систему кампусу. Для підключення легковагових точок доступу (LAP) до периферійних комутаторів доступу також застосовується 4-парна кручена пара категорії Cat6 з обов'язковою підтримкою технології дистанційного живлення по мережевому кабелю за стандартом IEEE 802.3at (PoE+). Це дозволяє подавати на кожну точку доступу постійне живлення потужністю до 30 Вт по тих самих сигнальних жилах, що використовуються для передачі даних. Інженерне рішення впровадження PoE+ дозволяє повністю відмовитися від проектування та прокладання окремих силових ліній електроживлення 220 В до місць фізичного монтажу антен під стелею або на колонах промислових та складських приміщень. Такий підхід суттєво спрощує монтаж обладнання, знижує капітальні витрати на силову кабельну продукцію та підвищує загальну пожежну безпеку об'єкта автоматизації за рахунок виключення високої напруги у зонах високої щільності обладнання.

Таким чином, комбінація високошвидкісних волоконно-оптичних магістралей між корпусами підприємства та захищеної від завад мідної інфраструктури всередині приміщень дозволяє створити збалансоване, стійке до зовнішніх факторів та відмовостійке фізичне середовище передачі даних. Такий підхід гарантує стабільну взаємодію всіх підрозділів компанії та створює надійну матеріальну базу для розгортання активного комутаційного обладнання вищих рівнів.

## 2.2 Вибір мережних пристроїв з визначенням технічних характеристик для кожного конкретного пристрою або групи ідентичних пристроїв, опис їх призначення та особливості застосування

Ефективність функціонування логічної структури корпоративної мережі безпосередньо залежить від правильно підбраного активного мережевого обладнання. Вибір пристроїв здійснюється відповідно до вимог дворівневої ієрархічної моделі, яка передбачає чіткий розподіл функцій між магістральним ядром та рівнем доступу. Для забезпечення високої продуктивності, керованості та сумісності всіх компонентів інфраструктури, проєктне рішення базується на апаратному забезпеченні компанії Cisco, яке є індустріальним стандартом у сфері побудови кампусних мереж. Технічні параметри та функціональні можливості обраних мережевих пристроїв зведено в таблиці 2.2.

Таблиця 2.2 – Технічні характеристики активного мережевого обладнання

| Тип пристрою                  | Модель обладнання        | Рівень моделі OSI | Кількість та тип портів                                | Пропускна здатність матриці | Функціональне призначення в мережі                                                           |
|-------------------------------|--------------------------|-------------------|--------------------------------------------------------|-----------------------------|----------------------------------------------------------------------------------------------|
| Багаторівневий комутатор ядра | Cisco Catalyst 3560-24PS | Другий та Третій  | 24 порти Fast Ethernet з PoE, 2 порти Gigabit Ethernet | 32 Гбіт/с                   | Апаратна маршрутизація між віртуальними інтерфейсами, агрегація магістральних каналів        |
| Комутатор рівня доступу       | Cisco Catalyst 2960-24TT | Другий            | 24 порти Fast Ethernet, 2 порти Gigabit Ethernet       | 16 Гбіт/с                   | Підключення кінцевих робочих станцій, серверів та точок доступу, маркування трафіку          |
| Контролер бездротової мережі  | Cisco WLC 3504           | Другий та Третій  | 4 порти Gigabit Ethernet, 1 порт Multigigabit Ethernet | 4 Гбіт/с                    | Централізоване управління радіоефіром, координація безшовного роумінгу, інкапсуляція тунелів |

Аналіз технічних даних, наведених у таблиці 2.2, дозволяє зробити висновок про повну відповідність обраної апаратної бази вимогам проєкту щодо швидкодії, масштабованості та надійності інформаційних потоків підприємства. Завдяки високій пропускну здатності внутрішньої матриці комутації пристроїв ядра, повністю нівелюється загроза утворення затримок при передачі великих масивів даних між різними сегментами мережі.

Фізична топологія та схема комутації портів спроектовані за принципом архітектурної достатності та високої економічної ефективності. Оскільки основний обсяг корпоративного трафіку на периферійних ділянках промислового кампусу складається з телеметрії промислових систем, транзакцій систем складського обліку та текстового документообігу, що мають низьку інтенсивність, використання інтерфейсів Fast Ethernet, швидкість до 100 Мбіт/с, для міжкомутаторних зв'язків є технічно повністю обґрунтованим і достатнім. Це дозволяє уникнути надлишкових витрат на дорогі гігабітні модулі розширення, зберігаючи при цьому стабільні показники передачі даних.

Для реалізації згорнутого ядра мережі (Collapsed Core) в центральній серверній шафі кампусу використовуються багаторівневі комутатори третього рівня серії Cisco Catalyst 3560-24PS. Вибір цієї моделі обґрунтований інженерними критеріями та відповідністю міжнародним стандартам. Комутатор поєднує функції другого та третього рівнів моделі OSI. Це дозволяє йому виступати безпосереднім основним шлюзом для всіх налаштованих підмереж підприємства. Маршрутизація між VLAN здійснюється на базі апаратної технології Cisco Express Forwarding, що зводить затримки комутації до мікросекундного рівня і повністю виключає потребу у використанні зовнішнього маршрутизатора. Наявність гігабітних портів на пристроях ядра дозволяє об'єднати інтерфейси GigabitEthernet0/1 та GigabitEthernet0/2 комутаторів Core-1 та Core-2 у логічний пучок EtherChannel. Це гарантує максимальну відмовостійкість центрального вузла: у разі аварії на одній з гігабітних ліній, трафік миттєво перенаправляється через іншу без простоїв мережі. Наявність вбудованої підтримки PoE на портах Fast Ethernet комутаторів ядра дозволяє

забезпечити безпосереднє дистанційне живлення інфраструктурних пристроїв (серверів, контролера) безпосередньо з серверної стійки.

Периферійний рівень доступу (Access Layer) у будівлях кампусу формується на базі комутаторів другого рівня Cisco Catalyst 2960-24TT. Комутатори забезпечують надійну ізоляцію широкомовних доменів на рівні окремих підрозділів підприємства. Користувацькі інтерфейси жорстко переведені в режим access, а для передачі тегового трафіку між комутаторами доступу та ядром використовуються магістральні порти у режимі trunk з підтримкою стандарту інкапсуляції dot1q. Для запобігання утворенню петель комутації на другому рівні моделі OSI в умовах подвійного підключення до резервованого ядра, на пристроях активовано протокол Rapid Spanning Tree. Це гарантує перерахунок топології мережі за час менше двох секунд у разі аварійних ситуацій. Пристрої підтримують механізми Port Security для фільтрації клієнтів за MAC-адресами, а також технологію DHCP Snooping, що виключає можливість підключення стороннього несанкціонованого обладнання до портів доступу у виробничих приміщеннях.

Центральним інтелектуальним вузлом бездротового сегмента є апаратний контролер локальної мережі Cisco WLC 3504. Контролер виступає єдиною точкою термінації для тунелів від полегшених точок доступу (LAP). Весь бездротовий трафік користувачів інкапсулюється в CAPWAP і передається безпосередньо в комутаційне ядро, де автоматично спрямовується у виділену бездротову підмережу VLAN 50. Контролер координує процеси безпеки за стандартом WPA2-Enterprise, взаємодіючи з RADIUS-сервером підприємства. Це дозволяє уникнути вразливого статичного шифрування та забезпечує індивідуальну перевірку кожного мобільного клієнта. Модель WLC 3504 підтримує керування великою кількістю точок доступу, що дозволяє вільно нарощувати кількість бездротових вишок у цехах та на складах у разі розширення бізнесу без заміни центрального апаратного вузла.

### 2.3 Вибір кінцевих пристроїв. Опис технічних характеристик для кожного пристрою або групи пристроїв та особливості застосування

Кінцеві пристрої є безпосередніми джерелами та споживачами корпоративного трафіку в інформаційній системі підприємства. Під час проектування робочих місць та серверного сегмента необхідно враховувати специфіку функціональних обов'язків персоналу кожної будівлі, вимоги прикладного програмного забезпечення до продуктивності, а також типи підтримуваних мережевих інтерфейсів. Особлива увага приділяється здатності кінцевого обладнання підтримувати сучасні стандарти безпеки, зокрема механізми взаємодії з точками доступу та серверами автентифікації на базі захищених корпоративних протоколів.

Узагальнені інженерні параметри та особливості мережевої взаємодії для кожної групи пристроїв наведено в таблиці 2.3.

Таблиця 2.3 – Технічні характеристики та особливості застосування кінцевих пристроїв

| Категорія пристроїв                       | Моделльний тип у симуляторі | Мережевий інтерфейс             | Тип отримання адреси | Роль та особливості застосування в інфраструктурі                                                |
|-------------------------------------------|-----------------------------|---------------------------------|----------------------|--------------------------------------------------------------------------------------------------|
| Багатофункціональний корпоративний сервер | Server-PT                   | Fast Ethernet, Gigabit Ethernet | Статичний            | Розгортання служб динамічного налаштування вузлів та централізованої автентифікації користувачів |
| Стаціонарні робочі станції                | PC-PT                       | Fast Ethernet                   | Динамічний           | Забезпечення повсякденної діяльності персоналу адміністрації, лабораторії та виробництва         |
| Мобільні клієнти та термінали             | Laptop-PT, Smartphone-PT    | Wireless 802.11a/b/g/n          | Динамічний           | Оперативний збір даних, мобільні робочі місця з підтримкою безшовного роумінгу                   |

Систематизовані в таблиці 2.3 дані показують, що кінцеві пристрої мають різні типи фізичних підключень, середовища передачі даних та механізми первинної конфігурації, що вимагає гнучкого налаштування портів комутаторів периферійного рівня доступу. Використання автоматизованого динамічного розподілу адрес для більшості кінцевих користувачів дозволяє оптимізувати утилізацію наявного адресного простору, мінімізувати трудовитрати на адміністрування та виключити людський фактор. Водночас жорстка статична адресація сервера гарантує постійну доступність критично важливих мережевих служб для всієї інфраструктури компанії.

Центральне місце у групі кінцевих пристроїв займає багатофункціональний корпоративний сервер, розміщений в адміністративному корпусі кампусу. Його апаратна частина орієнтована на забезпечення безперебійної цілодобової роботи в режимі високого навантаження. Особливістю інженерного застосування цього сервера є паралельне виконання двох найважливіших інфраструктурних завдань на системному рівні.

Перше завдання — автоматизація розподілу мережевих параметрів (IP-адреса, Subnet Mask, Default Gateway, DNS-server) для всіх п'яти віртуальних локальних мереж, що реалізується за допомогою конфігурування ізольованих пулів адрес у межах служби DHCP (Dynamic Host Configuration Protocol). Сервер взаємодіє з агентами ретрансляції DHCP Relay (команда `ip helper-address`), налаштованими на комутованих віртуальних інтерфейсах шлюзів згорнутого ядра.

Друге завдання — забезпечення інформаційної безпеки шляхом перевірки облікових даних дротових та бездротових клієнтів за протоколом корпоративного рівня через службу віддаленої автентифікації RADIUS (Remote Authentication in Dial-In User Service), що функціонує в межах загальної архітектури AAA. Сервер обробляє запити Access-Request, перевіряє відповідність хешів паролів у базі даних користувачів та повертає керуючі пакети Access-Accept або Access-Reject на бездротовий контролер.

Стаціонарні персональні комп'ютери (робочі станції) розгорнуті в усіх чотирьох функціональних зонах підприємства для забезпечення операційної діяльності персоналу. Їх підключення здійснюється виключно за допомогою мідного екранованого кабелю крученої пари категорії Cat6 до найближчого периферійного комутатора доступу Catalyst 2960. Вбудовані мережеві плати (NIC) комп'ютерів налаштовані на роботу в режимі автоматичного визначення швидкості та дуплексу (Auto-Negotiation), з базовим пріоритетом функціонування у режимі Full-Duplex на швидкості 100 Мбіт/с, що спрощує їх інтеграцію та виключає утворення колізій у середовищі передачі.

Особливістю функціонування цих пристроїв є те, що вони логічно та фізично прив'язані до конкретних інтерфейсів комутаторів доступу, які заздалегідь переведені в режим switchport mode access із чітким закріпленням за відповідним ідентифікатором віртуальної мережі відділу VLAN 10, 20, 30 або 40. Це обмежує їхній широкомовний трафік і захищає від міжсегментного несанкціонованого перехоплення пакетів.

Група мобільних бездротових клієнтів, що включає корпоративні ноутбуки, смартфони та портативні термінали збору даних (ТСД), забезпечує високу гнучкість бізнес-процесів у будівлях логістики, наукової лабораторії та виробничого цеху. Ці пристрої оснащені універсальними бездротовими адаптерами з підтримкою стандартів радіозв'язку IEEE 802.11a/b/g/n. Головною особливістю їхнього інженерного застосування є здатність динамічно змінювати точку приєднання до мережі (асоціацію з антеною) під час переміщення працівника територією промислового кампусу.

При цьому операційні системи мобільних девайсів підтримують повну інтеграцію зі службою автентифікації 802.1X за захищеними протоколами EAP-PEAP (Protected Extensible Authentication Protocol) або EAP-MSCHAPv2. Це дозволяє мобільним користувачам один раз ввести свої унікальні персональні облікові дані при первинній сесії, після чого контролер WLC спільно з точками LAR реалізує для них безшовний роумінг (Fast Roaming) без повторного запиту пароля та без зміни отриманої IP-адреси з пулу бездротової мережі VLAN 50.

## 2.4 Розробка функціональної схеми

Функціональна схема корпоративної мережі є базовим графічним інженерним документом, який відображає логіку взаємодії компонентів системи, апаратний склад основного активного обладнання, а також топологію зв'язків між її вузлами. Розробка функціональної схеми здійснювалася на основі оптимізації класичної тривірневої ієрархічної моделі Cisco, що дозволило закласти в проект високі показники масштабованості, централізованої керованості та стійкості інфраструктури до відмов (Fault Tolerance) на апаратному рівні. Оскільки мережева інфраструктура підприємства обслуговує чотири окремі територіально розподілені будівлі (Адміністрація, Логістика, Лабораторія, Виробництво) з різними специфікаціями та інтенсивністю обміну даними, як архітектурний базис було обрано дворівневу модель згорнутого ядра (Collapsed Core). Ця архітектура передбачає суміщення функцій магістрального рівня (Core Layer) та рівня розподілу (Distribution Layer) на єдиній стійкій апаратній платформі. Таке рішення є найбільш технічно обґрунтованим для промислових кампусних мереж середнього масштабу, оскільки суттєво спрощує маршрутизаційну матрицю, мінімізує затримки при міжсегментному пересиланні пакетів та оптимізує витрати на закупівлю заліза. Центральним елементом розробленої функціональної схеми є відмовостійкий комутаційний комплекс, що складається з двох високопродуктивних багаторівневих комутаторів L3 серії Cisco Catalyst 3560-24PS (позначені як Core-1 та Core-2). Для забезпечення внутрішньої зв'язності та синхронізації таблиць маршрутизації комутатори ядра об'єднані між собою високошвидкісним транковим каналом EtherChannel за стандартом IEEE 802.3ad (LACP) і працюють у режимі взаємного гарячого резервування.

Периферійні комутатори рівня доступу Cisco Catalyst 2960-24TT, розташовані в кожному з корпусів кампусу, підключаються до комутаційного ядра за відмовостійкою топологією «подвійна зірка» (Dual-Homing). Це означає,

що кожен комутатор доступу має два незалежних фізичних підключення Fast Ethernet: одне до комутатора Core-1, інше — до Core-2.

Така надлишкова топологія у поєднанні з активованим протоколом IEEE 802.1w (RSTP) гарантує, що у разі виходу з ладу одного з магістральних L3-комутаторів або фізичного пошкодження основної лінії зв'язку, мережевий трафік усього підрозділу буде автоматично і непомітно для користувачів перенаправлено на резервний маршрут за час, що не перевищує 2 секунди. Використання ліній Fast Ethernet для підключення периферійних комутаторів доступу є повністю достатнім, оскільки розрахована щільність трафіку промислових контролерів, ТСД та робочих станцій не перевищує межі пропускну здатності каналу у 100 Мбіт/с.

До периферійних комутаторів рівня доступу безпосередньо підключаються кінцеві пристрої користувачів відповідних відділів: стаціонарні робочі станції персоналу, промислове автоматизоване обладнання (PLC-контролери) та мережеві принтери. Для розгортання бездротового сегмента мережі до комутаторів рівня доступу також підключаються легковагові точки доступу (LAP).

З метою централізації управління радіоефіром та забезпечення безпеки, апаратний бездротовий контролер Cisco WLC 3504 разом із корпоративним сервером автентифікації RADIUS інтегровані у структуру мережі через комутатор адміністративного сегмента. Таке інженерне рішення дозволяє повністю локалізувати службовий трафік управління (CAPWAP-тунелі, запити 802.1X, DHCP-запити) в єдиному захищеному центрі обробки даних, не створюючи надлишкового навантаження на комутаційні матриці інших виробничих підрозділів кампусу.

Розроблену функціональну схему корпоративної мережі підприємства наведено на рисунку 2.1.

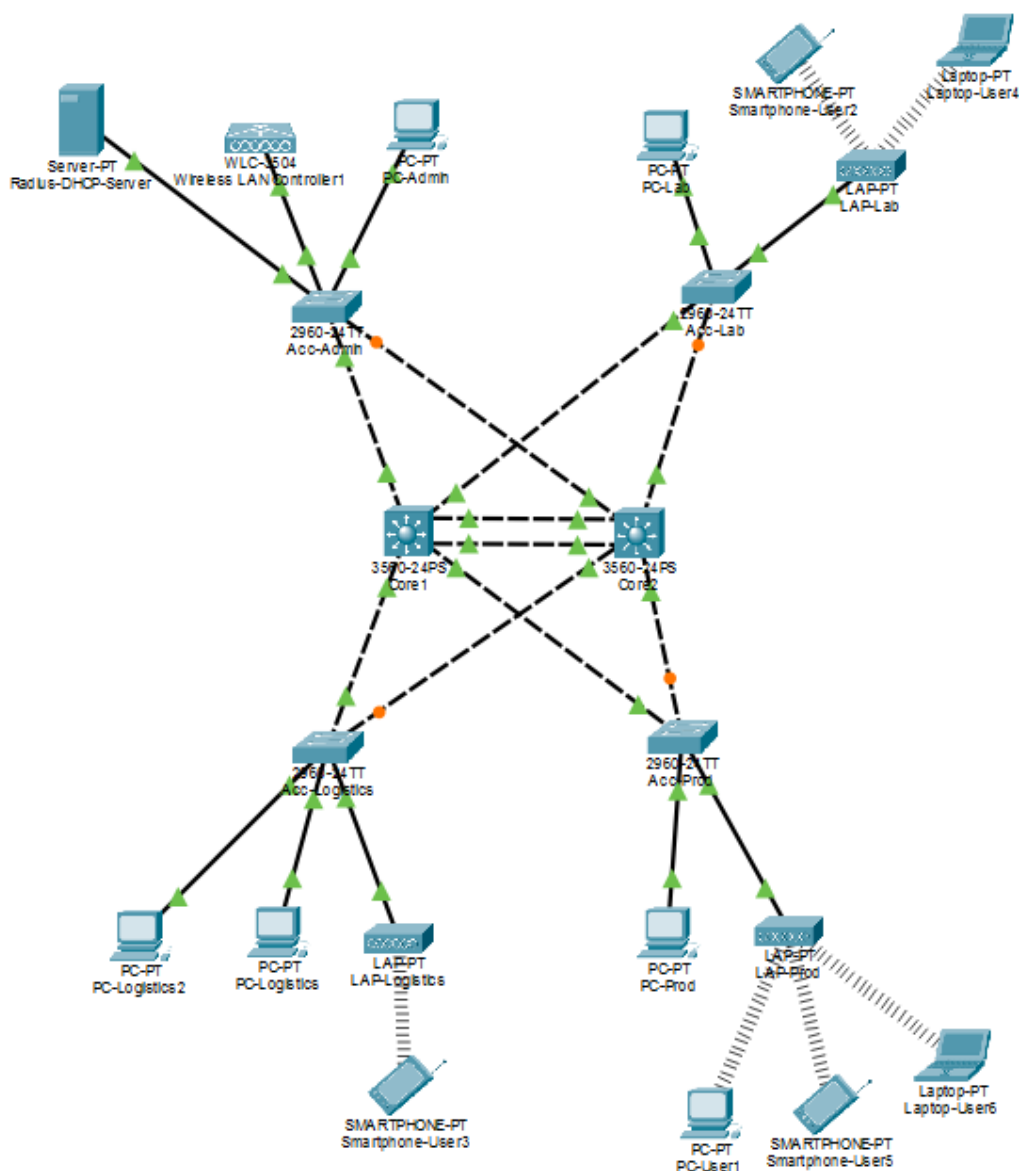


Рисунок 2.1 – Функціональна схема корпоративної мережі

Наведена функціональна схема повністю задовольняє вимоги технічного завдання щодо логічної ізоляції трафіку та апаратної відмовостійкості. Спроектowana фізична топологія усуває єдину точку відмови та слугує надійним фундаментом для подальшого етапу логічного налаштування параметрів маршрутизації, віртуальних мереж та політик безпеки.

## 2.5 Розробка схеми при'єднування мережі

Схема при'єднування мережі визначає точний порядок комутації портів активного мережевого обладнання та організацію ліній зв'язку між різними рівнями ієрархічної моделі. Правильний розподіл портів дозволяє уникнути петель комутації, забезпечити необхідну пропускну здатність транкових каналів та чітко розмежувати трафік різних віртуальних мереж на фізичному рівні.

Для забезпечення прозорості архітектури та систематизації всіх фізичних з'єднань промислового кампусу було розроблено детальну матрицю комутації. Повний перелік підключень між магістральними пристроями ядра, комутаторами доступу будівель та ключовими інфраструктурними вузлами наведено в таблиці 2.4.

Таблиця 2.4 – Схема комутації портів та розподілу інтерфейсів мережі

| Початковий пристрій | Інтерфейс відправника | Цільовий пристрій | Інтерфейс отримувача | Тип налаштування порту та логічний сегмент |
|---------------------|-----------------------|-------------------|----------------------|--------------------------------------------|
| Core-1              | GigabitEthernet 0/1   | Core-2            | GigabitEthernet 0/1  | Магістральний транк, агрегація ядра        |
| Core-1              | FastEthernet 0/1      | Acc-Admin         | FastEthernet 0/1     | Магістральний транк, основний лінк         |
| Core-2              | FastEthernet 0/1      | Acc-Admin         | FastEthernet 0/2     | Магістральний транк, резервний лінк        |
| Core-1              | FastEthernet 0/2      | Acc-Logistics     | FastEthernet 0/1     | Магістральний транк, основний лінк         |
| Core-2              | FastEthernet 0/2      | Acc-Logistics     | FastEthernet 0/2     | Магістральний транк, резервний лінк        |
| Core-1              | FastEthernet 0/3      | Acc-Lab           | FastEthernet 0/1     | Магістральний транк, основний лінк         |
| Core-2              | FastEthernet 0/3      | Acc-Lab           | FastEthernet 0/2     | Магістральний транк, резервний лінк        |
| Core-1              | FastEthernet 0/4      | Acc-Prod          | FastEthernet 0/1     | Магістральний транк, основний лінк         |
| Core-2              | FastEthernet 0/4      | Acc-Prod          | FastEthernet 0/2     | Магістральний транк, резервний лінк        |

Продовження таблиці 2.4

| Початковий пристрій | Інтерфейс відправника  | Цільовий пристрій              | Інтерфейс отримувача | Тип налаштування порту та логічний сегмент |
|---------------------|------------------------|--------------------------------|----------------------|--------------------------------------------|
| Acc-Admin           | FastEthernet 0/3 – 19  | Робочі станції адміністрації   | Ethernet-адаптер     | Порт доступу, віртуальна мережа 10         |
| Acc-Admin           | FastEthernet 0/21      | Контролер бездротової мережі   | GigabitEthernet 0/1  | Порт доступу, віртуальна мережа 50         |
| Acc-Admin           | FastEthernet 0/22      | Сервер автентифікації та адрес | FastEthernet 0/0     | Порт доступу, віртуальна мережа 50         |
| Acc-Logistics       | FastEthernet 0/3 – 19  | Робочі станції логістики       | Ethernet-адаптер     | Порт доступу, віртуальна мережа 20         |
| Acc-Logistics       | FastEthernet 0/20 – 24 | Точки доступу та управління    | Ethernet-адаптер     | Порт доступу, віртуальна мережа 50         |
| Acc-Lab             | FastEthernet 0/3 – 19  | Станції наукової лабораторії   | Ethernet-адаптер     | Порт доступу, віртуальна мережа 30         |
| Acc-Lab             | FastEthernet 0/20 – 24 | Точки доступу та управління    | Ethernet-адаптер     | Порт доступу, віртуальна мережа 50         |
| Acc-Prod            | FastEthernet 0/3 – 19  | Станції виробничого цеху       | Ethernet-адаптер     | Порт доступу, віртуальна мережа 40         |
| Acc-Prod            | FastEthernet 0/20 – 24 | Точки доступу та управління    | Ethernet-адаптер     | Порт доступу, віртуальна мережа 50         |

Наведена у таблиці 2.4 схема при'єднування наочно демонструє реалізацію принципу подвійної зірки для підключення будівель промислового кампусу. Кожен комутатор рівня доступу має два незалежні магістральні підключення, налаштовані за стандартом тегування трафіку, що повністю нівелює загрозу ізоляції будівлі у разі аварії на одній з ліній зв'язку.

На рівні комутаторів доступу застосовується чіткий модульний розподіл портів. Клієнтські робочі місця відокремлені від інфраструктурних пристроїв та бездротових точок доступу. Закріплення інтерфейсів з 20 по 24 за окремим службовим сегментом управління гарантує, що трафік контролера бездротової мережі, сервера автентифікації та полегшених точок доступу ізолюваний від загального користувацького потоку даних, забезпечуючи високу стабільність обміну службовими пакетами.

## 2.6 Монтаж мережі

Фізичний монтаж мережевої інфраструктури відіграє критичну роль у забезпеченні її довговічності, надійності та зручності подальшого обслуговування. Монтажні роботи на підприємстві проєктуються з урахуванням архітектурних особливостей кожної з чотирьох будівель та вимог стандартів щодо побудови структурованих кабельних систем.

Центральне комутаційне обладнання, включаючи магістральні комутатори ядра, апаратний контролер бездротового зв'язку та корпоративний сервер, розміщується в головній телекомунікаційній шафі адміністративного корпусу. Для монтажу обладнання головної будівлі використовується стандартна дев'ятнадцятидюймова серверна шафа закритого типу, оснащена системами активного охолодження та блоками безперебійного живлення. Застосування великої підлогової шафи дозволяє зручно розмістити масивні пристрої ядра, забезпечити належний кабель-менеджмент та захистити критичні вузли від пилу й несанкціонованого доступу. Загальний вигляд конструкції великої телекомунікаційної шафи головного комутаційного вузла наведено на рисунку 2.2.

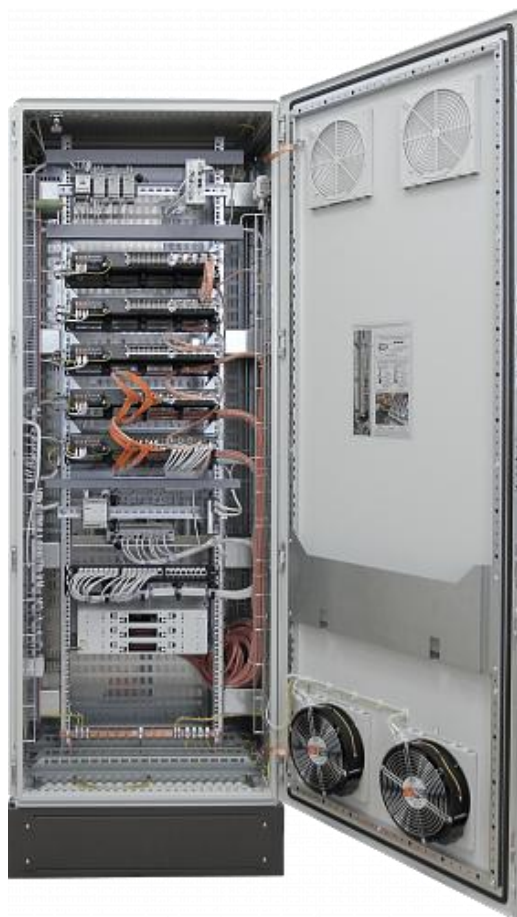


Рисунок 2.2 - Телекомунікаційна шафа

Для будівель логістики, лабораторії та виробничого цеху, де кількість кінцевих пристроїв є меншою, а простір для розміщення обладнання обмежений, проєктується встановлення малих настінних комутаційних боксів. У цих компактних шафах монтуються комутатори доступу та пасивні комутаційні панелі. Підключення горизонтальної кабельної розводки від робочих місць до комутаторів здійснюється виключно через патч-панелі за допомогою заводських комутаційних шнурів, що дозволяє уникнути зношування портів активного обладнання при перемикаваннях. Типове конструктивне виконання настінного комутаційного боксу для проміжних розподільчих вузлів відображено на рисунку 2.3.



Рисунок 2.3 - Настінний комутаційний бокс

Кабельні траси всередині приміщень прокладаються у спеціалізованих пластикових коробах та металевих лотках. Це забезпечує надійний захист екранованої крученої пари від механічних пошкоджень та впливу електромагнітних полів виробничого обладнання. Полегшені точки доступу монтуються на стелях приміщень за допомогою спеціальних кронштейнів, що забезпечує оптимальну зону покриття радіосигналу та унеможливорює несанкціонований фізичний доступ до обладнання.

Обраний підхід до вибору конструкцій телекомунікаційних шаф та боксів повністю задовольняє вимоги щодо раціонального використання простору підприємства. Організація центрального вузла у великій підлоговій шафі забезпечує необхідний тепловий режим для високопродуктивного обладнання ядра, тоді як настінні бокси в цехах та на складах гарантують надійний захист локальних комутаторів доступу за мінімальних просторових витрат.

## **2.7 Обґрунтування масштабованості фізичної та апаратної структури мережі**

Під час проектування корпоративної мережі промислового кампусу одним із ключових критеріїв ефективності інфраструктури є її масштабованість (Scalability) — здатність системи адаптуватися до зростаючих навантажень, збільшення обсягів трафіку та розширення штату співробітників або виробничих потужностей підприємства без необхідності докорінної перебудови наявної архітектури та заміни базового активного обладнання. У розробленому проєктному рішенні високий потенціал масштабованості забезпечується комплексно на чотирьох взаємопов'язаних рівнях.

Перший рівень - Масштабованість пасивної кабельної інфраструктури (СКС). Внутрішня кабельна розводка в усіх чотирьох будівлях кампусу виконується на базі екранованої крученої пари структури F/UTP категорії Cat6. Фізичні та частотні характеристики цього середовища передачі даних (смуга пропускання до 250 МГц) закладають значний технологічний запас. У разі модернізації виробництва або виникнення потреби в обміні мультимедійним трафіком високої чіткості, поточна кабельна система дозволить здійснити плавний перехід із технології 1000BASE-T на вищі швидкості до 2.5 Гбіт/с та 5 Гбіт/с (стандарти NBASE-T / IEEE 802.3bz) або навіть 10 Гбіт/с (10GBASE-T) на відстанях до 55 метрів без необхідності демонтажу та повторного прокладання ліній зв'язку. Магістральні волоконно-оптичні лінії між корпусами (стандарт IEEE 802.3ae) підтримують інтеграцію систем спектрального мультиплексування (WDM/CWDM), що дозволяє збільшувати пропускну здатність ядра в десятки разів по тих самих оптичних жилах.

Другий рівень - Резервування ємності портів активного обладнання. При виборі периферійних комутаторів рівня доступу серії Cisco Catalyst 2960-24TT було враховано коефіцієнт надлишковості на рівні 25–30%. Кількість активних підключень (робочих станцій, промислових контролерів PLC та точок доступу

LAP) у кожному корпусі залишає вільними від 6 до 12 портів Fast Ethernet на кожному пристрої. Це дозволяє оперативно організовувати нові робочі місця або підключати додаткове автоматизоване обладнання методом горизонтального розширення. Наявність двох вільних гігабітних портів Uplink (Gigabit Ethernet) на кожному комутаторі доступу та вільних SFP-слотів на комутаторах згорнутого ядра Cisco Catalyst 3560-24PS забезпечує можливість підключення нових периферійних комутаторів у разі будівництва п'ятого чи шостого корпусів підприємства, при цьому архітектура згорнутого ядра не зазнає структурних змін.

Третій рівень - Масштабованість бездротового сегмента WLAN. Централізована архітектура бездротової мережі на базі полегшених точок доступу (LAP) є максимально гнучкою з точки зору розширення зони покриття. Обраний апаратний контролер бездротової мережі Cisco WLC 3504 має вбудовану ліцензійну та апаратну підтримку керування великою кількістю точок доступу (до 150 одиниць) та обслуговування до 3000 одночасних клієнтських сесій.

Якщо на підприємстві буде розширено площу складських приміщень або змонтовано нові конвеєрні лінії, що вимагатимуть додаткових ТСД-сканерів, процедура масштабування Wi-Fi полягатиме суто у фізичному монтажі нової точки LAP та її підключенні до найближчого комутатора доступу. Завдяки протоколу CAPWAP (RFC 5415), точка доступу автоматично знайде контролер WLC, завантажить із нього єдину корпоративну конфігурацію, політики безпеки WPA2-Enterprise та автоматично включить нових абонентів у виділену бездротову підмережу VLAN 50 без додаткових маніпуляцій з боку адміністратора.

Четвертий рівень - Логічна масштабованість адресного простору. Спроектowana схема IP-адресації на базі приватних мереж класу C (192.168.X.X) та використання масок змінної довжини (VLSM) виконані з урахуванням майбутнього розвитку. Кожен пул адрес, закріплений за певним відділом VLAN 10 — Адміністрація, VLAN 20 — Логістика, VLAN 30 — Лабораторія, VLAN 40 — Виробництво, ємність підмереж задовольняє поточні потреби з двократним запасом (до 62 або 126 хостів на сегмент).

Таким чином, закладені архітектурні та апаратні рішення гарантують тривалий життєвий цикл створеної корпоративної мережі, захищають інвестиції підприємства в IT-інфраструктуру та забезпечують її повну готовність до швидкого горизонтального й вертикального масштабування в умовах розвитку бізнес-процесів.

### **3 ЛОГІЧНА РЕАЛІЗАЦІЯ МЕРЕЖІ**

#### **3.1 Вибір протоколів каналного та мережного рівнів**

Логічна реалізація корпоративної комп'ютерної мережі передбачає визначення оптимального набору мережевих протоколів та стандартів, які забезпечать стабільну, безпечну та керовану взаємодію між усіма апаратними компонентами інфраструктури. Вибір протоколів здійснюється відповідно до семирівневої моделі взаємодії відкритих систем, з особливим фокусом на каналному та мережному рівнях, які безпосередньо відповідають за локальну комутацію, ізоляцію трафіку, усунення топологічних петель та маршрутизацію інформаційних потоків.

На каналному рівні базою для побудови провідної інфраструктури є сімейство стандартів Ethernet. Для забезпечення логічної сегментації єдиного фізичного простору промислового кампусу на ізольовані зони застосовується технологія віртуальних локальних мереж відповідно до стандарту IEEE 802.1Q. Це дозволяє штучно розділити широкомовні домени для адміністрації, логістики, науково-дослідної лабораторії та виробничого цеху, підвищуючи безпеку та знижуючи навантаження на процесори пристроїв. Для запобігання виникненню широкомовних штормів в умовах резервування магістральних каналів зв'язку обов'язковим є використання протоколу RSTP. У бездротовому сегменті взаємодія між полегшеними точками доступу та центральним контролером

базується на спеціалізованому протоколі CAPWAP, який реалізує концепцію розділення функцій обробки даних.

На мережному рівні для забезпечення унікальної адресації всіх вузлів системи використовується стек протоколів IPv4. Автоматизація процесу розподілу мережових налаштувань, таких як маска підмережі, основний шлюз та адреси серверів, покладається на протокол DHCP. Для здійснення діагностики, моніторингу та перевірки зв'язності між пристроями інтегрується протокол ICMP.

Зазначені протоколи обох рівнів не функціонують ізольовано, а утворюють чітку технологічну ієрархію інкапсуляції даних. Загальну логічну схему взаємодії та взаємозв'язку обраних протоколів канального та мережного рівнів у структурі проєктуємої інфраструктури наведено на рисунку 3.1.

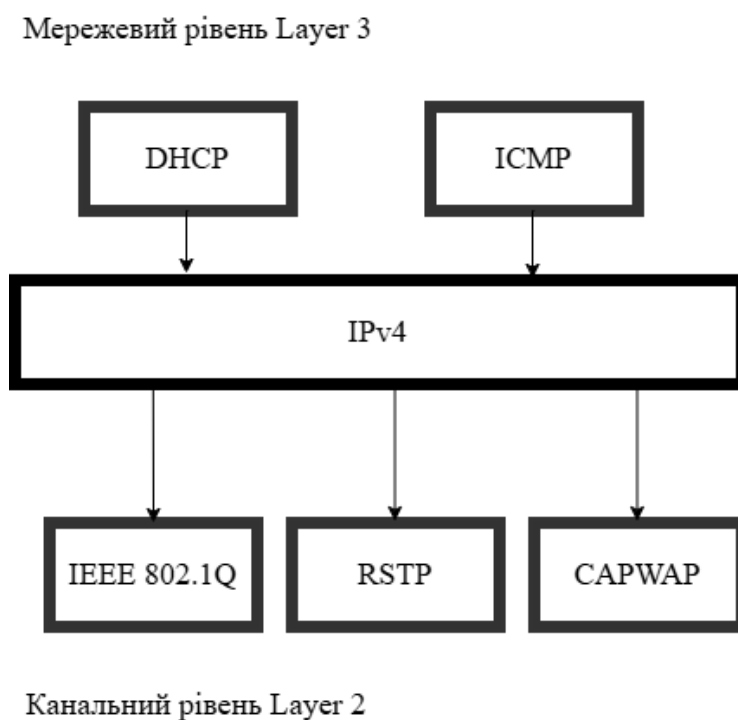


Рисунок 3.1 - Логічна схема взаємодії протоколів канального та мережного рівнів

Для детального аналізу функціонального призначення кожного елемента цієї структури, системні інженерні характеристики та обґрунтування вибору конкретних стандартів зведено в таблиці 3.1.

Таблиця 3.1 - Характеристика протоколів канального та мережного рівнів

| Рівень моделі OSI | Назва протоколу або стандарту | Основна функція в інфраструктурі         | Інженерне обґрунтування вибору                                          |
|-------------------|-------------------------------|------------------------------------------|-------------------------------------------------------------------------|
| Канальний рівень  | IEEE 802.1Q                   | Тегування трафіку віртуальних мереж      | Надійна логічна ізоляція інформаційних потоків підрозділів              |
| Канальний рівень  | RSTP                          | Автоматичне усунення топологічних петель | Швидка реконфігурація мережі за частки секунди при аваріях на лініях    |
| Канальний рівень  | CAPWAP                        | Тунелювання бездротового трафіку         | Централізоване транспортування даних клієнтів від антен до контролера   |
| Мережний рівень   | IPv4                          | Міжмережева адресація вузлів             | Забезпечення унікального адресного простору та маршрутизації пакетів    |
| Мережний рівень   | DHCP                          | Динамічна конфігурація клієнтів          | Виключення помилок ручного налаштування та спрощення адміністрування    |
| Мережний рівень   | ICMP                          | Тестування та діагностика каналів        | Верифікація доступності пристроїв за допомогою утиліт перевірки зв'язку |

Дані таблиці 3.1 та архітектурна залежність на рисунку 3.1 свідчать про те, що обраний набір стандартів сформований за принципом функціонального доповнення, де кожен протокол вирішує конкретну інженерну задачу. Сумісність цих технологій на апаратному рівні дозволяє створити монолітну логічну структуру, яка мінімізує обсяг службового трафіку в магістральних каналах зв'язку. Впровадження зазначених протоколів канального рівня забезпечує надійний захист від архітектурних помилок комутації, а обрані інструменти мережного рівня створюють передумови для повної автоматизації керування адресним простором промислового кампусу.

### 3.2 Налаштування конфігураційних параметрів комутаторів

Процес логічної конфігурації комутаційного обладнання є одним із найважливіших етапів розгортання мережі, оскільки саме на цьому рівні

реалізується сегментація інформаційних потоків та застосовуються політики доступу. Налаштування параметрів проводилося в інтерфейсі командного рядка операційної системи Cisco IOS для магістральних комутаторів ядра та комутаторів рівня доступу в кожній будівлі кампусу.

Першочерговим завданням логічної конфігурації стало створення глобальної бази даних віртуальних локальних мереж. Для забезпечення чіткої ідентифікації та зручності адміністрування кожному функціональному підрозділу було виділено унікальний ідентифікатор та присвоєно відповідне текстове ім'я. Повний перелік спроектованих логічних сегментів, їхнє функціональне призначення та режими функціонування інтерфейсів зв'язку зведено в таблиці 3.2.

Таблиця 3.2 – Схема розподілу віртуальних локальних мереж підприємства

| Ідентифікатор VLAN | Назва сегмента | Функціональне призначення підмережі                                          | Основний режим роботи портів доступу | Мережевий адресний простір |
|--------------------|----------------|------------------------------------------------------------------------------|--------------------------------------|----------------------------|
| VLAN 10            | Admin          | Обслуговування робочих місць адміністративного корпусу та керівництва        | Access                               | 192.168.10.0/24            |
| VLAN 20            | Logistics      | Забезпечення роботи персоналу складу та мобільних терміналів обліку          | Access                               | 192.168.20.0/24            |
| VLAN 30            | Lab            | Ізольовано середовище науково-дослідної лабораторії та вимірювальних станцій | Access                               | 192.168.30.0/24            |
| VLAN 40            | Production     | Обмін даними промислових систем та інженерного персоналу цеху                | Access                               | 192.168.40.0/24            |
| VLAN 50            | Management     | Службове управління інфраструктурою, серверами та тунелями CAPWAP            | Access / Trunk                       | 192.168.50.0/24            |

Дані, наведені в таблиці 3.2, демонструють чітку територіально-функціональну ізоляцію інформаційних потоків компанії, що дозволяє повністю локалізувати ширококомовний трафік у межах кожного конкретного відділу.

Створення бази даних віртуальних локальних мереж виконувалося примусово у режимі глобальної конфігурації на всіх пристроях комутації кампусу. Послідовність команд командного рядка для ініціалізації та найменування спроектованих сегментів відображено у лістингу 3.1.

### Лістинг 3.1 – Конфігурація бази даних віртуальних мереж на обладнанні

```
Switch# configure terminal
Switch(config)# vlan 10
Switch(config-vlan)# name Admin
Switch(config-vlan)# vlan 20
Switch(config-vlan)# name Logistics
Switch(config-vlan)# vlan 30
Switch(config-vlan)# name Lab
Switch(config-vlan)# vlan 40
Switch(config-vlan)# name Production
Switch(config-vlan)# vlan 50
Switch(config-vlan)# name Management
Switch(config-vlan)# exit
```

Впровадження конфігурації з лістингу 3.1 дозволяє розмежувати фізичне середовище комутаторів на логічні домени колізій та широкомовні домени. Команда `vlan [ID]` створює відповідний індекс у загальній таблиці комутації, а директива `name` прив'язує до нього текстовий маркер для спрощення подальшого моніторингу трафіку.

Наступним кроком стала конфігурація користувацьких інтерфейсів на комутаторах рівня доступу будівель. Порти, до яких підключаються кінцеві пристрої, такі як стаціонарні комп'ютери чи промислові контролери, були примусово переведені в режим доступу, логічно прив'язані до відповідного ідентифікатора та оптимізовані за допомогою активації функції швидкого переходу стану порту. Типовий інженерний приклад налаштування групи користувацьких інтерфейсів на комутаторі адміністративного підрозділу наведено у лістингу 3.2.

### Лістинг 3.2 – Налаштування користувацьких інтерфейсів рівня доступу

```
Acc-Admin(config)# interface range fastEthernet 0/3-19
Acc-Admin(config-if-range)# switchport mode access
Acc-Admin(config-if-range)# switchport access vlan 10
Acc-Admin(config-if-range)# spanning-tree portfast
Acc-Admin(config-if-range)# no shutdown
Acc-Admin(config-if-range)# exit
```

Під час налаштування периферійних інтерфейсів команда `interface range` дозволяє згрупувати порти з 3 по 19 для одночасного застосування конфігурації. Директива `switchport mode access` виключає можливість динамічного узгодження типу підключення та жорстко визначає порт як клієнтський, а команда `switchport access vlan 10` перенаправляє весь вхідний нетегований трафік з цих інтерфейсів у відповідний логічний сегмент.

Для оптимізації роботи робочих місць застосовано технологію `spanning-tree portfast`. Завдяки їй клієнтські порти при фізичному підключенні кабелю миттєво переходять у стан пересилання даних (`Forwarding`), минаючи стандартні 30-секундні стадії прослуховування (`Listening`) та навчання (`Learning`) протоколу STP. Це запобігає затримкам та збоям при отриманні мережевих реквізитів від служби DHCP кінцевими пристроями.

Окрему увагу приділено налаштуванню магістральних ліній зв'язку між рівнем доступу та згорнутим ядром мережі. Оскільки по одному фізичному кабелю необхідно передавати трафік різних віртуальних мереж одночасно, відповідні порти Uplink були переведені в транковий режим із впровадженням протоколу інкапсуляції та відключенням механізмів динамічного узгодження для запобігання кібератакам. Послідовність команд для конфігурації магістральних інтерфейсів комутації наведено у лістингу 3.3.

### Лістинг 3.3 – Конфігурація магістральних транкових каналів

```
Acc-Admin(config)# interface range fastEthernet 0/1-2
Acc-Admin(config-if-range)# switchport trunk encapsulation dot1q
Acc-Admin(config-if-range)# switchport mode trunk
Acc-Admin(config-if-range)# switchport nonegotiate
Acc-Admin(config-if-range)# no shutdown
```

```
Acc-Admin(config-if-range)# exit
```

Для портів магістральних аплінків fastEthernet 0/1-2 першочергово застосовано команду `switchport trunk encapsulation dot1q`, яка визначає міжнародний стандарт IEEE 802.1Q як базовий метод тегування кадрів, який полягає у додаванні 4-байтового тегу з VLAN ID у заголовок Ethernet-фрейму. Наступна команда `switchport mode trunk` переводить інтерфейси в режим магістралі для транзиту трафіку всіх створених VLAN кампусу.

З метою посилення безпеки та захисту від атак типу VLAN Hopping (несанкціоноване проникнення в інші підмережі), впроваджено команду `switchport nonegotiate`. Вона повністю вимикає пропрієтарний протокол Cisco DTP Dynamic Trunking Protocol, що унеможливорює підміну ролі порту зловмисником за допомогою надсилання фіктивних пакетів динамічного узгодження.

Для захисту всієї інфраструктури другого рівня від утворення топологічних петель в умовах подвійного підключення кожного комутатора доступу до резервованого ядра, було активовано швидку модифікацію протоколу дерева комутації. З метою оптимізації маршрутів проходження магістрального трафіку та призначення пріоритетів, головний комутатор ядра був налаштований як первинний кореневий міст, а резервний комутатор ядра – як вторинний. Алгоритм налаштування параметрів відмовостійкості для пристроїв згорнутого ядра відображено у лістингу 3.4.

Лістинг 3.4 – Налаштування параметрів пріоритету протоколу дерева комутації

```
Core-1(config)# spanning-tree mode rapid-pvst
Core-1(config)# spanning-tree vlan 10,20,30,40,50 root primary

Core-2(config)# spanning-tree mode rapid-pvst
Core-2(config)# spanning-tree vlan 10,20,30,40,50 root secondary
```

Активація режиму `rapid-pvst` запускає сучасний стандарт IEEE 802.1w (Rapid STP) окремо для кожної віртуальної локальної мережі. Оскільки

комутатори доступу підключені до двох магістральних пристроїв одночасно через інтерфейси Fast Ethernet, утворення фізичних петель та широкомовних штормів є неминучим.

Для чіткої та прогнозованої побудови логічного дерева без петель, на комутаторі Core-1 виконано команду spanning-tree vlan 10,20,30,40,50 root primary. Вона автоматично знижує його власну вагу пріоритету (Bridge Priority) з базового значення 32768 до 24576, роблячи цей пристрій головним кореневим мостом (Root Bridge) для всього кампусу. Усі найкоротші та пріоритетні маршрути трафіку від підрозділів будуть будуватися саме через Core-1.

На комутаторі Core-2 команда root secondary встановлює проміжний пріоритет 28672. Це переводить резервне ядро в стан очікування. За такої конфігурації Rapid-PVST+ блокує надлишкові лінії на портах доступу, але у разі фізичного пошкодження основного кабелю або виходу з ладу комутатора Core-1, протокол за час менше 2 секунд активує резервні інтерфейси Fast Ethernet і перенаправляє трафік через Core-2 без критичного переривання сесій користувачів.

Аналіз наведених конфігураційних лістингів показує, що логічна структура другого рівня побудована на базі суворих індустріальних рекомендацій. Поєднання ізоляції широкомовних доменів, відключення вразливих протоколів автоматичного узгодження транків та оптимізація топології за допомогою примусового розподілу ролей корневих мостів у протоколі швидкого розгортання дерева комутації дозволяє забезпечити стабільну та захищену основу для функціонування мережевих сервісів вищих рівнів моделі OSI.

### **3.3 Налаштування маршрутизаторів**

Оскільки в розробленій архітектурі кампусної мережі використовується ієрархічна модель зі згорнутим ядром, функції традиційних маршрутизаторів

щодо передачі інформаційних потоків між різними підмережами виконують магістральні багаторівневі комутатори третього рівня. Такий підхід дозволяє здійснювати пересилання пакетів на апаратному рівні за допомогою спеціалізованих мікросхем, що забезпечує значно вищу пропускну здатність та мінімізує затримки порівняно з використанням зовнішніх маршрутизаторів.

Основою для забезпечення взаємодії між ізольованими віртуальними сегментами є технологія міждоменної маршрутизації. Для її реалізації на головному магістральному комутаторі ядра була глобально активована функція обробки мережного рівня. Далі для кожного функціонального підрозділу було створено комутований віртуальний інтерфейс. Цьому інтерфейсу призначається перша вільна статична адреса з відповідного діапазону, яка надалі виступає основним шлюзом для всіх кінцевих пристроїв цієї підмережі. Послідовність команд для активації маршрутизації, створення віртуальних шлюзів та налаштування агентів ретрансляції на комутаторі ядра наведено у лістингу 3.5.

### Лістинг 3.5 – Активація маршрутизації та налаштування віртуальних інтерфейсів

```
Core-1# configure terminal
Core-1(config)# ip routing
Core-1(config)# interface vlan 10
Core-1(config-if)# description Gateway-Admin
Core-1(config-if)# ip address 192.168.10.1 255.255.255.0
Core-1(config-if)# no shutdown
Core-1(config-if)# exit
Core-1(config)# interface vlan 20
Core-1(config-if)# description Gateway-Logistics
Core-1(config-if)# ip address 192.168.20.1 255.255.255.0
Core-1(config-if)# no shutdown
Core-1(config-if)# exit
Core-1(config)# interface vlan 30
Core-1(config-if)# description Gateway-Lab
Core-1(config-if)# ip address 192.168.30.1 255.255.255.0
Core-1(config-if)# no shutdown
Core-1(config-if)# exit
Core-1(config)# interface vlan 40
Core-1(config-if)# description Gateway-Production
Core-1(config-if)# ip address 192.168.40.1 255.255.255.0
Core-1(config-if)# no shutdown
Core-1(config-if)# exit
```

```
Core-1(config)# interface vlan 50
Core-1(config-if)# description Gateway-Management
Core-1(config-if)# ip address 192.168.50.1 255.255.255.0
Core-1(config-if)# no shutdown
Core-1(config-if)# exit
```

Аналіз конфігурації лістингу 3.5 показує, що першочергова команда `ip routing` переводить комутатор Core-1 з режиму роботи звичайного пристрою другого рівня у режим повноцінного маршрутизатора. Створення логічних інтерфейсів типу `interface vlan [ID]` дозволяє зв'язати ізольовані ширококомовні домени Layer 2 із відповідними IP-інтерфейсами Layer 3.

Команда `description` виконує службову функцію документування, полегшуючи подальше обслуговування мережі оператором. Директива `ip address` призначає IP-адресу та маску підмережі класу C для кожного SVI, формуючи таблицю маршрутизації комутатора (Routing Table) на основі безпосередньо підключених мереж (Directly Connected). Команда `no shutdown` примусово активує логічний інтерфейс.

Паралельно із забезпеченням міждоменного обміну даними, на магістральний комутатор ядра покладено функцію централізованого автоматичного розподілу мережевих параметрів для кінцевих пристроїв. Для кожної віртуальної мережі підприємства у глобальній конфігурації пристрою було розгорнуто окремі пули адрес із чітким визначенням маски підмережі, координатора основного шлюзу та сервера доменних імен. З метою уникнення конфліктів адресного простору та захисту критично важливих вузлів інфраструктури, перші десять доступних адрес у кожному логічному сегменті були заздалегідь зарезервовані для статичного призначення серверам, бездротовому контролеру WLC та інтерфейсам комутаторів. Алгоритм конфігурації пулів динамічного налаштування вузлів безпосередньо на комутаційному обладнанні ядра відображено у лістингу 3.6.

### Лістинг 3.6 – Конфігурація пулів динамічного розподілу адрес

```
Core-1(config)# ip dhcp excluded-address 192.168.10.1 192.168.10.10
Core-1(config)# ip dhcp excluded-address 192.168.20.1 192.168.20.10
Core-1(config)# ip dhcp excluded-address 192.168.30.1 192.168.30.10
Core-1(config)# ip dhcp excluded-address 192.168.40.1 192.168.40.10
Core-1(config)# ip dhcp excluded-address 192.168.50.1 192.168.50.10
Core-1(config)# ip dhcp pool Pool-Admin
Core-1(dhcp-config)# network 192.168.10.0 255.255.255.0
Core-1(dhcp-config)# default-router 192.168.10.1
Core-1(dhcp-config)# dns-server 192.168.50.10
Core-1(dhcp-config)# exit
Core-1(config)# ip dhcp pool Pool-Logistics
Core-1(dhcp-config)# network 192.168.20.0 255.255.255.0
Core-1(dhcp-config)# default-router 192.168.20.1
Core-1(dhcp-config)# dns-server 192.168.50.10
Core-1(dhcp-config)# exit
Core-1(config)# ip dhcp pool Pool-Lab
Core-1(dhcp-config)# network 192.168.30.0 255.255.255.0
Core-1(dhcp-config)# default-router 192.168.30.1
Core-1(dhcp-config)# dns-server 192.168.50.10
Core-1(dhcp-config)# exit
Core-1(config)# ip dhcp pool Pool-Production
Core-1(dhcp-config)# network 192.168.40.0 255.255.255.0
Core-1(dhcp-config)# default-router 192.168.40.1
Core-1(dhcp-config)# dns-server 192.168.50.10
Core-1(dhcp-config)# exit
```

У процесі побудови системи динамічної адресації критично важливим є використання команд глобальної конфігурації `ip dhcp excluded-address`. Вони вказують службі Cisco IOS DHCP вилучити діапазони від .1 до .10 з автоматичної видачі. Це повністю унеможливило виникнення IP-конфліктів, оскільки адреси .1 зафіксовані за віртуальними шлюзами, а адреси з .2 по .10 виділені для статичного призначення активному обладнанню та серверам (наприклад, корпоративний DNS-сервер у сегменті керування розташований на адресі 192.168.50.10).

Команда `ip dhcp pool [ім'я]` ініціалізує конфігураційний підрежим конкретного пулу. Директива `network` задає межі адресного простору та маску підмережі, з якої клієнти отримуватимуть параметри. Налаштування `default-router` вказує кінцевим робочим станціям IP-адресу їхнього шлюзу за замовчуванням (відповідний інтерфейс SVI ядра), куди вони мають надсилати трафік, призначений для інших підмереж або глобальної мережі Інтернет. Команда `dns-`

server забезпечує автоматичне налаштування клієнтів на роботу з єдиним центром роздільної здатності доменних назв компанії.

Реалізована схема суміщення функцій апаратної маршрутизації та динамічної адресації на базі єдиного пристрою третього рівня дозволяє оптимізувати інформаційні потоки промислового кампусу. Локальна обробка запитів на виділення адрес безпосередньо мережевим ядром для всіх функціональних та службових зон усуває потребу в трансляції широкомовних пакетів (DHCP Discover) через магістральні канали до сторонніх серверів у кожній будівлі. Це суттєво мінімізує обсяг службового трафіку, підвищує швидкість ініціалізації клієнтських станцій у робочих зонах та забезпечує високу автономність і відмовостійкість функціонування кожного підрозділу компанії.

### **3.4 Налаштування бездротової мережі**

Розгортання бездротового сегмента корпоративної інфраструктури промислового кампусу базується на принципах централізованого управління та чіткого розділення функцій обробки даних (архітектура Split-MAC). На відміну від застарілих архітектур з автономними точками доступу (Fat AP), які вимагають децентралізованого адміністрування та ручного внесення змін на кожному пристрої, спроектована система покладає всю інтелектуальну логіку керування радіоефіром, автентифікації користувачів та координації мобільності на спеціалізований апаратний контролер бездротової локальної мережі (WLC).

Логічна конфігурація бездротового середовища виконувалася через спеціалізований графічний веб-інтерфейс (HTTPS) системи управління контролера, доступ до якого здійснювався з робочої станції адміністратора, підключеної до адміністративного сегмента управління інфраструктурою. Першим етапом розгортання став запуск майстра початкової ініціалізації (Setup Wizard), де було створено обліковий запис головного адміністратора та визначено

базові мережеві реквізити пристрою. Інтерфейсу управління (Management Interface) було призначено статичну IP-адресу 192.168.50.11 із прив'язкою до основного шлюзу магістрального комутатора ядра. Вікно конфігурації базових параметрів та керуючого інтерфейсу контролера наведено на рисунку 3.2.

92.168.50.11

**CISCO** Cisco 3500 Series Wireless LAN Controller

1 Set Up Your Controller

System Name

Country

Date & Time

Timezone

NTP Server

Management IP Address

Subnet Mask

Default Gateway

Management VLAN ID

Рисунок 3.2 – Налаштування у графічному веб-інтерфейсі

На наступному кроці майстра ініціалізації було створено первинний профіль бездротової мережі для співробітників із призначенням ідентифікатора бездротової мережі SSID (Corporate\_WLAN). Для забезпечення можливості початкового тестування радіоефіру та підключення точок доступу, профіль було тимчасово ініціалізовано з базовим рівнем захисту (WPA2-PSK), з подальшим плановим переведенням його на корпоративний стандарт безпеки з використанням зовнішньої служби автентифікації. Загальний підсумок введених

конфігураційних параметрів перед їхнім застосуванням у пам'ять пристрою відображено на рисунку 3.3.

Please confirm settings and apply

1

Controller Settings

Username

admin

System Name

WLC-Corp

Country

Netherlands (NL)

Date & Time

05/22/2026 15:19:17

Timezone

Amsterdam, Berlin, Rome, Vienna

NTP Server

-

Management IP Address

192.168.50.11

Management IP Subnet

255.255.255.0

Management IP Gateway

192.168.50.1

Management VLAN ID

0

2

Wireless Network Settings

Employee Network

Network Name

Corp\_WLAN

Security

WPA2 Personal

Passphrase:

\*\*\*\*\*

Employee VLAN

Management VLAN

DHCP Server Address

-

Guest Network

3

Advanced Settings

RF Parameter Optimization

Virtual IP Address

1.1.1.1

Local Mobility Group

Default

Back

Apply

Рисунок 3.3 – Підсумок введених конфігураційних параметрів

Для систематизації та наочного представлення спроектованих фінальних налаштувань, ключові конфігураційні параметри бездротового контролера після завершення налаштування та переходу до розширеного інженерного режиму Advanced Mode зведено в таблиці 3.3.

Таблиця 3.3 – Конфігураційні параметри бездротового контролера WLC

| Назва параметра конфігурації | Логічне значення у системі | Функціональне призначення та прив'язка                              |
|------------------------------|----------------------------|---------------------------------------------------------------------|
| Management Interface IP      | 192.168.50.11              | Основна адреса управління контролером у службовому VLAN 50          |
| AP Manager Interface IP      | 192.168.50.12              | Службовий інтерфейс для термінації тунелів CAPWAP від точок доступу |

Продовження таблиці 3.3

| Назва параметра конфігурації | Логічне значення у системі | Функціональне призначення та прив'язка                              |
|------------------------------|----------------------------|---------------------------------------------------------------------|
| Profile Name / SSID          | Corporate_WLAN             | Єдине ім'я бездротової мережі для користувачів кампусу              |
| WLAN ID                      | 1                          | Логічний ідентифікатор бездротового профілю всередині WLC           |
| Interface / Interface Group  | VLAN_Wireless_Interface    | Динамічний інтерфейс, прив'язаний до користувацького сегмента даних |
| Security Layer 2             | WPA2-Enterprise            | Стандарт шифрування та захисту радіоефіру корпоративного рівня      |
| Authentication Server IP     | 192.168.50.10              | Адреса виділеного сервера автентифікації RADIUS                     |

Дані, наведені в таблиці 3.3, відображають логічну структуру бездротової архітектури, де чітко розділено інтерфейси безпосереднього управління пристроєм та інтерфейси взаємодії з легковаговими точками доступу. Першим кроком конфігурації стало створення динамічного інтерфейсу користувацьких даних (VLAN\_Wireless\_Interface), який логічно пов'язує бездротовий сегмент із відповідним магістральним тегованим каналом trunk на комутаторі ядра. Це гарантує, що весь трафік, який генерують мобільні клієнти, після деінкапсуляції на контролері безпосередньо спрямовується у визначений простір адрес підприємства, забезпечуючи надійну Inter-VLAN маршрутизацію.

Наступним етапом стало створення бездротового профілю із призначенням унікального ідентифікатора мережі SSID. Для забезпечення виключно високого рівня кібербезпеки в промислових та адміністративних зонах підприємства, у налаштуваннях безпеки другого рівня було повністю відкинуто використання спільних статичних ключів WPA2-PSK. Замість цього активовано режим корпоративного захисту WPA2-Enterprise, який потребує обов'язкової перевірки кожного пристрою через зовнішню службу. У розділі конфігурації серверів автентифікації було вказано статичну адресу корпоративного сервера RADIUS (192.168.50.10) та визначено унікальний пароль спільного секрету (Shared Secret) для криптографічного захисту каналу передачі облікових даних користувачів.

Фінальним кроком налаштування бездротового сегмента стала автоматична ініціалізація легковагових точок доступу LAP (Lightweight Access Point). Після

фізичного підключення до комутаторів рівня доступу в будівлях логістики, лабораторії та виробництва, кожна точка доступу автоматично отримала IP-адресу в сегменті управління від пулу Pool-Management комутатора ядра. Завдяки зчитаній з пулу налаштованій інженерній опції DHCP Option 43, пристрої LAP виявили точну IP-адресу керуючого інтерфейсу бездротового контролера WLC (192.168.50.11).

Після цього точки доступу встановили з контролером захищені логічні тунелі за протоколом CAPWAP (RFC 5415). Контролер в автоматичному режимі провів звірку версій, завантажив на точки доступу актуальне програмне забезпечення та єдину конфігурацію створеного бездротового профілю Corporate\_WLAN, що дозволило запустити синхронне радіомовлення в єдиному безшовному просторі кампусу.

Реалізована схема централізованого налаштування бездротового простору забезпечує тотальний контроль за станом радіоефіру підприємства. Завдяки інкапсуляції та тунелюванню всього користувацького трафіку через контролер WLC, система миттєво адаптується до переміщень працівників складів та цехів. Це забезпечує безшовне перемикання мобільних клієнтів (роумінг) між антенами точок LAP без втрати пакетів, затримок та розриву мережевих сесій, а інтеграція з сервером автентифікації повністю нівелює ризик проникнення сторонніх осіб до внутрішніх технологічних ресурсів компанії.

### **3.5 Забезпечення безпеки мережі**

Забезпечення комплексного захисту корпоративної телекомунікаційної інфраструктури промислового кампусу є критично важливим завданням, оскільки несанкціонований доступ до внутрішніх ресурсів компанії або перехоплення даних може призвести до втрати конфіденційної науково-технічної інформації, витоку службових відомостей чи дестабілізації промислових автоматизованих

комплексів. Стратегія безпеки проектованої мережі реалізується за допомогою впровадження стандарту безпеки корпоративного рівня IEEE 802.1X у бездротовому радіоефірі, що дозволяє організувати строгий порт-орієнтований контроль доступу на етапі первинного підключення кінцевих пристроїв.

На відміну від побутових мереж, де використовується єдиний статичний пароль для всіх пристроїв (архітектура WPA2-Personal), яка є вразливою до компрометації та перехоплення, технологія WPA2-Enterprise вимагає від кожного клієнта проходження індивідуальної автентифікації за унікальними обліковими даними. Процес перевірки легітимності користувачів проєктується із залученням централізованого бездротового контролера WLC та виділеного сервера віддаленої автентифікації RADIUS (Remote Authentication in Dial-In User Service), що реалізує концепцію безпеки AAA (Authentication, Authorization, Accounting).

Практична реалізація цієї моделі безпеки в середовищі моделювання починається з конфігурації корпоративного сервера. Через вбудований веб-інтерфейс налаштування служб сервера виконується активація відповідного параметра безпеки та реєстрація бездротового контролера WLC як легітимного клієнта RADIUS із зазначенням його керуючої IP-адреси (192.168.50.11) та спільного секретного ключа (Shared Secret). Окрім цього, у базу даних сервера вносяться персональні облікові записи, логіни та стійкі хешовані паролі, працівників для різних віртуальних мереж. Вікно конфігурації параметрів клієнта AAA на сервері та створення облікових записів користувачів у базі даних відображено на рисунку 3.4.

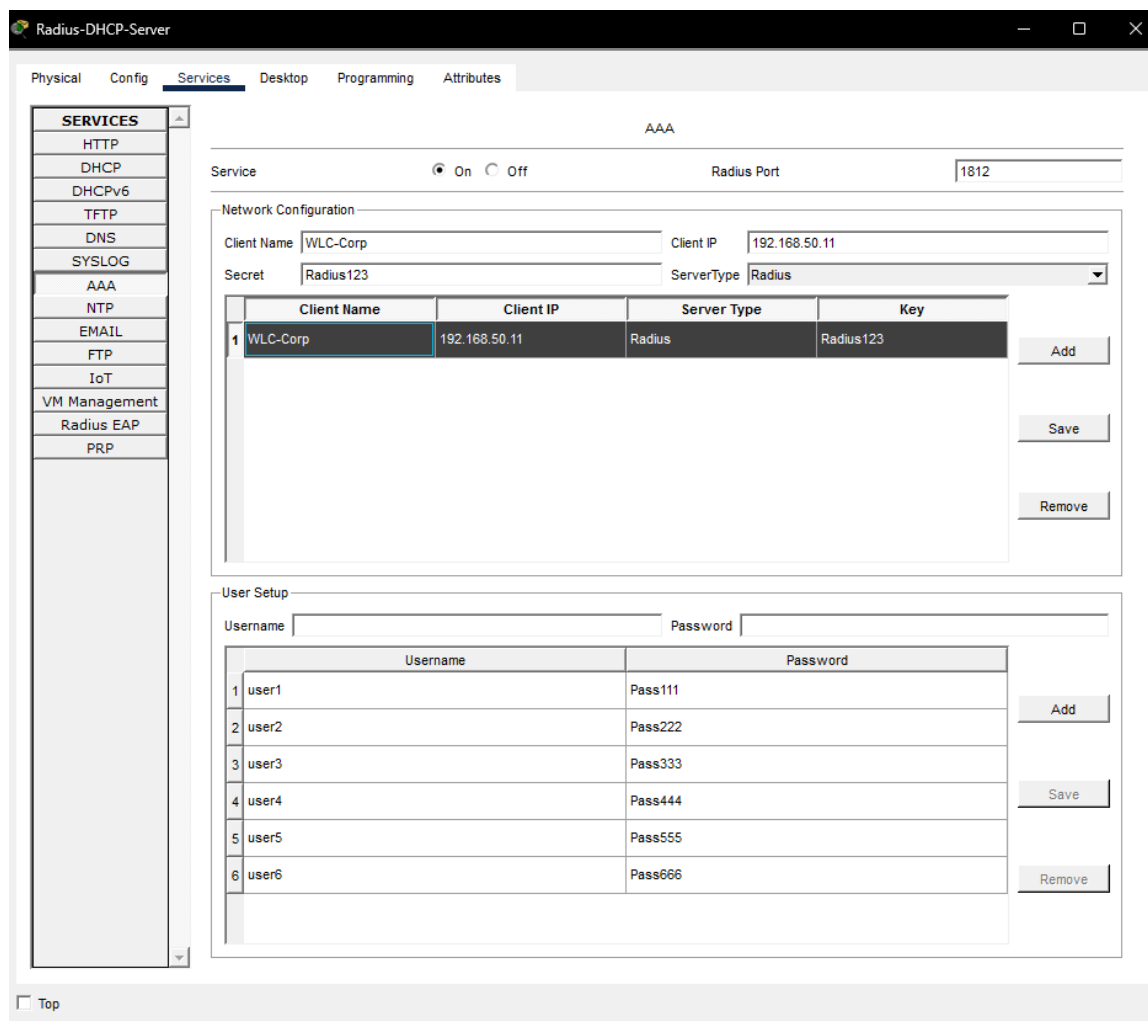


Рисунок 3.4 - Вікно конфігурації параметрів клієнта та користувачів на сервері

Наступним кроком є інтеграція сервера автентифікації з бездротовою інфраструктурою через графічний веб-інтерфейс керування контролера WLC. У розділі розширених параметрів безпеки створюється новий запис, де вказується статична IP-адреса сервера автентифікації, стандартний UDP-порт 1812, що використовується для передачі запитів автентифікації, та вноситься аналогічний секретний ключ для взаємної криптографічної верифікації повідомлень між WLC та сервером. Вікно прив'язки зовнішнього сервера автентифікації у веб-інтерфейсі системи управління WLC наведено на рисунку 3.5.

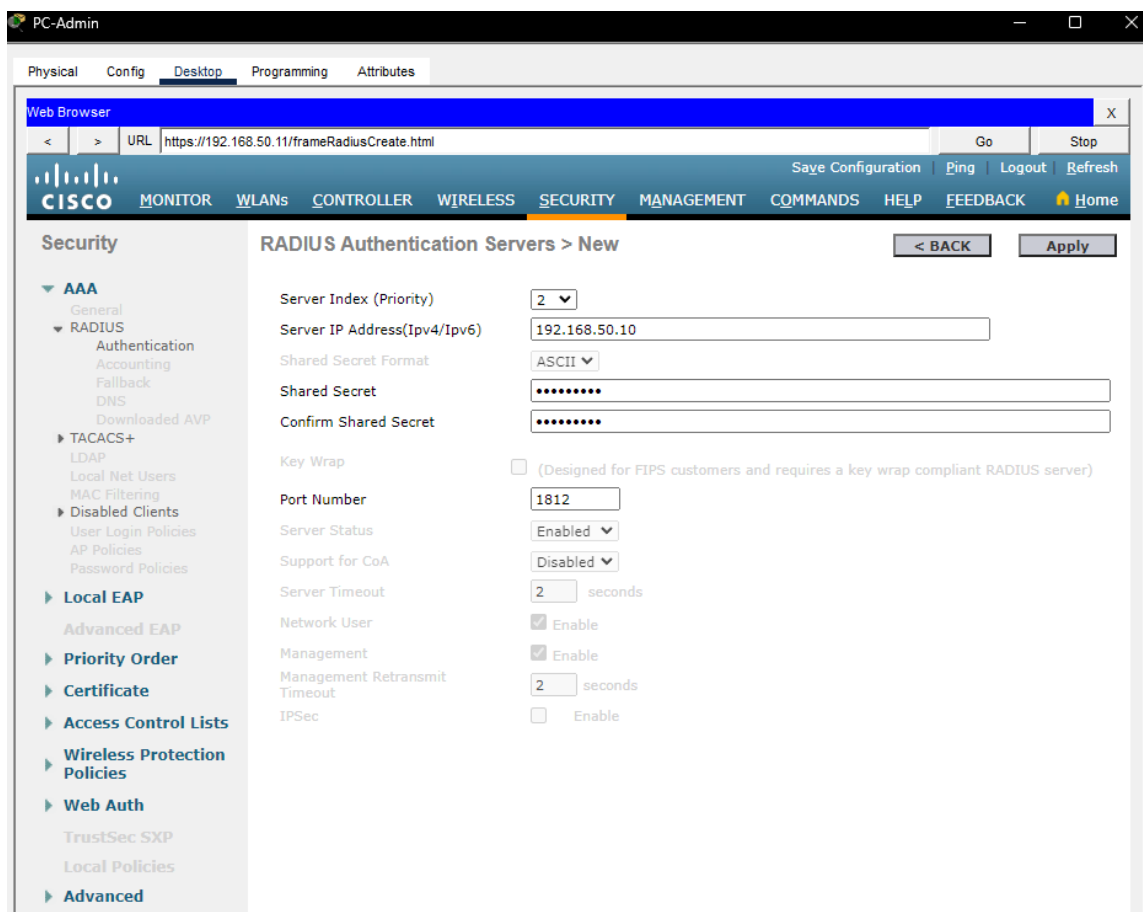


Рисунок 3.5 – рив’язка зовнішнього сервера автентифікації RADIUS у веб-інтерфейсі WLC

При спробі підключення мобільного девайса, ноутбука, смартфона чи інших приладів до легковагової точки доступу LAP, його безпосередній доступ до мережевих ресурсів кампусу повністю блокується на канальному рівні. Клієнт (Supplicant) надсилає запит на автентифікацію за протоколом EAPoL (Extensible Authentication Protocol over LAN). Точка доступу LAP транслює цей запит через захищений тунель CAPWAP до бездротового контролера WLC, який виконує роль автентифікатора (Authenticator).

Контролер перепаковує отримані облікові дані у формат пакетів RADIUS Access-Request і перенаправляє їх по дротовій гігабітній магістралі на RADIUS-сервер. Перевірка автентифікаційного вектора здійснюється за захищеним індустріальним протоколом EAP-PEAP (Protected Extensible Authentication

Protocol), що створює зашифрований TLS-тунель між клієнтом та сервером для захисту паролів.

Лише після успішного звіряння даних сервер повертає на WLC пакет RADIUS Access-Accept. Отримавши позитивну відповідь, контролер WLC генерує унікальний тимчасовий сесійний ключ шифрування (Pairwise Master Key) для конкретного абонента, передає його на точку LAP і динамічно відкриває логічний порт для пристрою, спрямовуючи його трафік у бездротовий сегмент VLAN 50. Логічну послідовність етапів взаємодії пристроїв під час процесу автентифікації наведено на рисунку 3.6.

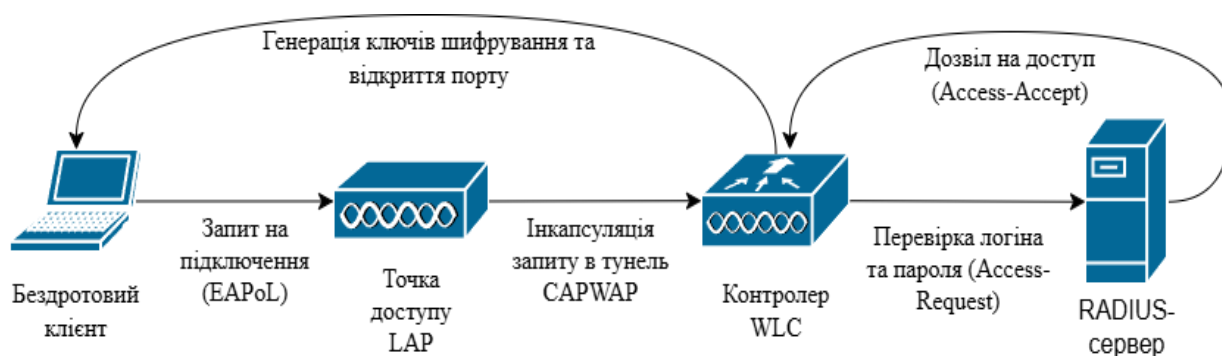


Рисунок 3.6 - Процес автентифікації клієнтів за стандартом IEEE 802.1X у мережі WLAN

Впроваджений комплекс засобів централізованого контролю у поєднанні з індивідуальною сертифікацією бездротових користувачів повністю нівелює ризик проникнення сторонніх осіб до внутрішніх технологічних та інформаційних ресурсів компанії. Навіть у разі перехоплення бездротового радіосигналу за межами фізичного периметра будівель, злоумисник не зможе отримати доступ до корпоративних даних без наявності активованого індивідуального облікового запису на центральному RADIUS-сервері, що забезпечує найвищий рівень стійкості інформаційного середовища підприємства до зовнішніх векторів кібератак.

## **4 ІМІТАЦІЙНЕ МОДЕЛЮВАННЯ ТА ТЕСТУВАННЯ МЕРЕЖІ**

### **4.1 Обґрунтування вибору програмного забезпечення для моделювання**

Перед безпосереднім розгортанням спроектованої телекомунікаційної інфраструктури на реальному фізичному обладнанні промислового кампусу критично важливим етапом є проведення комп'ютерного імітаційного моделювання. Це дозволяє виконати комплексну перевірку працездатності мережевих протоколів, оцінити коректність логічної адресації, протестувати налаштування політик безпеки та виявити потенційні помилки чи архітектурні недоліки ще на етапі проєктування, що мінімізує фінансові витрати та ризики збоїв у майбутньому.

Для реалізації імітаційного моделювання в межах бакалаврської кваліфікаційної роботи було обрано спеціалізоване програмне середовище Cisco Packet Tracer, яке є потужним інструментом візуалізації та симуляції мережевих процесів, розробленим компанією Cisco Systems. Даний програмний комплекс дозволяє створювати масштабні мережеві топології, що поєднують десятки різнотипних пристроїв, та забезпечує повну емуляцію операційної системи Cisco IOS, надаючи інженеру доступ до інтерфейсу командного рядка для тонкого налаштування маршрутизаторів, комутаторів другого та третього рівнів.

Основними технічними та функціональними перевагами використання Cisco Packet Tracer є висока точність емуляції апаратних компонентів. Програма містить точні логічні моделі сучасного обладнання Cisco, включаючи магістральні багатофункціональні комутатори як Cisco Catalyst 3650/3560, що виконують роль згорнутого ядра, інтелектуальні бездротові контролери WLC серії 3504 та полегшені точки доступу Lightweight AP, що повністю відповідає апаратній специфікації проєкту.

Підтримка широкого стека мережевих технологій. Середовище дозволяє в повному обсязі симулювати роботу технологій, закладених в архітектуру підприємства: агрегацію каналів, протоколи усунення петель, віртуальні локальні

мережі, міждоменну маршрутизацію Inter-VLAN routing, а також централізовані сервіси DHCP та AAA RADIUS.

Режим моделювання в реальному часі та режим симуляції. Крім стандартного виконання команд, Cisco Packet Tracer підтримує унікальний інструмент покрокового перехоплення пакетів. У цьому режимі інженер має можливість детально аналізувати структуру блоків даних на кожному рівні еталонної моделі OSI, відстежувати проходження кадрів через конкретні інтерфейси комутаторів та візуалізувати процеси інкапсуляції і деінкапсуляції трафіку.

Завдяки інтегрованим алгоритмам аналізу, обране програмне забезпечення дозволяє не лише відтворити статичну схему з'єднань, а й змодельовати динамічну поведінку мережі під час виникнення критичних подій, наприклад, при аварійному розриві одного з магістральних каналів зв'язку або при масовому підключенні мобільних терміналів у зонах логістики та виробництва. Таким чином, використання Cisco Packet Tracer забезпечує створення адекватного та репрезентативного віртуального полігону для всебічної верифікації розробленого інженерного рішення.

## **4.2 Аналіз результатів тестування та верифікація мережевих сервісів**

Після завершення етапу конфігурування всіх активних компонентів системи у середовищі Cisco Packet Tracer було проведено серію комплексних випробувань для верифікації працездатності розробленої архітектури промислового кампусу. Тестування мало на меті підтвердити коректність функціонування трьох основних технологічних блоків: системи динамічної адресації, підсистеми апаратної міждоменної маршрутизації на рівні згорнутого ядра та механізмів бездротового доступу із захистом користувачів.

Першим етапом тестування стала перевірка працездатності централізованої служби DHCP, розгорнутої безпосередньо на магістральному багаторівневому комутаторі Core-1. Для цього тестові робочі станції (персональні комп'ютери та ноутбуки), розташовані в різних будівлях та підключені до відповідних портів комутаторів доступу, були переведені в режим автоматичного отримання мережевих реквізитів. Результати тестування показали, що пристрої успішно ініціюють широкомовний запит та миттєво отримують унікальні конфігураційні параметри з виділеного для їхнього VLAN пулу. При цьому перші десять IP-адрес у кожному сегменті залишилися незайнятими, що підтверджує точність роботи команд виключення адрес. Графічне вікно успішного отримання параметрів наведено на рисунку 4.1.

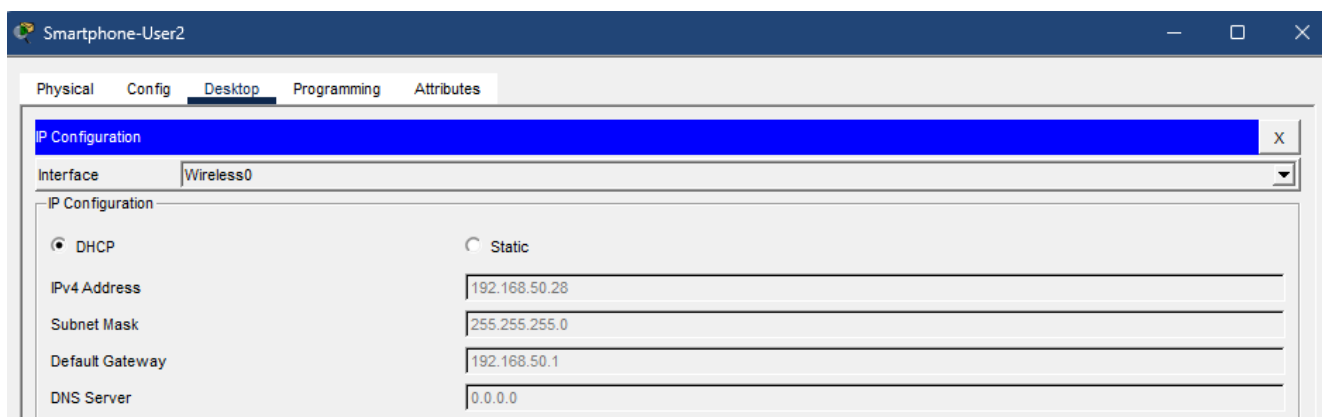
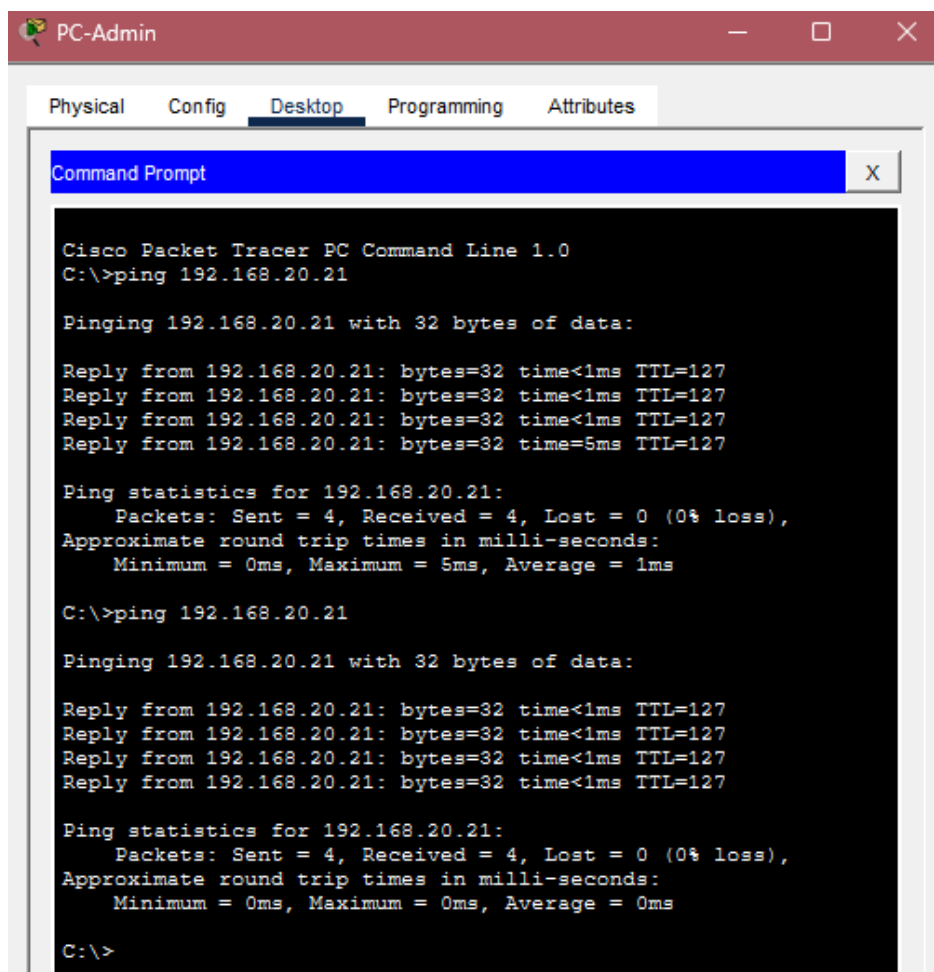


Рисунок 4.1 - Успішна ініціалізація та отримання мережевих параметрів кінцевим пристроєм через пул DHCP Core-1

Другим, найбільш критичним етапом випробувань стала верифікація підсистеми міждоменної маршрутизації Inter-VLAN routing. Оскільки за замовчуванням трафік між різними віртуальними мережами повністю ізольований, успіх обміну даними залежав від коректності роботи логічних інтерфейсів другого та третього рівнів на магістралі. Перевірка здійснювалася шляхом відправлення тестових ехо-запитів за протоколом ICMP між клієнтами, які знаходяться в різних структурних підрозділах, наприклад з робочого місця адміністратора у VLAN 10 до термінала зони логістики у VLAN 20. Результати

комп'ютерної симуляції в інтерфейсі командного рядка відображено на рисунку 4.2.



```

PC-Admin
Physical Config Desktop Programming Attributes
Command Prompt X
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.20.21

Pinging 192.168.20.21 with 32 bytes of data:

Reply from 192.168.20.21: bytes=32 time<1ms TTL=127
Reply from 192.168.20.21: bytes=32 time<1ms TTL=127
Reply from 192.168.20.21: bytes=32 time<1ms TTL=127
Reply from 192.168.20.21: bytes=32 time=5ms TTL=127

Ping statistics for 192.168.20.21:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 5ms, Average = 1ms

C:\>ping 192.168.20.21

Pinging 192.168.20.21 with 32 bytes of data:

Reply from 192.168.20.21: bytes=32 time<1ms TTL=127
Reply from 192.168.20.21: bytes=32 time<1ms TTL=127
Reply from 192.168.20.21: bytes=32 time<1ms TTL=127
Reply from 192.168.20.21: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.20.21:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>

```

Рисунок 4.2 – Верифікація зв'язності та міждоменної маршрутизації між ізолюваними сегментами мережі

Стабільні відповіді від ув'язаних вузлів із нульовим відсотком втрат пакетів, показані на рисунку 4.2, свідчать про те, що комутатор ядра успішно виконує функції маршрутизатора на швидкості з'єднання каналів, забезпечуючи високошвидкісну провідну комутацію інформаційних потоків усього підприємства.

Паралельно було перевірено доступність критичної мережевої інфраструктури, а саме — виділеного корпоративного сервера, на якому функціонують сервіси DNS та AAA. Успішне проходження пакетів до вузла з

адресою 192.168.50.10 з будь-якої точки кампусу підтвердило правильність налаштування магістральних тегованих каналів та відсутність петель маршрутизації завдяки роботі протоколу STP. Візуалізацію процесу тестування доступності сервера наведено на рисунку 4.3.

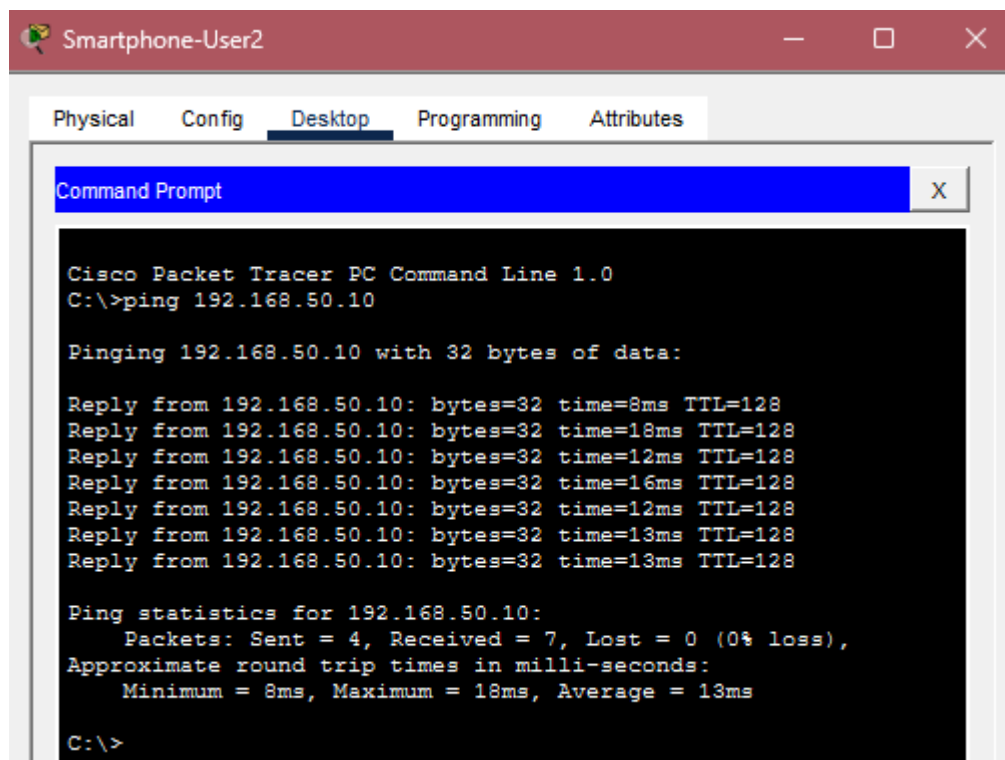


Рисунок 4.3 – Перевірка доступності центрального сервера автентифікації та мережеслужб

Фінальним етапом стало тестування бездротового середовища. Під час аналізу було зафіксовано, що легковагові точки доступу LAP успішно завершили побудову CAPWAP-тунелів до керуючого інтерфейсу WLC та транслують у простір SSID Corp\_WLAN. При спробі підключення бездротових клієнтів система автоматично перенаправляла запити на сервер RADIUS. Клієнти, які вводили валідні облікові дані, створені в базі даних AAA, успішно проходили фазу автентифікації, отримували динамічний сесійний ключ шифрування та легітимну IP-адресу, отримуючи повний доступ до дозволених ресурсів кампусу.

Таким чином, результати проведеного імітаційного моделювання та тестування повністю підтвердили технічну спроможність, надійність та

архітектурну цілісність розробленого проєкту корпоративної мережі підприємства.

#### **4.3 Управління трафіком та адміністрування мережі**

Організація ефективного інформаційного обміну всередині промислового кампусу та безперервний моніторинг стану активного обладнання є ключовими завданнями адміністрування сучасних телекомунікаційних систем. У розробленому проєкті управління трафіком на каналному та мережевому рівнях реалізовано за допомогою логічної сегментації адресного простору на віртуальні локальні мережі VLAN 10, 20, 30, 40, 50. Такий підхід дозволив локалізувати широкомовний шторм у межах кожного окремого підрозділу компанії, суттєво розвантажуючи магістральні канали зв'язку.

Адміністрування та передача керуючого трафіку здійснюється через спеціалізований виділений інтерфейс управління Management VLAN 50, у якому розташовані вебінтерфейси бездротового контролера WLC та інтерфейси комутаторів. Для централізованого моніторингу та конфігурування бездротової інфраструктури адміністратор мережі використовує захищений доступ до WLC, де в режимі реального часу відображається стан підключених полегшених точок доступу LAP, кількість активних мобільних клієнтів, обсяг переданих даних та рівень завантаження радіоефіру в кожній робочій зоні.

#### **4.4 Надання якості обслуговування**

Специфіка функціонування промислового підприємства вимагає забезпечення гарантованої доставки різних типів трафіку в межах єдиної

конвергентної мережі. Для запобігання затримкам критично важливих інформаційних потоків в архітектурі кампусу передбачено застосування механізмів забезпечення якості обслуговування QoS.

На магістральних комутаторах третього рівня та бездротовому контролері реалізовано класифікацію та маркування трафіку на основі профілів бездротових мереж та ідентифікаторів віртуальних мереж. Трафіку управління та пакетам від виробничого цеху присвоюється вищий пріоритет обробки у чергах обладнання, тоді як загальний користувацький трафік та інтернет-сесії обслуговуються за залишковим принципом. Це гарантує стабільну роботу автоматики та диспетчерських служб навіть у моменти пікових навантажень на мережу.

#### **4.5 Резервування модулів критичних для роботи мережі**

Для забезпечення високого рівня відмовостійкості та мінімізації часу простою інфраструктури у разі аварійних ситуацій у проєкті реалізовано апаратне та логічне резервування критичних вузлів мережі кампусу.

На каналному рівні резервування магістральних з'єднань між комутаторами доступу та згорнутим ядром мережі забезпечується розгортанням надлишкових фізичних ліній зв'язку. Для запобігання утворенню петель комутації та широкомовних штормів у конфігурації обладнання активовано роботу протоколу STP. У разі пошкодження основного оптичного або мідного кабелю цей протокол автоматично перераховує топологію за декілька секунд і перенаправляє інформаційні потоки через резервний інтерфейс. Крім того, для критичних ліній зв'язку ядра використовується технологія агрегації каналів EtherChannel, яка об'єднує кілька фізичних інтерфейсів в один логічний, забезпечуючи одночасно як балансування навантаження, так і миттєве резервування без переривання сесій користувачів.

## ВИСНОВКИ

У кваліфікаційній роботі бакалавра успішно вирішено актуальне науково-практичне завдання щодо проектування та реалізації корпоративної комп'ютерної мережі промислового підприємства з інтеграцією сучасних дротових і бездротових технологій зв'язку. Проведений аналіз архітектурних особливостей та специфіки функціонування сучасного промислового об'єкта дозволив повністю обґрунтувати вибір трирівневої ієрархічної моделі побудови мережі, реалізованої у форматі згорнутого ядра. Такий підхід забезпечив високу масштабованість інфраструктури, гнучкість управління інформаційними потоками та мінімальні затримки при передачі даних між різними територіально розподіленими корпусами кампусу.

Важливим етапом проектування розробленого рішення стало впровадження технології віртуальних локальних мереж, яка дозволила логічно розділити єдиний фізичний простір підприємства на п'ять повністю ізольованих функціональних та службових сегментів, що охоплюють адміністрацію, логістику, наукову лабораторію, виробничий цех та окремий простір управління інфраструктурою. Це заклало надійну основу для оптимізації внутрішнього трафіку шляхом повної локалізації широкомовних штурмів та дозволило реалізувати базовий рівень безпеки безпосередньо на каналах комутації доступу. Паралельно з цим було розроблено та практично реалізовано централізовану систему автоматичного розподілу адресного простору на основі конфігурування пулів протоколу динамічного налаштування вузлів безпосередньо на комутаційному обладнанні третього рівня, що значно спростило подальше адміністрування мережі та виключило ризик виникнення конфліктів адрес при підключенні нових робочих станцій.

Особливу увагу приділено розгортанню бездротової інфраструктури, побудованої на базі сучасної централізованої архітектури під управлінням апаратного контролера та полегшених точок доступу. Інтеграція службових

тунелів між антенами та контролером дозволила створити єдиний безшовний простір радіопокриття для мобільних терміналів на складах та у виробничих зонах, забезпечуючи надійний роумінг співробітників без розриву сесій та втрати інформаційних пакетів. Захист цього сегменту радіоефіру було підсилено за допомогою створення надійного комплексу засобів кібербезпеки корпоративного рівня через розгортання служби автентифікації та впровадження суворого стандарту безпеки, що повністю виключило можливість несанкційованого доступу сторонніх осіб до внутрішніх ресурсів кампусу.

Для всебічної верифікації розробленого інженерного рішення було проведено імітаційне моделювання проєкту в спеціалізованому програмному середовищі, результати якого повністю підтвердили високу працездатність, надійність, відмовостійкість та загальну архітектурну цілісність створеної мережі. Успішне проходження тестових ехо-запитів між різними підмережами та стабільне функціонування налаштованих мережевих сервісів довели правильність обраної стратегії маршрутизації та конфігурації активного обладнання. Таким чином, розроблений проєкт повністю задовольняє всі вимоги початкового технічного завдання, демонструє високу інженерну точність і є повністю готовим до практичного впровадження на реальному промисловому підприємстві.

## ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Tanenbaum A. S., Feamster N., Wetherall D. J. Computer Networks. 6th ed. Pearson, 2021. 960 p.
2. Буров Є. В. Комп'ютерні мережі: сучасні технології та архітектура : навч. посіб. Львів : Магнолія-2006, 2021. 412 с.
3. Кулаков Ю. О., Луцький Г. М. Комп'ютерні мережі : підручник. Київ : Книжковий дім, 2019. 405 с.
4. Логінова Н. І., Задерейко О. В., Толокнов А. А. Комп'ютерні мережі : навчальний посібник. Одеса : Фенікс, 2022. 249 с.
5. Kurose J. F., Ross K. W. Computer Networking: A Top-Down Approach. 8th ed. Pearson, 2021. 864 p.
6. IEEE 802.1Q-2022. IEEE Standard for Local and Metropolitan Area Networks—Bridges and Bridged Networks. IEEE, 2022. 2543 p.
7. IEEE 802.11-2020. IEEE Standard for Information Technology—Telecommunications and Information Exchange between Systems - Local and Metropolitan Area Networks—Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. IEEE, 2021. 4379 p. URL: <https://standards.ieee.org/ieee/802.11/7028/> (дата звернення: 20.05.2026).
8. Understand and Configure Spanning Tree Protocol (STP) : Cisco Technology Guide. Cisco Systems, 2024. URL: <https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/10556-16.html> (дата звернення: 20.05.2026).
9. Wireless LAN Controller (WLC) Configuration Guide : Cisco Catalyst 9800 Series. Cisco Systems, 2025. URL: <https://www.cisco.com/c/en/us/support/wireless/wireless-lan-controller-software/products-installation-and-configuration-guides-list.html> (дата звернення: 20.05.2026).

10. 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>

11. Литовченко М. С., Киричек Г. Г. Корпоративна мережа підприємства з інтеграцією бездротових технологій фіксованого зв'язку // 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.

Киричек Г.Г., Литовченко М.С., Тягунова М.Ю. Аналіз ефективності MPLS та Carrier Ethernet у магістральних мережах. Міжнародна науково-практична конференція “Взаємозв'язок науки, освіти та суспільства в умовах глобалізації: від теорії до практики”. (Ізмаїл, 8 трав. 2026). Ізмаїл, Україна, 2026. С.102-106. URL: <https://drive.google.com/file/d/1HhVMVsK7DBoqu9tq9d6NSOHKML5rKSHK/view>

## ДОДАТОК А

### ФУНКЦІОНАЛЬНА СХЕМА МЕРЕЖІ

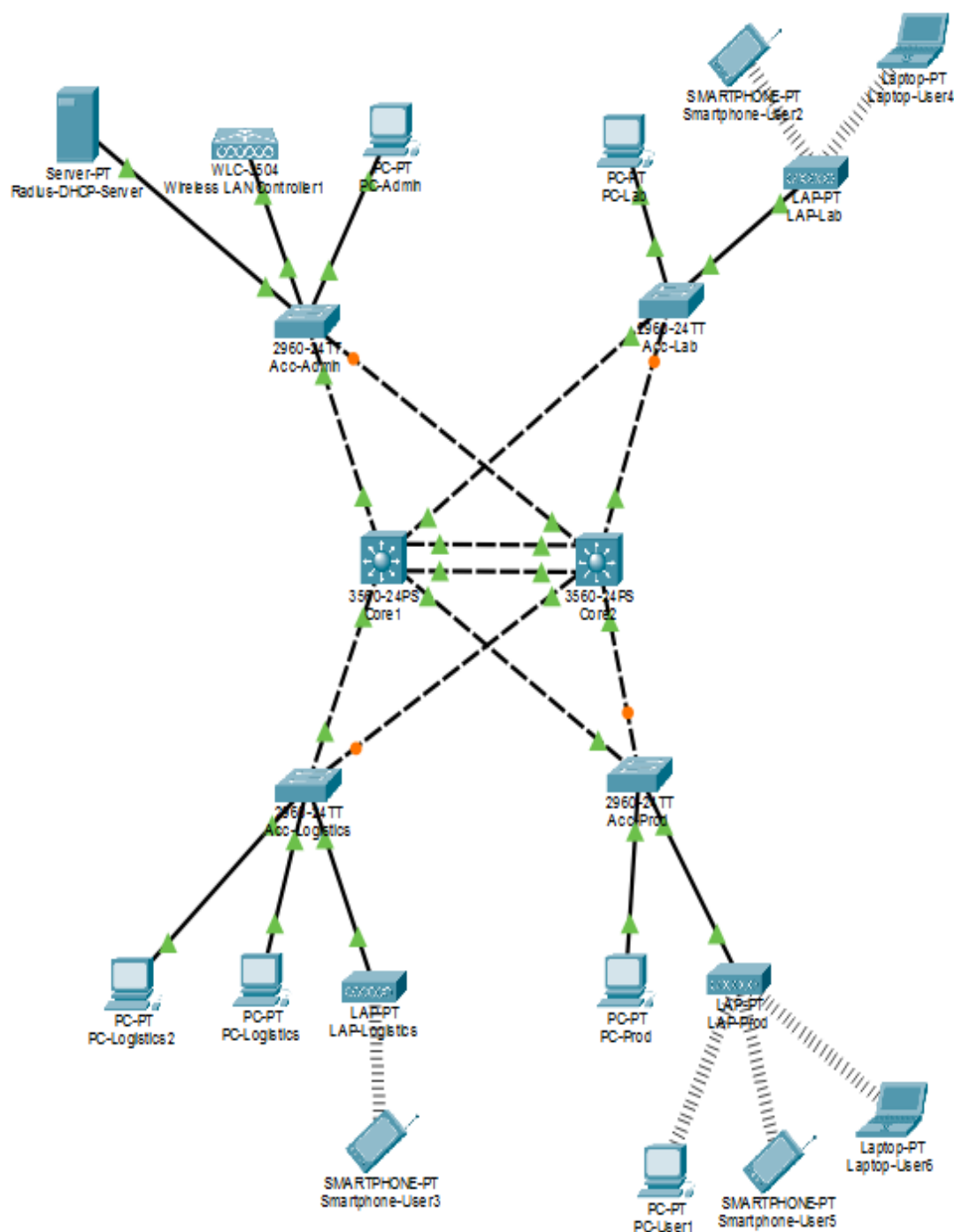


Рисунок А.1 – Функціональна схема мережі

ДОДАТОК Б

СХЕМА ПРИ'ЄДНУВАННЯ МЕРЕЖІ

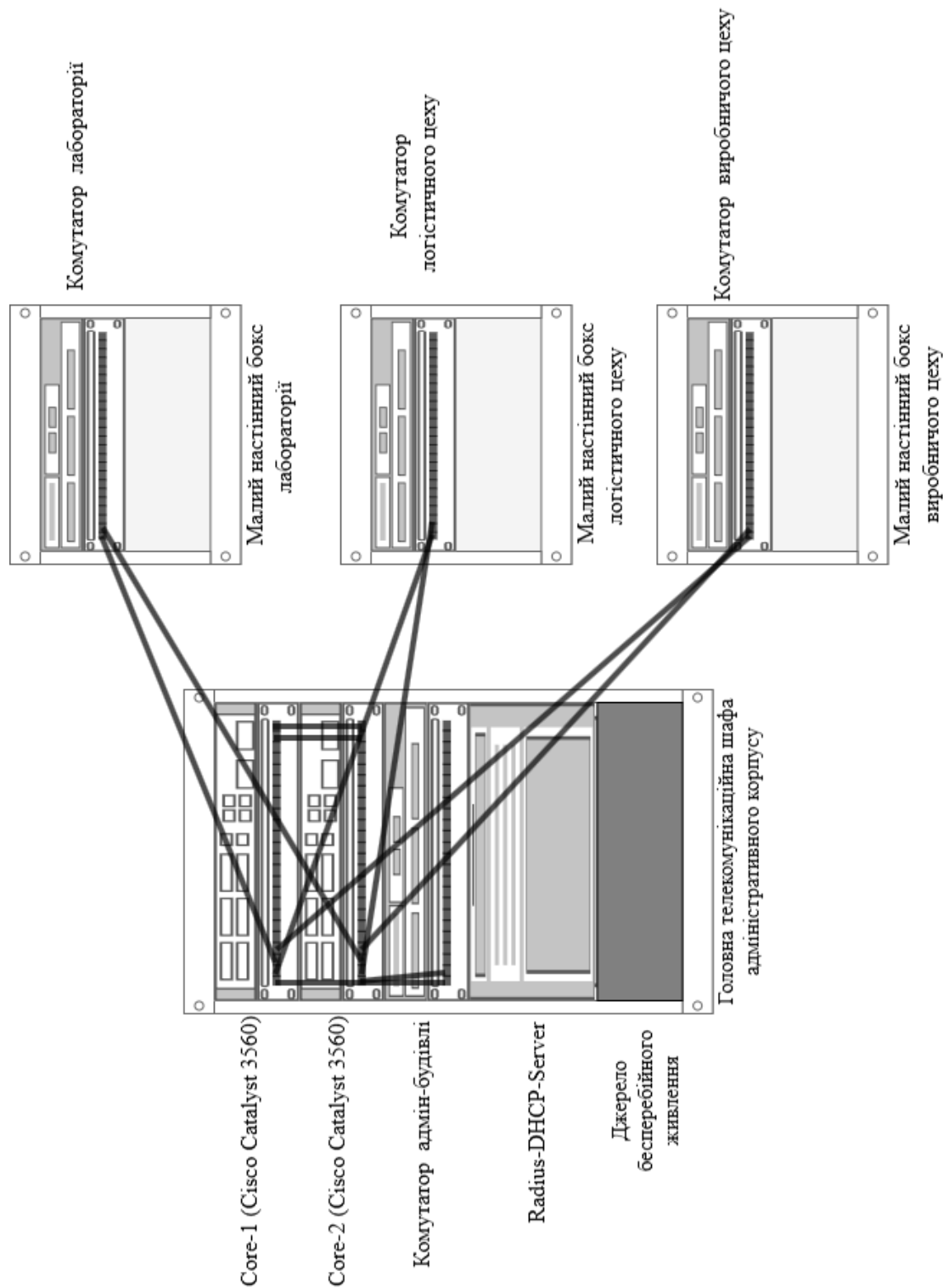


Рисунок Б.1 - Схема при'єднування мережі

ДОДАТОК В

СТРУКТУРНА СХЕМА МЕРЕЖІ

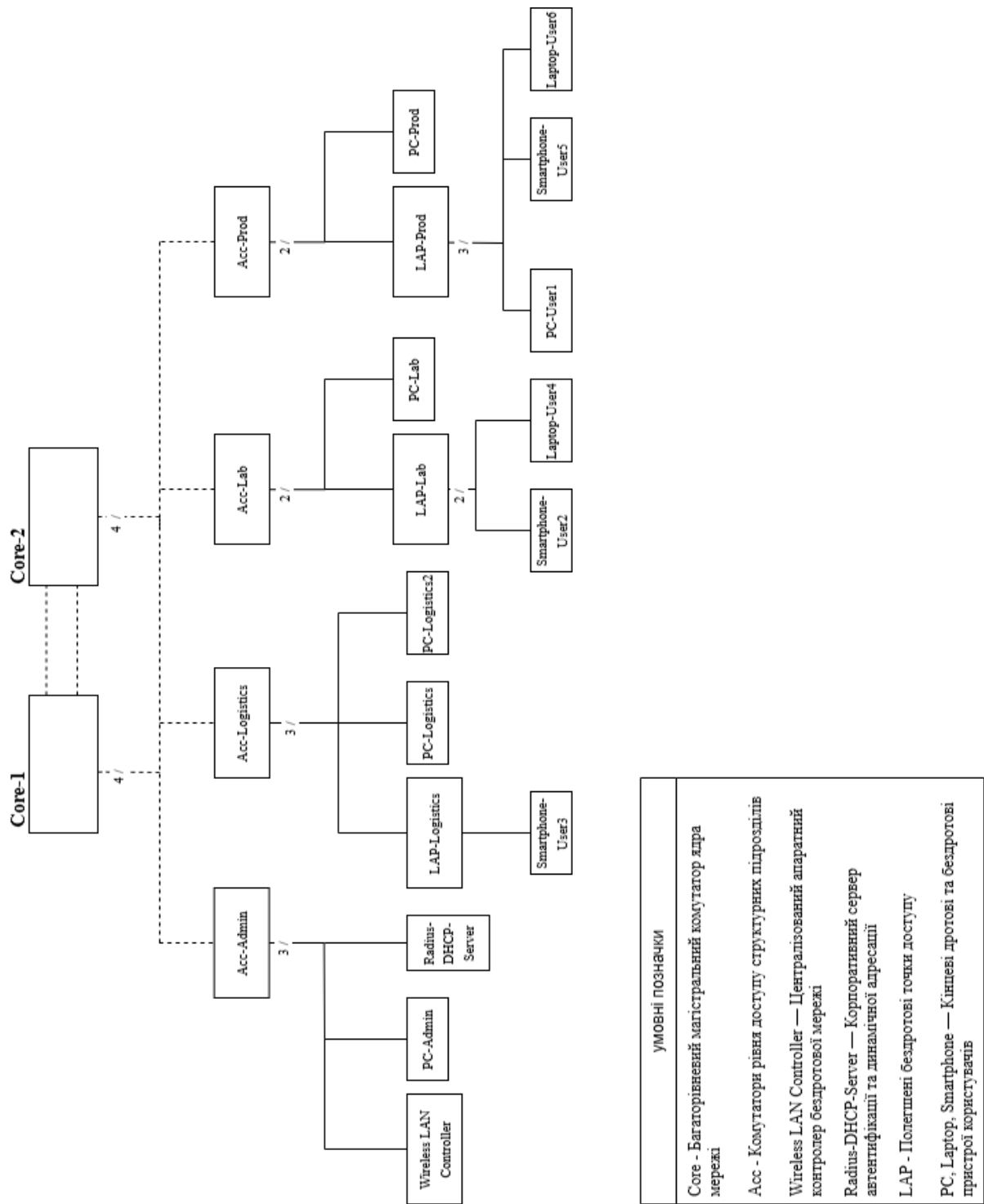


Рисунок В.1 – Структурна схема мережі

## ДОДАТОК Г

### СЛАЙДИ ПРЕЗЕНТАЦІЇ

#### ПРОЄКТУВАННЯ КОРПОРАТИВНОЇ МЕРЕЖІ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЙ ETHERNET ТА ЦЕНТРАЛІЗОВАНОЇ АРХІТЕКТУРИ WLAN

дипломна робота бакалавра

Виконав:

Максим ЛИТОВЧЕНКО

Студент КНТ-522

Керівник:

Галина КИРИЧЕК

Доцент, к.т.н.

Рисунок Г.1 – Слайд 1

#### **Мета та завдання дослідження**

**Мета роботи:** проєктування та логічна реалізація відмовостійкої мережевої інфраструктури з інтеграцією сучасних дротових і бездротових технологій зв'язку.

**Завдання дослідження:**

- Проаналізувати вимоги об'єкта та обґрунтувати вибір архітектури згорнутого ядра.
- Розробити схему логічної сегментації мережі на віртуальні локальні території VLAN.
- Спроєктувати систему централізованого управління бездротовим доступом на базі контролера WLC.
- Впровадити корпоративні механізми безпеки та автентифікації користувачів за стандартом 802.1X.
- Виконати імітаційне моделювання для комплексної верифікації працездатності мережевих сервісів.

Рисунок Г.2 – Слайд 2

## Актуальність

**Модернізація виробництва:** впровадження концепції індустрії чотири нуль вимагає безперервного та швидкого обміну даними між цехами, складами та диспетчерськими службами.

### ПРОБЛЕМИ ІСНУЮЧИХ МЕРЕЖ

- Висока вразливість до кібератак та несанкціонованого доступу.
- Відсутність підтримки безшовного роумінгу для мобільних вузлів.
- Значний час простою через відсутність резервних магістралей.
- Трудомістке адміністрування розрізнених мережевих сегментів.

### ЗАПРОПОНОВАНЕ ВИРІШЕННЯ

- Впровадження суворої автентифікації користувачів через RADIUS.
- Побудова безперервної бездротової інфраструктури на базі WLC.
- Гарантована відмовостійкість завдяки резервуванню ліній ядра.
- Централізоване управління та моніторинг всієї мережі.

Рисунок Г.3 – Слайд 3

## Опис об'єкта проектування

- **Характеристика об'єкта:** промисловий кампус із чотирма територіально розподіленими корпусами різного функціонального призначення.
- **Адміністративний корпус:** виконує роль центрального вузла управління, де зосереджено серверне обладнання та магістральні комутатори ядра.
- **Логістика та виробничі зони:** потребують створення безперервного бездротового покриття для стабільної роботи мобільних терміналів та систем автоматизації.
- **Науково-дослідна лабораторія:** вимагає підвищеного рівня логічної ізоляції трафіку та суворого розмежування прав доступу до внутрішніх ресурсів.

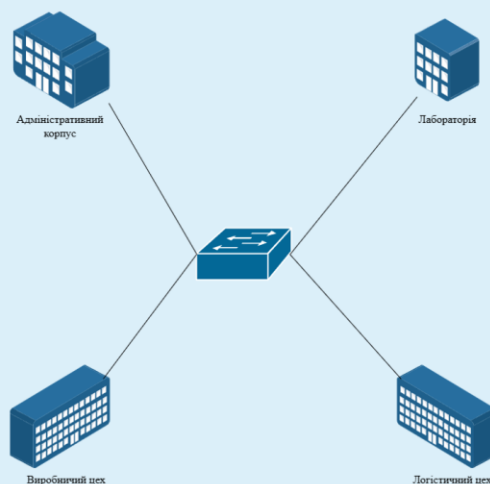


Рисунок Г.4 – Слайд 4

## Функціональна реалізація мережі

- **Архітектурна модель:** побудова інфраструктури за ієрархічним принципом Cisco із використанням згорнутого ядра.
- **Рівень ядра та агрегації:** два магістральні комутатори третього рівня Catalyst 3560, що працюють у режимі високої доступності для маршрутизації між VLAN.
- **Рівень доступу:** інтелектуальні комутатори другого рівня Catalyst 2960, розміщені у кожному корпусі для підключення кінцевих пристроїв та точок доступу.
- **Управління Wi-Fi:** використання апаратного контролера WLC для централізованого керування радіоефіром та CAPWAP-тунелями.

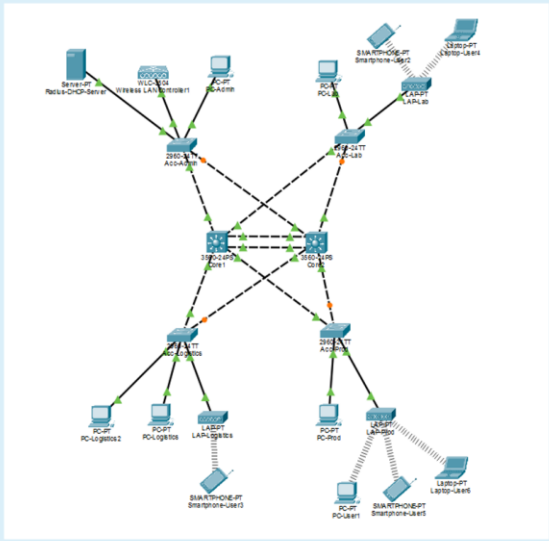


Рисунок Г.5 – Слайд 5

## Логічна сегментація та VLAN

**Метод організації:** розділення мережі підприємства на ізольовані ширококомовні домени для оптимізації трафіку та підвищення безпеки.

**Маршрутизація:** міждоменна комутація здійснюється на магістральному обладнанні ядра за допомогою віртуальних інтерфейсів шлюзів.

| ІДЕНТИФІКАТОР VLAN | НАЗВА СЕГМЕНТУ МЕРЕЖІ          | ДІАПАЗОН IP-АДРЕС |
|--------------------|--------------------------------|-------------------|
| VLAN 10            | Адміністративний корпус        | 192.168.10.0/24   |
| VLAN 20            | Логістика та склади            | 192.168.20.0/24   |
| VLAN 30            | Науково-дослідна лабораторія   | 192.168.30.0/24   |
| VLAN 40            | Виробничий цех                 | 192.168.40.0/24   |
| VLAN 50            | Корпоративна бездротова мережа | 192.168.50.0/24   |

Рисунок Г.6 – Слайд 6

## Бездротова інфраструктура та CAPWAP

- **Архітектура WLAN:** побудова бездротової мережі за технологією Light-weight Access Points (LAP) під управлінням центрального контролера WLC 3504.
- **Логічні тунелі:** весь трафік від бездротових клієнтів інкапсулюється в захищені тунелі CAPWAP та спрямовується безпосередньо на контролер.
- **Мобільність персоналу:** реалізація централізованого керування радіоефіром для забезпечення безшовного роумінгу при переміщенні між корпусами кампусу.
- **Сегментація Wi-Fi:** автоматичне перенаправлення бездротових пристроїв у виділену підмережу VLAN 50 з динамічним отриманням IP-адрес.

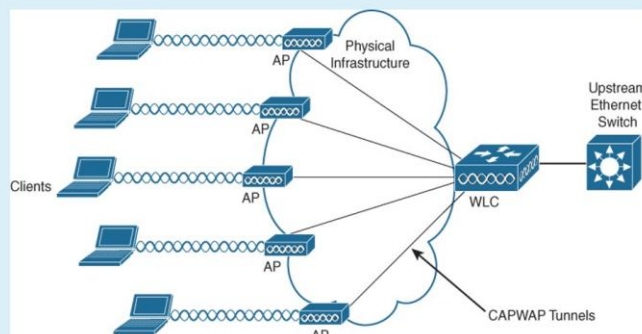


Рисунок Г.7 – Слайд 7

## Забезпечення мережевої безпеки

- **Стандарт захисту:** впровадження порт-орієнтованого контролю доступу IEEE 802.1X для захисту бездротового периметра кампусу.
- **Централізована архітектура AAA:** використання корпоративного сервера RADIUS як єдиної бази даних для автентифікації користувачів.
- **Алгоритм авторизації:** Клієнт надсилає запит на підключення до точки доступу LAP. Контролер WLC перенаправляє облікові дані на RADIUS-сервер. Після успішної верифікації клієнт отримує доступ та IP-адресу.
- **Результат:** надійний захист від несанкціонованого доступу та повна ізоляція службового трафіку підприємства.

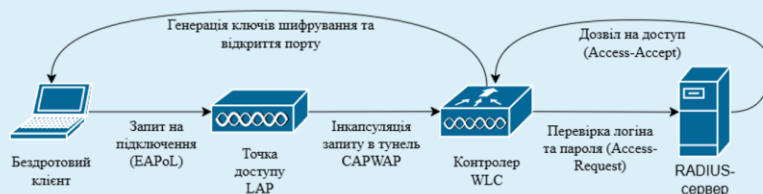


Рисунок Г.8 – Слайд 8

## Схема приєднування обладнання

- **Центральний комутаційний вузол:** встановлення головної телекомунікаційної шафи 42U в адміністративному корпусі для розміщення ядра мережі та серверів.
- **Компонування обладнання:** монтаж магістральних комутаторів Catalyst 3560, сервера RADIUS та контролера WLC за допомогою стандартних 19-дюймових кріплень.
- **Система життєзабезпечення:** інтеграція джерела безперебійного живлення (ДБЖ) для захисту активного обладнання від перепадів напруги та забезпечення автономної роботи.
- **Локальні вузли:** використання компактних настінних боксів (6U або 9U) у виробничих цехах та лабораторії для розміщення комутаторів рівня доступу та патч-панелей.

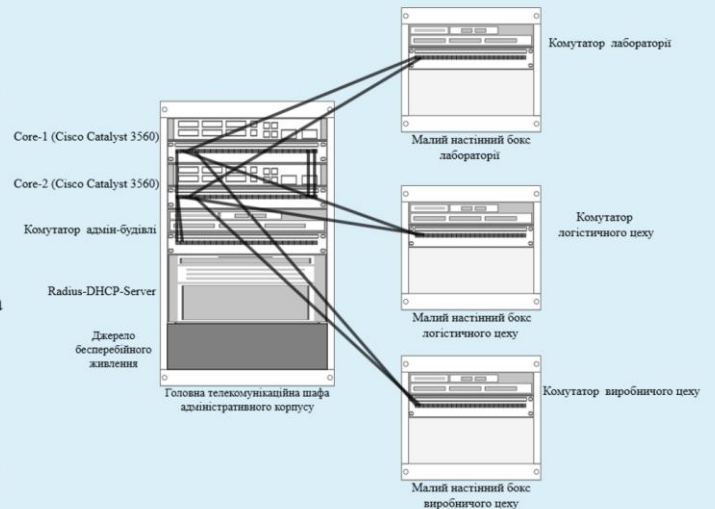


Рисунок Г.9 – Слайд 9

## Верифікація та тестування мережі

- **Метод перевірки:** проведення серії імітаційних тестів у середовищі Cisco Packet Tracer для аналізу зв'язності та коректності роботи служб.
- **Результати адресації:** підтвердження успішного отримання мережевих реквізитів (IP, Mask, Gateway) кінцевими пристроями через DHCP.
- **Міждоменна маршрутизація:** успішна верифікація доступності ресурсів між різними віртуальними сегментами кампусу за допомогою команди Ping.
- **Аналіз надійності:** підтвердження відмовостійкості системи при імітації розриву магістральних ліній зв'язку завдяки протоколам EtherChannel та STP.

```

Core-1#show etherchannel summary
Flags: D - down        P - in port-channel
       I - stand-alone  s - suspended
       R - Hot-standby (LACP only)
       L - Layer3       S - Layer2
       U - in use       f - failed to allocate aggregator
       u - unsuitable for bundling
       V - waiting to be aggregated
       d - default port

Number of channel-groups in use: 1
Number of aggregators: 1

Group  Port-channel  Protocol    Ports
-----
1      Po1(SU)           LACP       Gi0/1(P) Gi0/2(P)
Core-1#
  
```

Рисунок Г.10 – Слайд 10

## Висновки

- **Спроектовано та оптимізовано** ієрархічну архітектуру корпоративної мережі промислового кампусу на базі моделі згорнутого ядра Collapsed Core 3560 та комутаторів Catalyst 2960.
- **Реалізовано логічну сегментацію** адресного простору на п'ять ізольованих віртуальних мереж, що дозволило суттєво знизити широкомовний шторм та підвищити загальний рівень безпеки інформаційних ресурсів.
- **Впроваджено централізоване управління** бездротовим сегментом на базі контролера WLC 3504 та точок доступу LAP, що забезпечило підтримку безшовного роумінгу для бездротових пристроїв.
- **Забезпечено надійний захист** периметра мережі за допомогою розгортання порт-орієнтованого контролю доступу за стандартом IEEE 802.1X та корпоративного сервера автентифікації RADIUS AAA.
- **Проведено імітаційне моделювання** у середовищі Cisco Packet Tracer, результати якого повністю підтвердили відмовостійкість магістральних каналів та працездатність усіх налаштованих мережевих сервісів.



Рисунок Г.11 – Слайд 11

## Перелік публікацій

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. Литовченко М. С., Киричек Г. Г. Корпоративна мережа підприємства з інтеграцією бездротових технологій фіксованого зв'язку // *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., Литовченко М.С., Тягунова М.Ю. Аналіз ефективності MPLS та Carrier Ethernet у магістральних мережах. *Міжнародна науково-практична конференція “Взаємозв'язок науки, освіти та суспільства в умовах глобалізації: від теорії до практики”*. (Ізмаїл, 8 трав. 2026). Ізмаїл, Україна, 2026. С.102-106. URL: <https://drive.google.com/file/d/1HhVMVsK7DBoqu9tq9d6NSOHKMI5rKSHK/view> (тези)



Рисунок Г.12 – Слайд 12