Міністерство освіти і науки України

Луцький національний технічний університет
(повне найменування закладу вищої освіти)

Факультет комп'ютерних та інформаційних технологій
(повне найменування факультету)

Кафедра комп'ютерної інженерії та безпеки
(повне найменування кафедри)

КВАЛІФІКАЦІЙНА РОБОТА ЗА СТУПЕНЕМ ВИЩОЇ ОСВІТИ «БАКАЛАВР»

МОДЕРНІЗОВАНА КОМП'ЮТЕРНА МЕРЕЖА ГОТЕЛЬНОГО КОМПЛЕКСУ

MODERNISED COMPUTER NETWORK OF A HOTEL COMPLEX

спеціальність 123 Комп'ютерна інженерія
(шифр і назва спеціальності)

освітня програма Комп'ютерна інженерія
(назва освітньої програми)

Виконав: здобувач вищої освіти
групи КІс-21
Тарасевич Максим Олегович

(підпис)

Керівник: к.е.н., доцент
Гордєєва Дар'я Валеріївна

(підпис)

Кваліфікаційну роботу
допущено до захисту
« 12 » червня 2025 р.
Гарант освітньої програми:
к.т.н., доцент
Лавренчук Світлана Василівна

(підпис)

Луцьк – 2025 року

ЛУЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Факультет *комп'ютерних та інформаційних технологій*
Кафедра *комп'ютерної інженерії та безпеки*
Ступінь вищої освіти: *бакалавр*
Галузь знань: *12 Інформаційні технології*
Спеціальність: *123 Комп'ютерна інженерія*
Освітня програма: *«Комп'ютерна інженерія»*

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ доц. Т. Терлецький
« 10 » 01 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ ЗДОБУВАЧУ ВИЩОЇ ОСВІТИ

Тарасевичу Максиму Олеговичу
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи *Модернізована комп'ютерна мережа готельного комплексу*

Керівник роботи *к.е.н., доцент Гордєєва Дар'я Валеріївна*

затверджені наказом закладу вищої освіти від «04» січня 2025 року № 11/01-02
2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 10.06.2025р.

3. Вихідні дані до роботи *джерелом розробки є науково-технічна література та публікації в періодичних виданнях з даного питання, опубліковані зарубіжні та вітчизняні роботи в даній області та різні інтернет-ресурси технічного спрямування.*

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити):
Вступ
Аналіз завдання
Техніко-економічне обгрунтування
Налаштування обладнання
Висновки

5. Перелік графічного (ілюстративного) матеріалу:
Структура схема комп'ютерної мережі готелю
Схема логічного розподілу VLAN у мережі
Схема фізичного підключення комутаторів у 1-му та 2-му корпусах
Приклад підключення бездротової точки доступу до комутатора
Інтерфейс налаштування маршрутизатора (CLI/GUI)
Приклад виводу команди show vlan brief
Скріншоти налаштування SSH-доступу та банера MOHTD

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис	
		завдання видав	завдання прийняв
Аналіз завдання	*Гордєєва Д.В., доцент*		
Техніко-економічне обгрунтування	*Гордєєва Д.В., доцент*		
Налаштування обладнання	*Гордєєва Д.В., доцент*		
Нормоконтроль	*Багнюк Н.В., доцент*		
Гарант ОП	*Лавренчук С.В., доцент*		
Показник запозичень тексту	***___%***		
Академічна доброчесність	*Міскевич О.І.,ст.викладач*		

7. Дата видачі завдання 10.01.2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	*Огляд літератури із досліджуваної проблеми, аналіз проблемної області на наявних рішень*	до 10.02.2025 р.	Виконано
2.	*Аналіз завдання, техніко-економічне обгрунтування*	до 02.03.2025 р.	Виконано
3.	*Налаштування обладнання*	до 02.04.2025 р.	Виконано
4.	*Висновки та пропозиції*	до 10.04.2025 р.	Виконано
5.	*Формування списку використаних джерел*	до 15.04.2025 р.	Виконано
6.	*Формування додатків*	до 02.05.2025 р.	Виконано
7.	*Оформлення ілюстративного матеріалу*	до 10.05.2025 р.	Виконано
8.	*Представлення остаточного варіанту кваліфікаційної роботи керівникові*	до 15.05.2025 р.	Виконано
9.	*Нормоконтроль*	до 30.05.2025 р.	Виконано
10	*Інструментальна перевірка на академічний плагіат*	до 03.06.2025 р	Виконано
11.	*Здача кваліфікаційної роботи та всіх супровідних документів на кафедру*	до 10.06.2025 р.	Виконано

Здобувач вищої освіти _____ Тарасевич М.О.
(підпис) (прізвище, ініціали)

Керівник кваліфікаційної роботи _____ Горєєва Д.В.
(підпис) (прізвище, ініціали)

АНОТАЦІЯ

Тарасевич М. О. Модернізована комп'ютерна мережа готельного комплексу. Рукопис.

Кваліфікаційна робота бакалавра ОП «Комп'ютерна інженерія» спеціальності 123 Комп'ютерна інженерія. Луцький національний технічний університет. Луцьк, 2025.

Кваліфікаційна робота складається зі вступу, трьох розділів, висновків, списку використаних джерел та додатків. Перший розділ присвячений аналізу існуючої комп'ютерної мережі готельного комплексу «Сонячний берег» та обґрунтуванню необхідності її модернізації. Проведено детальне дослідження основних характеристик мережевої інфраструктури, виявлено її недоліки та обмеження. Сформульовано технічні вимоги до модернізованої мережі з урахуванням розширення кількості користувачів, зростання потреб структурних підрозділів, необхідності підвищення рівня безпеки, а також покращення можливостей моніторингу й адміністрування мережі.

Другий розділ присвячений проектуванню оновленої інфраструктури комп'ютерної мережі. Обґрунтовано вибір фізичної топології з використанням резервних каналів зв'язку, що забезпечує підвищену надійність функціонування мережі. Виконано розрахунки оптимального розміщення точок доступу для стабільного бездротового покриття на всій території готелю. Розроблено схему логічної адресації з використанням VLAN з метою розмежування трафіку між підрозділами, підвищення безпеки та забезпечення масштабування мережі. Обґрунтовано вибір мережевого обладнання відповідно до технічних вимог і функціональних потреб системи.

У третьому розділі розглянуто процес налаштування ключових мережевих сервісів. Зокрема, реалізовано VLAN для сегментації мережі й ізоляції трафіку між підрозділами, налаштовано DHCP-сервер для автоматичної видачі IP-адрес.

Ключові слова: комп'ютерна мережа, модернізація, VLAN, топологія, адресація, масштабування, резервування, трафік, протоколи.

ANNOTATION

Tarasevych M. Modernized computer network of a hotel complex. Manuscript.

Qualification work of a bachelor of the specialty "Computer Engineering" of the specialty 123 Computer Engineering. Lutsk National Technical University. Lutsk, 2025.

The qualification work consists of an introduction, three sections, conclusions, a list of sources used and appendices. The first section is devoted to the analysis of the existing computer network of the hotel complex "Sunny Beach" and the justification of the need for its modernization. A detailed study of the main characteristics of the network infrastructure was conducted, its shortcomings and limitations were identified. Technical requirements for the modernized network were formulated taking into account the expansion of the number of users, the growth of the needs of structural units, the need to increase the level of security, as well as improving the capabilities of monitoring and administering the network.

The second section is devoted to the design of the updated computer network infrastructure. The choice of physical topology using redundant communication channels is justified, which ensures increased reliability of network operation. Calculations of optimal placement of access points for stable wireless coverage throughout the hotel are performed. A logical addressing scheme using VLAN is developed to separate traffic between departments, increase security, and ensure network scalability. The choice of network equipment is justified in accordance with the technical requirements and functional needs of the system.

The third section considers the process of configuring key network services. In particular, VLAN is implemented for network segmentation and traffic isolation between departments, and a DHCP server is configured for automatic IP address assignment.

Keywords: computer network, modernization, VLAN, topology, addressing, scaling, redundancy, traffic, protocols.

ЗМІСТ

ВСТУП

У сучасному цифровому світі, де бізнес-процеси дедалі більше залежать від онлайн-інструментів, критично важливо мати надійну комп'ютерну мережу, яка гарантує безперебійний доступ до цифрових сервісів. Це особливо актуально для готелів, котрі залежать від якісного інтернет-з'єднання як для внутрішніх потреб персоналу, так і для надання клієнтам послуг найвищої якості. Стабільна та захищена мережева інфраструктура є фундаментом для функціонування численних сервісів, серед яких онлайн-бронювання, бездротовий доступ до інтернету, IP-телефонія та централізовані системи обліку.

Мета даної роботи полягає у модернізації комп'ютерної мережі для готельного комплексу «Сонячний берег». Така мережа повинна забезпечувати ефективну взаємодію між усіма підрозділами, високий рівень захисту даних та можливість масштабування для майбутнього зростання.

Об'єкт дослідження: комп'ютерна мережа готельного комплексу «Сонячний берег» та її інфраструктура.

Предмет дослідження: методи та засоби модернізації комп'ютерної мережі «Сонячний берег» з метою забезпечення надійної, продуктивної та безпечної роботи готельного комплексу з урахуванням специфіки його інфраструктури, вимог до безперебійної взаємодії між підрозділами та високих очікувань клієнтів щодо якості мережевого сервісу.

У межах даної кваліфікаційної роботи потрібно виконати насттупні завдання:

– здійснити аналіз поточного стану комп'ютерної мережі готельного комплексу «Сонячний берег» – дослідити наявну топологію, способи приєднання пристроїв, рівень безпеки й виявити критичні недоліки, які впливають на надійність та масштабованість мережі;

– сформувати вимоги до модернізованої мережі – визначити потреби всіх підрозділів, прогнозовані навантаження, потрібний рівень безпеки, резервування та централізованого адміністрування;

– здійснити аналіз інформаційних ресурсів та служб, та вибрати їх для використовуються в готелі, ідентифікувати критичні сервіси (сервери, Wi-Fi, IP-телефонію, локальні бази даних) та вимоги до їх підключення;

– обґрунтувати вибір фізичної топології, яка дозволить легко масштабувати інфраструктуру, забезпечити відмовостійкість та оптимізувати застосування обладнання;

– обчислити оптимальне розташування точок доступу з урахуванням плану будівлі, покриття, перешкоди та визначити місця їх встановлення для повного та стабільного сигналу на всій території;

– розробити логічну адресацію мережі та розділити мережу на VLAN-сегменти для окремих підрозділів, створити схему IP-адресації з урахуванням резерву та ізоляції;

– проаналізувати та обрати активне мережеве обладнання, яке підтримує VLAN, маршрутизацію, DHCP, SSH, STP та централізоване керування;

– налаштувати комутатори 2 та 3 рівнів – реалізувати резервування з’єднань (STP), базові налаштування VLAN, паролі, DHCP, а також обмеження доступу до мережевих пристроїв;

– організувати бездротовий доступ, створити гостьові VLAN та забезпечити стійке з’єднання для клієнтів.

РОЗДІЛ 1
АНАЛІЗ ЗАВДАННЯ

1.1 Аналіз поточного стану комп'ютерної мережі та виявлення її недоліків

Готельний комплекс «Сонячний берег» розташований у місті Ковель. Заклад надає повний спектр послуг для відпочинку та ділових подорожей, поєднуючи комфортні номери та сервіс високого рівня. Готель має рейтинг 4 зірки, що підтверджує його відповідність європейським стандартам якості в сфері готельного обслуговування.

Готель включає основний адміністративно-житловий корпус, у якому всі мережеві пристрої готелю об'єднані простою конфігурацією: від кожного офісу та від точок доступу WI-FI на 2 поверсі кабелі прямують безпосередньо до єдиного комутатора, що розміщений у серверній. До цього комутатора під'єднані всі комп'ютери, принтери та бездротові точки доступу.

Відсутність комутатора третього рівня та логічного сегментування призвели до того, що всі пристрої функціонують у спільному широкомовному домені. Це створює ризики безпеки: наприклад, комп'ютер фінансового відділу має повний доступ до ресурсів IT-відділу, що є неприйнятним у корпоративному середовищі. Основу безпеки становить ізоляція мережевого трафіку на фізичному рівні: кожен підрозділ має власне підключення через окремий порт комутатора. Для автоматичної видачі IP-адрес використовується протокол DHCP, що спрощує керування мережею.

Доступ до комутаторів здійснювався через Telnet, а всі паролі зберігалися в незашифрованому вигляді. Журналювання подій не було організовано – злом однієї точки доступу залишався би непоміченим. У деяких пристроях (маршрутизатор та комутатор) передбачено елементарний захист через паролі адміністратора, проте частіше за все вони залишаються стандартними або недостатньо складними.

На поточній стадії комп'ютерна мережа готелю збудована за фізичною

топологією «зірка». Всі кінцеві пристрої безпосередньо з'єднані з єдиним центральним комутатором TP-Link TL-SG1024D. Цей метод є звичайним для невеликих мереж, але він містить певні функціональні обмеження.

Центральним вузлом є один комутатор 2 рівня, до якого під'єднано все обладнання, зокрема:

– робочі станції адміністрації, IT-відділу, архіву, фінансового відділу та інших служб;

– сервер – підключено як звичайну робочу станцію;

– принтери – всі підключено до цього ж комутатора, без будь-якої логічної ізоляції;

– точки доступу Wi-Fi – забезпечують бездротове покриття, але також під'єднані до того ж комутатора, без окремого VLAN.

Використовуються застарілі моделі точок доступу моделі TP-Link TL-WR741ND, які не можуть похвалитися широкою зоною покриття (враховуючи перешкоди діапазон становить ~ 7-8 м.), швидкістю передачі даних (до 70 Мбіт/с), та й взагалі стабільним з'єднанням у всіх куточках. Результатом цього є «мертві зони» без сигналу, найчастіше – у віддалених офісах та кімнатах для гостей.

Протягом часу фізична структура точок доступу зазнала деградації, що зумовило проблеми зі стабільністю, перериванням та з'єднанням. Експлуатація застарілого обладнання не забезпечує необхідної масштабованості мережі та знижує загальну ефективність роботи мережі.

Існуюче обладнання створює перешкоди для впровадження нових послуг, а також не забезпечує потрібну гнучкість при розширенні мережі. Як наслідок, навіть незначні зміни в структурі готелю, або збільшення числа пристроїв зможуть призвести до потреби перебудови схеми з'єднання із самого початкуч.

План приміщення та комп'ютерна мережа готельного комплексу зображено на рисунку 1.1.

Рисунок 1.1 – План приміщення

Площа кабінетів та кількість працівників описана у таблицях 1.1-1.2.

Таблиця 1.1 – Площа кабінетів та кількість працівників 1 поверху

Назва кабінету	Довжина кабінету, м	Ширина кабінету, м	Кількість працівників
Ресепшен	12	10	1
Адміністрація	12	6	5
Архів	12	7,5	2
Серверна	7	4	–
Кабінет директора	7	10	1
IT	10,5	7	4
Фінанси	7	7	2

Таблиця 1.2 – Площа кабінетів та кількість працівників 2 поверху

Номер готелю	Довжина кабінету, м	Ширина кабінету, м
1	2	3
№1	9	10

Продовження таблиці 1.2

1	2	3
№2, №3, №4	5,3	12
№5, №6, №7, №8	6	7
№9	6,5	7

Наявна мережева інфраструктура готелю базується на застарілих підходах, не маючи логічного розподілу трафіку між відділами. Усі пристрої функціонують в одному широкомовному домені, що збільшує вірогідність витоку інформації та утруднює контроль над доступом. Відсутність сегментації мережі, як приклад використання – VLAN, не надає ефективної ізоляції критичних служб, таких як бухгалтерські комп'ютери та точки доступу, що може спровокувати розповсюдження вірусів чи здійснення атак у межах усієї мережі.

1.2 Формування вимог до модернізованої комп'ютерної мережі

У зв'язку із розширенням діяльності готелю, було ухвалено рішення щодо відкриття філіалу, що знаходиться орієнтовно за 80 метрів від головної споруди. Новий корпус призначений для розміщення додаткових гостьових номерів, а також приміщень для адміністративних потреб. Це сприятиме не тільки збільшенню числа відвідувачів, але й покращенню рівня комфорту надання послуг та розділенню функціональних зон готелю. Через це виникла потреба у побудові нової локальної мережі з подальшою інтеграцією в існуючу інфраструктуру для забезпечення повноцінної взаємодії між усіма компонентами готельної системи. Не було впроваджено сегментацію VLAN, що створювало потенційні ризики для безпеки мережевого трафіку та ускладнювало обслуговування.

Оновлена площа приміщень корпусу 1 подана в таблицях 1.3-1.4.

Таблиця 1.3 – Корпус 1, поверх1

Назва кабінету	Довжина кабінету, м	Ширина кабінету, м	Кількість працівників
Ресепшен	12	10	1
IT-відділ	12	6	5
Архів	12	7,5	2
Серверна	7	4	–
Кабінет директора	7	10	1
Кімната відпочинку	11,5	7	–

Таблиця 1.4 – Корпус 1, поверх 2

Номер готелю	Довжина кабінету, м	Ширина кабінету, м
№1	9	10
№2, №3, №4	5,3	12
№5, №6, №7, №8	6	7
№9	6,5	7

У структурі комплексу передбачено наявність ще одного окремого корпусу, призначеного для розміщення додаткових гостьових номерів та адміністративно-господарських приміщень.

Корпус розташований на відстані ~ 80 м. від основного, що визначає необхідність побудови каналу зв'язку між ними для забезпечення повноцінної взаємодії між усіма елементами мережі. Площа кабінетів та кількість працівників описані у таблицях 1.5-1.6.

Таблиця 1.5 – Корпус 2, поверх1

Назва кабінету	Довжина кабінету, м	Ширина кабінету, м	Кількість працівників
Ресепшен	14,5	10	1
Приймальня	8	7,5	1
Кабінет директора	8	9,5	1
Відділ фінансів	7	8	2
Адміністрація	9,5	6,5	2
Сервер	9,5	3,5	–
Логістика	7	8	2

Таблиця 1.6 – Корпус 2, поверх 2

Номер готелю	Довжина кабінету, м	Ширина кабінету, м
№1	10	12
№2	6,5	7
№3-№12	5,5	7

Відповідно до виявлених недоліків та обґрунтувань комп'ютерна мережа готельного комплексу «Сонячний берег» має відповідати таким критеріям:

– використовувати L3-комутатори для забезпечення міжмережевої взаємодії та маршрутизації між корпусами готелю. Це забезпечить кращу масштабованість та швидкість обробки трафіку, на відміну від класичних маршрутизаторів, які мають нижчу продуктивність при великій кількості підмереж;

– реалізувати сегментацію VLAN – для кожного підрозділу виділяється окрема віртуальна мережа, порти access/trunk налаштовуються відповідно до призначення. Це дозволить ізолювати трафік між службами, покращити безпеку та знизити навантаження на мережу;

– реалізувати централізоване адміністрування усіх мережевих пристроїв. Це забезпечить спрощення обслуговування, швидке впровадження змін та зменшення кількості помилок при налаштуванні;

– оновити застаріле Wi-Fi-обладнання до сучасного стандарту Wi-Fi 6. Це забезпечить високу швидкість, кращу якість з'єднання та підтримку великої кількості пристроїв одночасно;

– забезпечити безшовне Wi-Fi-покриття стандарту Wi-Fi 6 з ізоляцією гостьової мережі від службової. Це дозволить гарантувати високу швидкість, зменшення перешкод та підтримку більшої кількості пристроїв;

– передбачити резервування критичних елементів мережі, включно з комутаторами, зв'язками та джерелами живлення. Це на дасть гарантію стійкісті мережі до збоїв;

– застосувати системи контролю доступу, захищений протокол SSH v2, шифрування конфігурацій, централізоване журналювання через syslog. Це

дозволить забезпечити належний рівень інформаційної безпеки та швидке реагування на інциденти;

– вимкнути неактивні порти та на робочих – увімкнути PortFast для зменшення часу підключення. Це зменшить поверхню атаки і пришвидшить старт роботи кінцевих пристроїв.

1.3 Опис інформаційних ресурсів та служб

Серед сервісів з обмеженим доступом, що будуть використовуватися в мережі готельного комплексу, важливу роль відіграватимуть протоколи DHCP, SSH та STP. Вони забезпечують автоматичне налаштування мережевих параметрів та централізоване ведення журналів подій, що сприяє ефективному адмініструванню, діагностиці та безпеці мережі.

DHCP (Dynamic Host Configuration Protocol) – це мережевий протокол, призначений для автоматичного надання IP-адрес та інших параметрів конфігурації пристроям, які під'єднуються до мережі. Основна функція DHCP полягає в усуненні необхідності ручного налаштування IP-адрес на кожному пристрої, що особливо актуально у великих мережах з великою кількістю кінцевих точок. DHCP дозволяє динамічно призначати адреси на основі визначених пулів, уникаючи конфліктів адрес та полегшуючи обслуговування мережі.

Процес роботи DHCP складається з кількох етапів:

– DHCP Discover – коли пристрій (DHCP-клієнт) підключається до мережі, він транслює широкомовний запит, щоб відшукати DHCP-сервер;

– DHCP Offer – сервер відповідає, пропонуючи вільну IP-адресу та відповідні параметри (маску, шлюз, DNS);

– DHCP Request – клієнт підтверджує бажання прийняти запропоновану конфігурацію;

– DHCP Acknowledgment – сервер підтверджує виділення адреси, і клієнт починає її використовувати.

У розгорнутій мережі DHCP налаштовано на багатофункціональних комутаторах L3 типу Multilayer-SW1 та Multilayer-SW2. Для кожної VLAN створено окремий DHCP pool із чітко визначеним діапазоном адрес, шлюзом і DNS-сервером. Це дозволяє автоматично конфігурувати пристрої в адміністрації, логістиці, фінансах, гостьових зонах та ін. без залучення адміністратора [1]

Secure Shell (SSH) − це криптографічний мережевий протокол, розроблений для безпечного зв'язку через незахищену мережу.

Він широко використовується для віддаленого входу, виконання команд та передачі даних між комп'ютерами. SSH забезпечує безпечний канал через незахищену мережу, шифруючи дані, що обмінюються між клієнтом і сервером.

SSH пропонує низку функцій, які роблять його незамінним інструментом для безпечного зв'язку та віддаленого доступу. Деякі з ключових функцій включають:

– шифрування: SSH шифрує всі дані, що передаються між клієнтом і сервером, гарантуючи конфіденційність конфіденційної інформації та захист від прослуховування;

– автентифікація: SSH підтримує кілька методів автентифікації, включаючи автентифікацію на основі пароля, автентифікацію з відкритим ключем та багатофакторну автентифікацію;

– цілісність даних: SSH забезпечує цілісність за допомогою криптографічних хеш-функцій для перевірки того, що дані не були підроблені під час передачі;

– переадресація та тунелювання: SSH дозволяє переадресовувати портації та тунелювання, забезпечуючи безпечний доступ до служб, які працюють на віддалених серверах;

– безпечна передача файлів: SSH підтримує протоколи безпечної передачі файлів, такі як SCP (Secure Copy) та SFTP (SSH File Transfer Protocol) для безпечної передачі файлів між комп'ютерами;

– переадресація X11: SSH дозволяє безпечно переадресовувати

сеанси X11, що дозволяє віддаленим графічним програмам безпечно працювати на локальному комп'ютері;

– стиснення: SSH може стискати дані перед передачею, зменшуючи обсяг даних, що передають мережу, та підвищуючи продуктивність.

Його надійне шифрування, гнучкі методи автентифікації та універсальні функції створюють його стандартом для безпечного віддаленого адміністрування, передачі файлів та автоматизованих завдань.

Дотримуючись інструкцій з налаштування, розширених конфігурацій, найкращих практик безпеки та порядку щодо усунення несправностей, викладених у цьому посібнику, ви можете використовувати весь потенціал SSH для покращення робочого процесу та захисту своїх систем.

Якщо SSH продовжує розвиватися та адаптуватися до нових викликів безпеки та технологічних досягнень, він залишатиметься критично важливим компонентом безпечного обчислення [2].

Протокол STP – це мережевий протокол, який забезпечує топологію без петель для будь-якої локальної мережі Ethernet, підключеної через мости. Це означає, що він запобігає сценарію, коли пакети даних можуть потрапити в нескінченну петлю, нескінченно циркулюючи по мережі. STP був стандартизований IEEE як IEEE 802.1D.

Процес роботи протоколу STP передбачає такі етапи:

1) першим кроком у протоколі Spanning Tree є вибір кореневого мосту, який є основною опорною точкою мережі. Вважайте кореневим мостом штаб-квартиру компанії. Цей кореневий міст є місцем, де всі інші комутатори (гілки) шукають найефективніші шляхи. Ідентифікатор мосту: Ідентифікатор мосту є специфічним для кожного комутатора. Кореневий міст – це комутатор з найнижчим ідентифікатором мосту;

2) після вибору кореневого мосту протокол використовує принцип вартості, щоб знайти найкоротший шлях від кожного комутатора до кореневого мосту. Вартість шляху – бажані високошвидкісні лінії, оскільки вони мають меншу вартість;

3) після цього протокол STP підтримує працездатність резервних шляхів, намагаючись запобігти будь-яким надлишковим шляхам, які можуть призвести до утворення петель. Він досягає цього, блокуючи певні порти, що запобігає пересиланню фреймів даних на користь прослуховування змін у мережі [3].

У мережі готелю «Сонячний берег» протокол STP активовано на всіх комутаторах доступу та магістральної частини. Це забезпечує формування безциклової топології з резервними каналами зв'язку між корпусами й комутаторами різного рівня. У результаті у разі аварії критичних лінків система автоматично активує резервне з'єднання, що гарантує безперервність дротових і бездротових сервісів без втручання адміністратора.

У поєднанні, DHCP, SSH та STP утворюють потужний інструмент для побудови масштабованої, безпечної та автоматизованої мережі готельного комплексу.

РОЗДІЛ 2
ТЕХНІКО-ЕКОНОМІЧНЕ ОБГРУНТУВАННЯ

2.1 Обґрунтування фізичної топології комп'ютерної мережі

Топологія мережі стосується розташування або структури різних елементів комп'ютерної мережі, включаючи вузли, такі як комп'ютери, маршрутизатори та комутатори, а також з'єднання між ними. Вона визначає, як пристрої з'єднані між собою та як дані передаються в мережі і є критичним фактором, що визначає як продуктивність, так і надійність мережі.

Існує декілька поширених типів мережевих топологій, включаючи шинну, зірку, кільце, сітчасту, деревоподібну та гібридну, кожна з яких має свої сильні та слабкі сторони. Вибір топології безпосередньо впливає на ключові аспекти мережі, такі як швидкість передачі даних, масштабованість та простота обслуговування. Наприклад, у зірковій топології всі пристрої підключені до центрального концентратора, що спрощує керування, але потенційно обмежує продуктивність, якщо центральний концентратор стає вузьким місцем. Навпаки, сітчаста топологія забезпечує високу резервування та відмовостійкість, але може стати складною та дорогою в обслуговуванні в міру зростання мережі.

Зіркові топології використовуються найчастіше, оскільки ви можете керувати всією мережею з одного місця: центрального комутатора. Як наслідок, якщо вузол, який не є центральним, вийде з ладу, мережа залишатиметься працездатною. Це надає зірковим топологіям рівень захисту від збоїв, які не завжди присутні в інших топологіях.

Що стосується фізичної структури мережі, зіркові топології потребують менше кабелів, ніж інші типи топологій. Це спрощує їх налаштування та управління в довгостроковій перспективі. Простота загальної конструкції мережі значно полегшує адміністраторам усунення несправностей під час вирішення проблем із продуктивністю мережі [4].

Топологія «Зірка», яка використовувалась в готелі зображено на рисунку 2.1.

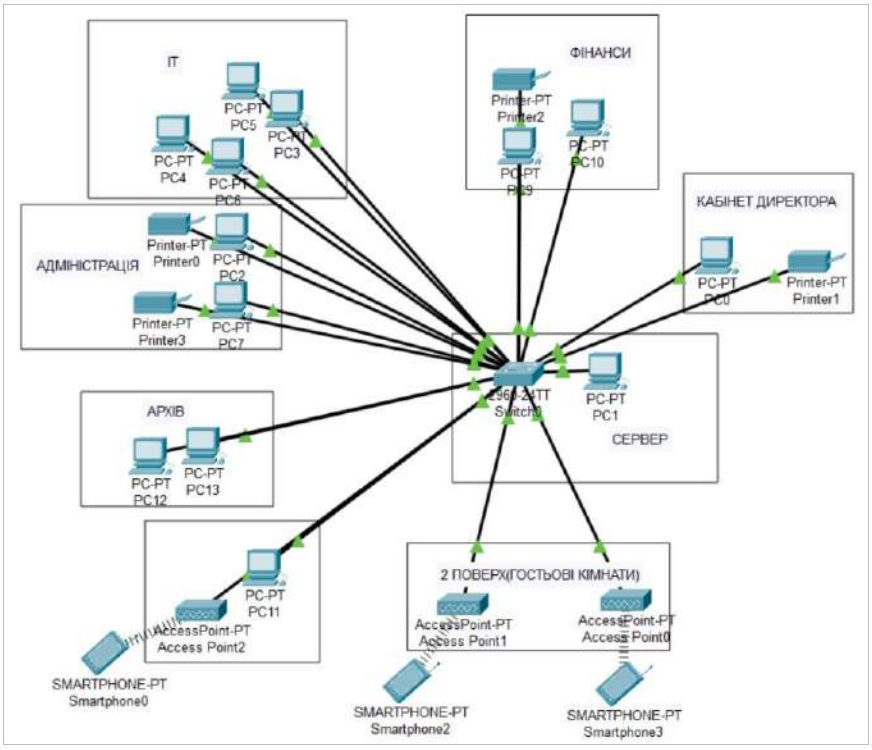

Рисунок 2.1 – Топологія «Зірка»

На основі аналізу наявного стану комп'ютерної мережі та беручи до уваги технічні й функціональні потреби до її модернізації, було обрано ієрархічну топологію типу «розширена зірка» (рис. 2.2).

Структура фізичної мережі поділяється довкола трьох типів обладнання:

– комутатори другого рівня – забезпечать підключення робочих місць, принтерів, камер тощо;

– комутатор третього рівня – буде виконувати роль агрегатора й маршрутизатора між VLAN сегментами, зводячи трафік від усіх L2-комутаторів. Таким чином він буде поєднувати функції розподільного й частково ядрового рівня;

– маршрутизатор буде виконувати роль шлюза у зовнішні мережі й забезпечуватиме доступ до Інтернету та віддалених сервісів.

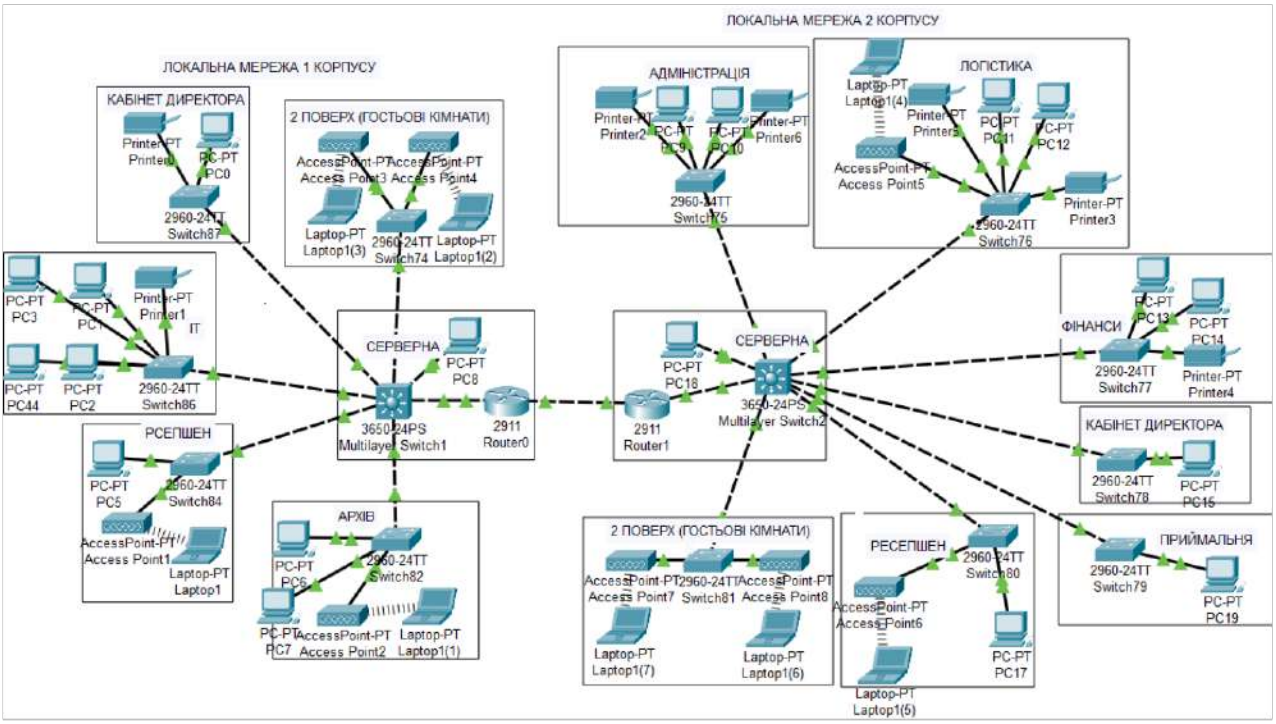

Рисунок 2.2 – Топологія «розширена зірка»

У такій конфігурації мережа зберігає ключові переваги ієрархічної топології – чіткий розподіл на логічні частини, зручність розширення та централізоване адміністрування – за мінімальної кількості мережних пристроїв.

Головними вимогами до мережі, які зумовили вибір топології, є:

– забезпечення надійного дротового з’єднання для стаціонарних пристроїв у службових приміщеннях (ПК, принтери, точки доступу);

– підключення двох фізично віддалених корпусів до єдиної мережної інфраструктури;

– централізоване адміністрування через серверну;

– резервування каналів зв’язку між головними мережевими вузлами;

– логічне розділення трафіку (гостьові номери, адміністративні кабінети, фінанси, тощо) через VLAN;

– масштабованість з урахуванням можливості добудови приміщень або розширення функціоналу.

2.2 Розрахунки оптимального розташування точок доступу Wi-Fi

Для забезпечення стабільного Wi-Fi покриття в межах приміщення 1 корпусу готелю площею 22×30,5 м та 2 корпусу готелю площею 22×40 м потрібно виконати розрахунок реальної дальності зв'язку, використовуючи модель точки доступу моделі Ubiquiti UniFi U6+.

Розрахунки втрат у вільному просторі проводяться за формулою (2.1) [5]:

$$FSL = 33 + 20\,(\lg F + \lg D), \tag{2.1}$$

де FSL (втрати у вільному просторі, дБ) – це ступінь загасання сигналу під час його проходження через відкритий простір без перешкод. Він залежить від частоти передачі (F, МГц) та відстані між передавачем і приймачем (D, км).

SOM (System Operating Margin) – запас енергії радіозв'язку (у дБ), що гарантує стабільну роботу системи в умовах впливу зовнішніх чинників (перешкод, загасання, коливань рівня сигналу тощо). Враховує можливі фактори негативно впливають на дальність зв'язку, такі як:

– температурний дрейф чутливості приймача та вихідної потужності передавача;

– всілякі погодні аномалії: туман, сніг, дощ;

– неузгодженість антени приймача, передавача до антенно-фідерним трактом.

Wcp – загасання сигналу в стінах, величина загасань у залежності від середовища поширення сигналу наведено в таблиці 2.1 [5].

Таблиця 2.1 – Величина загасання сигналу в різних середовищах

Назва	Од. вим.	Значення
Склопакет/вікно	дБ	6
Стіна (бетон, цегла)	дБ	10
Двері	дБ	7

Далі потрібно підставити вихідні дані і розрахувати дальність зв'язку при використанні ноутбука. У даному випадку швидкість передачі даних складає від 1 Мб/с до 100 Мб/с чутливість приймача, буде наступною. Залежність чутливості від швидкості передачі даних зазначено в таблиці 2.2.

Таблиця 2.2 – Залежність чутливості від швидкості передачі даних

Потужність передатчика	Швидкість	Pt (дБм)	Pmin (дБм)
23 dBm	1 Мбіт/с	23	-92
23 dBm	6 Мбіт/с	23	-90
23 dBm	11 Мбіт/с	23	-85
22 dBm	54 Мбіт/с	22	-72
21 dBm	108 Мбіт/с	21	-68

Розрахунки FSL визначаються за допомогою сумарного посилення системи проводяться за допомогою формули (2.2) [5]:

$$FSL = P_{t,дБ} - P_{\min,дБ} - G_{t,дБ} + G_{r,дБ} - W_{АФТпрд,дБ} - W_{АФТпрм,дБ} - SOM, \quad (2.2)$$

де Pt – це потужність сигналу, котрий передається (у дБ);

Pmin – найменший рівень сигналу, який здатний розпізнати приймач за заданої швидкості передачі;

Gt та Gr – коефіцієнти підсилення відповідно передавальної та приймальної антен, котрі показують, наскільки ефективно антени спрямовують або приймають сигнал (у дБ);

WАФТпрд (дБ) – втрати сигналу у передавальному тракті, котрі включають загасання в коаксіальному кабелі та роз'ємах обчислюють за формулою (2.3) [5]:

$$WАФТ_{прд} = \alpha \times l, \quad (2.3)$$

де α = 1 дБ/м – питомі втрати в кабелі;

WАФТпрм − втрати сигналу в коаксіальному кабелі і роз'єми приймального тракту;

WАФТпрм = 0, внаслідок близькості до пристрою антени;

WАФТпрд = 1 дБ/м*3=3дБ;

WAФТпрм – втрати на приймальному боці дорівнюють нулю, оскільки антена розміщена безпосередньо біля приймача.

Розрахунок втрат у вільному просторі зазначено в таблиці 2.3.

Таблиця 2.3 – Розрахунок FSL

Швидкість передавання	Формула FSL	FSL, дБ
1 Мбіт/с	23 - (-92) - 12 + 4 - 3 - 0 - 15	89
6 Мбіт/с	23 - (-90) - 12 + 4 - 3 - 0 - 15	87
11 Мбіт/с	23 - (-85) - 12 + 4 - 3 - 0 - 15	82
54 Мбіт/с	22 - (-72) - 12 + 4 - 3 - 0 - 15	68
108 Мбіт/с	21 - (-68) - 12 + 4 - 3 - 0 - 15	63

Розрахунки дальності виконуються за формулою (2.4) [5]:

$$D=10(FSL/20-33/20-LG*F). \quad (2.4)$$

Розрахунок відстані між передавачем і приймачем зазначено в таблиці 2.4.

Таблиця 2.4 – Розрахунок дальності

Швидкість передачі	FSL	D = 10^{(FSL/20 – 5,03)}	D (м)
1 Мбіт/с	96	10^(4,8 - 5,03) = 10^-0,23	~590 м
6 Мбіт/с	94	10^(4,7 - 5,03) = 10^-0,33	~470 м
11 Мбіт/с	90	10^(4,5 - 5,03) = 10^-0,53	~295 м
54 Мбіт/с	72	10^(3,6 - 5,03) = 10^-1,43	~37 м
108 Мбіт/с	71	10^(3,55 - 5,03) = 10^-1,48	~33 м

Із урахуванням типових втрат у стінах (близько 10 дБ на кожну), реальний радіус стабільного покриття з високою швидкістю зменшується до 10-12 метрів.

Плани корпусів готельного комплексу з накладеними радіусами дії точок доступу зображено на рисунках 2.3-2.4.

Рисунок 2.3 – План об’єкта 1 корпусу

Рисунок 2.4 – План об’єкта 2 корпусу

2.3 Розрахунок логічної адресації

Під час сегментування мережі кожен структурний підрозділ готелю отримав власну підмережу. Кожна підмережа була призначена для окремого VLAN, що покращує управління трафіком, підвищує безпеку та дозволяє об'єднувати віддалені хости. У межах проекту побудови модернізованої комп'ютерної мережі готельного комплексу було реалізовано 14 окремих VLAN (табл. 2.5-2.6), кожна з яких відповідає певному функціональному підрозділу в одному з двох корпусів. Сегментування мережі таким чином дозволяє досягнути:

– логічної ізоляції трафіку між підрозділами;

– спрощення адміністрування;

– гнучкості у розширенні та обслуговуванні мережі.

Таблиця 2.5 – Створення VLAN для корпусу 1

VLAN ID	Назва VLAN	Підрозділ
1	2	3
10	SW-ARCHIVE	Архів
20	SW-RECEPTION1	Ресепшен
30	VLAN-IT	IT-відділ
40	SW-DIRECTOR	Кабінет директора
50	SW-GUEST	Гостьові кімнати
60	SW-SERVER	Серверна

Таблиця 2.6 – Створення VLAN для корпусу 2

VLAN ID	Назва VLAN	Підрозділ
70	SW-ADMINISTRATION	Адміністрація
80	VLAN-LOGISTICS	Логістика
90	VLAN-FINANCE	Відділ фінансів
120	VLAN-GUEST	Гостьові кімнати
130	VLAN-PRYYMALNYA	Приймальня
110	VLAN-RECEPTION	Ресепшен
120	VLAN-GOUST	Гостьові кімнати
140	VLAN-SERVER	Серверна

Таке сегментування дозволить підтримувати принцип мінімально доступу (least privilege), підвищити контроль над трафіком і реалізувати політики безпеки

відповідно до потреб кожного підрозділу.

Для кожного приміщення було здійснено розрахунок кількості необхідних IP-адрес(табл. 2.7-2.8), що враховує кількість інформаційних розеток, коефіцієнт запасу та службову адресу.

Таблиця 2.7 – Маска IP мережевих сегментів, корпус 1

Назва приміщення	К-сть IP адрес вузлів, H2 (H2=R+0,5R+1)	Кількість бітів-вузла, h	IP маска мережевого сегменту (/n=32-h)
Ресепшен	4	5	/27
IT-відділ	10	5	/27
Архів	5	5	/27
Серверна	3	5	/27
Кабінет директора	4	5	/27

Таблиця 2.8 – Маска IP мережевих сегментів, корпус 2

Назва приміщення	К-сть IP адрес вузлів, H2 (H2=R+0,5R+1)	Кількість бітів-вузла, h	IP маска мережевого сегменту (/n=32-h)
Ресепшен	5	5	/27
Приймальня	4	5	/27
Кабінет директора	4	5	/27
Відділ фінансів	7	5	/27
Адміністрація	8	5	/27
Сервер	3	5	/27
Логістика	10	5	/27

Під час розрахунків логічної адресації було проведено сегментування мережі з адресою 10.13.0.0/16 (табл. 2.9) на функціональні блоки підмереж для корпусів, а також для серверів обмеженого та загального доступу.

Таблиця 2.9 – Сегментація загальної мережі 10.13.0.0/16 по масці /27

Номер підмережі	IP-адреса підмережі, /24	Призначення підмережі
1	2	3
0		Зарезервована

Продовження таблиці 2.9

1	2	3
1	10.13.101.0 - 10.13.106.0	Підмережі корпусу 1 (Wi-Fi гостьовий, архів, ресепшен, директор, серверна, IT)
2	10.13.201.0 - 10.13.207.0	Підмережі корпусу 2 (адміністрація, логістика, фінанси, директор, ресепшен, Wi-Fi гостьовий, приймальня)
3	10.13.192.0	Сегмент Wi-Fi доступу
4		Зарезервована

2.4 Аналіз варіантів технічних засобів телекомунікацій

Для побудови мережі необхідне відповідне апаратне забезпечення, яке відповідає вимогам, встановленим у завданні. До нього входять такі телекомунікаційні пристрої:

– маршрутизатор;

– комутатор 3 рівня;

– комутатори 2 рівня моделі OSI;

– безпровідна точка доступу.

Таблиця 2.10 містить порівняльний аналіз технічних характеристик бездротових точок доступу TP-Link EAP615-Wall і Ubiquiti UniFi U6+, які можуть бути використані у мережі.

Таблиця 2.10 – Порівняльна характеристика точок доступу WI-FI

Характеристика	TP-Link EAP615-Wall	Ubiquiti UniFi U6+
1	2	3
Швидкість передачі даних	До 2,4 Гбіт/с (Wi-Fi 6)	До 3 Гбіт/с (Wi-Fi 6)
Стандарти Wi-Fi	IEEE 802.11a/b/g/n/ac/ax	IEEE 802.11a/b/g/n/ac/ax
Кількість антен	2 вбудовані (MU-MIMO)	4 внутрішніх (2x2 + 2x2 MU-MIMO)
Ethernet портів	1 × 2,5 Гбіт/с (RJ-45 PoE)	1 × 1 Гбіт/с (RJ-45 PoE)

Продовження таблиці 2.10

1	2	3
Максимум клієнтів	До ~100 (оцінка виробника)	До ~300 одночасних користувачів (оцінка)
Безпека	WPA3, WPA2, 802.1X, Captive Portal	WPA3, WPA2, 802.1X, наскрізна автентифікація
Управління	Безкоштовний хмарний контролер Omada	Локальне/хмарне через UniFi Controller
Вартість	4599 ₴	4932 ₴

Обидва пристрої повністю відповідають бюджетному обмеженню (до 5 000 грн), мають високий рейтинг серед користувачів та підтримують актуальні протоколи безпеки (WPA3, 802.1X). З урахуванням ціни, функціоналу та масштабованості, було впровадження Ubiquiti UniFi U6+ як базового рішення для більшості зон покриття готельної мережі (рис. 2.5).

Рисунок 2.5 – Точка доступу Ubiquiti UniFi U6+ [6]

Комутатор третього рівня – це спеціальний тип мережевого пристрою, який здатний виконувати функції двох рівнів моделі OSI , тобто канального рівня (рівень 2) та мережевого рівня (рівень 3). Простими словами, комутатор третього рівня – це мережевий пристрій, який може виконувати комутацію (функції рівня 2), а також маршрутизацію (функції рівня 3). Він здатний з’єднувати пристрої, що знаходяться в одній підмережі або одній VLAN

(віртуальній локальній мережі), для обміну інформацією з дуже високою швидкістю, що є роботою традиційного комутатора, а також можна підключати пристрої з різних підмереж та вмикати деякі протоколи маршрутизації, які є роботою маршрутизатора [7].

Таблиця 2.11 містить порівняльний аналіз технічних характеристик комутаторів 3 рівня Ubiquiti USW-24-POE і Ruijie RG-NBS5200-24GT4XS, які можуть бути використані.

Таблиця 2.11 – Порівняльна характеристика комутаторів 3 рівня

Характеристика	Ubiquiti USW-24-POE	Ruijie RG-NBS5200-24GT4XS
Кількість портів	24	24
Швидкість передачі даних	10/100/1000 Мбіт/с	10/100/1000 Мбіт/с
Швидкість передачі даних між комутаторами	До 70 Гбіт/с	До 128 Гбіт/с (Stacking через 10G SFP+)
Підтримка стандартів безпеки	802.1X, ACL, DHCP Snooping, IGMP, Port Isolation	802.1X, ACL, DHCP Snooping, IP Source Guard, Private VLAN
Можливість розширення мережі	Ні, стекування не підтримується	Так, підтримка стекування (до 8 комутаторів)
Підтримка VLAN	Так, до 4096 VLAN	Так, до 4096 VLAN
Підтримка протоколів маршрутизації	Статична маршрутизація, Inter-VLAN, DHCP Relay	Статична маршрутизація, RIP, OSPF
Управління	CLI, SNMP, UniFi Controller (локальне/хмарне)	CLI, SNMP, Web GUI, Ruijie Cloud
Характеристика	Ubiquiti USW-24-POE	Ruijie RG-NBS5200-24GT4XS
Вартість	18465 ₴	19 550 ₴

Ці два комутатори мають схожі базові характеристики, однак Ubiquiti USW-24-POE (рис. 2.6) забезпечує більшу практичність для використання в готельному середовищі завдяки вбудованій підтримці PoE, зручному централізованому управлінню через UniFi Controller та простій інтеграції з іншими мережевими пристроями. Додатково комутатор підтримує базові функції маршрутизації третього рівня, необхідні для сегментації трафіку в

локальній мережі. Завдяки цим перевагам дана модель була обрана для використання як центральний комутатор у магістральній частині мережі.

Рисунок 2.6 – Комутатор 3 рівня Ubiquiti USW-24-POE [8]

Комутатор 2-го рівня – це мережевий пристрій, який працює на канальному рівні (рівень 2) моделі OSI. Він використовує MAC-адреси (Media Access Control – керування доступом до середовища) для пересилання даних між пристроями в одному сегменті мережі, по суті функціонуючи як багатопортовий міст. Комутатори 2-го рівня призначені для покращення продуктивності мережі шляхом зменшення колізій та створення окремих доменів колізій для кожного підключеного пристрою [9].

Таблиця 2.12 містить порівняльний аналіз технічних характеристик комутаторів TP-Link TL-SG1218MP і TP-Link TL-SG2016P, які можуть бути використані у мережі.

Таблиця 2.12 – Порівняльна характеристика комутаторів 2 рівня

Характеристика	TP-Link TL-SG1218MP	TP-Link TL-SG2016P
1	2	3
Кількість портів	18	16
Швидкість передачі даних	10/100/1000 Mbps	10/100/1000 Mbps
Керування мережею	Smart-керований	Smart-керований
Мережеві протоколи	TCP/IP, IEEE 802.3, 802.3u, 802.3ab, 802.3af, 802.3at, 802.1Q, 802.1p, 802.3x	TCP/IP, IEEE 802.3, 802.3u, 802.3ab, 802.3af, 802.3at, 802.1Q, 802.1p, 802.3x
Таблиця адресів MAC	8K записів	8K записів

Продовження таблиці 2.12

1	2	3
Широкомовність і керування потоками	Підтримується	Підтримується
VLAN	Підтримується	Підтримується
Типи кабелів	Ethernet/Fast/Gigabit Ethernet (10/100/1000Base-T)	Ethernet/Fast/Gigabit Ethernet (10/100/1000Base-T)
Буферна пам’ять	4,1 МБ	4,1 МБ
Розміри	29,4 x 18 x 4,4 см	29,4 x 18 x 4,4 см
Вартість	8 599 ₴	6 999 ₴

Після проведення аналізу технічних характеристик обраних комутаторів було прийнято рішення зупинитися на TP-Link TL-SG2016P (рис. 2.7), оскільки цей пристрій має оптимальне співвідношення ціни та функціональності. Комутатор підтримує технологію PoE+, базове мережеве керування, VLAN та QoS, що дозволяє ефективно реалізувати сегментацію мережі та підключення пристроїв, таких як точки доступу або IP-камери, без додаткових інжекторів живлення. Його параметри найкраще відповідають вимогам проектованої мережі готельного комплексу.

Рисунок 2.7 – Комутатор TP-Link TL-SG2016P [10]

Таблиця 2.13 містить порівняльний аналіз технічних характеристик маршрутизаторів від фірм Ubiquiti та MikroTik, які можуть бути використані у комп’ютерній мережі.

Таблиця 2.13 – Порівняльна характеристика маршрутизаторів

Характеристика	Ubiquiti EdgeRouter ER-12	MikroTik RB4011iGS+5HacQ2HnD-IN
Кількість портів	10	10
Швидкість передачі даних	До 6.8 Gbps (1518 байт) / 3.4 Mpps (64 байт)	До ~2.6 Gbps
Керування мережею	EdgeOS CLI / Web UI / UISP	RouterOS CLI / WebFig
Підтримка протоколів маршрутизації	OSPF, RIP, BGP, VLAN, ACL, NAT, IPSec	OSPF, RIP, VLAN, ACL, NAT, IPSec
Широкомовність та керування потоками	IGMP Snooping, QoS / CoS	Auto MDI/X, switch-chip QoS
Підтримка VLAN	Так, до 4096 VLAN	Так, до 4096 VLAN
Типи кабелів	RJ-45 (Cat5e/6), SFP	RJ-45, SFP+, Auto MDI/X
Буферна пам’ять	1 GB DDR3 + 4 GB eMMC + 8 MB SPI	1 GB RAM + 512 MB NAND
Вартість	10113 ₴	10565 ₴

Після проведення аналізу технічних характеристик обраних маршрутизаторів було обрано маршрутизатор Ubiquiti EdgeRouter ER-12 (рис. 2.8), як оптимальне рішення. Він забезпечує високу продуктивність, надійну маршрутизацію, підтримку до 12 портів та розширене керування, що повністю відповідає потребам готельної мережі в межах бюджету.

Рисунок 2.8 – Маршрутизатор Ubiquiti EdgeRouter ER-12 [11]

2.5 Вибір активного мережевого обладнання

Вибір відповідного активного мережевого обладнання має першорядне значення для гарантування стійкості, продуктивності та безпеки вашої комп'ютерної мережі. Якщо застосовувати техніку, яка не відповідає потребам навантаження або не підтримує актуальні стандарти, це може призвести до затримок при передачі даних, втрати пакетів та частих перебоїв зі з'єднанням. Крім того, морально застаріле обладнання зазвичай не отримує оновлень безпеки, що робить мережу вразливою перед сучасними кібератаками. Таким чином, інвестиції в передову мережеву інфраструктуру є не лише технічним, але й стратегічним рішенням для кожної організації [12].

Відповідно до вимог комп'ютерної мережі та фізичної топології, для забезпечення ефективного функціонування обчислювальної мережі необхідно правильно вибрати мережеве обладнання для корпусів.

Перелік активного мережевого обладнання корпусу 1 представлено в таблиці 2.14.

Таблиця 2.14 – Перелік активного мережевого обладнання, корпус 1

Поверх/ Зона	Назва приміщення	Мережеве обладнання, модель
1	Ресепшен	TP-Link TL-SG2016P
		Ubiquiti UniFi U6+
1	Архів	TP-Link TL-SG2016P
		Ubiquiti UniFi U6+
1	Кабінет директора	TP-Link TL-SG2016P
1	Серверна	Ubiquiti USW-24-POE
		Ubiquiti EdgeRouter ER-12
1	Відділ IT	Cisco WS-C2960-24LT-L
2	Коридор	Cisco WS-C2960-24LT-L
		Ubiquiti UniFi U6+

Перелік активного мережевого обладнання корпусу 2 представлено в таблиці 2.15.

Таблиця 2.15 – Перелік активного мережевого обладнання, корпус 2

Поверх/ Зона	Назва приміщення	Мережеве обладнання, модель
1	Адміністрація	TP-Link TL-SG2016P
1	Логістика	TP-Link TL-SG2016P
		Ubiquiti UniFi U6+
1	Фінанси	TP-Link TL-SG2016P
1	Кабінет директора	TP-Link TL-SG2016P
1	Приймальня	TP-Link TL-SG2016P
1	Ресепшен	TP-Link TL-SG2016P
		Ubiquiti UniFi U6+
1	Сервер	Ubiquiti USW-24-POE
		Ubiquiti EdgeRouter ER 12
2	Коридор	TP-Link TL-SG2016P
		Ubiquiti UniFi U6+

Загальна кількість мережевого обладнання для об’єктів:

– 8 точок безпровідового доступу Ubiquiti UniFi U6+;

– 2 комутатори Ubiquiti USW-24-POE;

– 2 маршрутизатора Ubiquiti EdgeRouter ER 12;

– 12 комутаторів Cisco Catalyst TP-Link TL-SG2016P.

РОЗДІЛ 3
ОБЛАДНЕННЯ ТА НАЛАШТУВАННЯ

3.1 Комутація

3.1.1 Базові налаштування комутаторів

Комутація мережі – це процедура пересилання пакетів до пункту призначення. Коли дані досягають порту, це називається вхідним, тоді як дані, що виходять з порту, – вихідним. Як правило, у великих мережах існують різні шляхи від передавача до приймача. Тому найкращий маршрут для передачі даних визначається методом комутації.

Кожен із трьох типів мережевої комутації має свої переваги та недоліки, і найкращий з них залежить від конкретних потреб і характеристик мережі та даних, що передаються.

Комутація каналів може забезпечити високоякісні, передбачувані з'єднання, але вона також може бути неефективною та дорогою.

Комутація пакетів широко використовується в сучасних мережах і ефективна для передачі даних пакетами, але вона може бути вразливою до перевантажень та затримок.

Комутація повідомлень трапляється рідко і зазвичай використовується лише в спеціалізованих застосуваннях, таких як військові або наукові мережі, де надійність важливіша за швидкість [13].

Нижче наведено набір команд та для базових налаштувань комутатора Multilayer-SW1 (рис. 3.1-3.4).

```
SW-IT>en
Password:
SW-IT#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW-IT(config)#hostname SW-IT
SW-IT(config)#!
SW-IT(config)#enable secret hoteladmin
SW-IT(config)#no ip domain-lookup
```

Рисунок 3.1 – Налаштування доступу

```
SW-IT(config)#line con 0
SW-IT(config-line)# password hoteladmin
SW-IT(config-line)# login
SW-IT(config-line)#!
SW-IT(config-line)#line vty 0 4
SW-IT(config-line)# password hoteladmin
SW-IT(config-line)# login local
SW-IT(config-line)# transport input ssh
SW-IT(config-line)# exec-timeout 5 0
```

Рисунок 3.2 – Налаштування паролів

```
Multilayer-SW1>en
Password:
Multilayer-SW1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Multilayer-SW1(config)#ip dhcp pool WIFI-LAN
Multilayer-SW1(dhcp-config)# network 10.13.193.0 255.255.255.0
Multilayer-SW1(dhcp-config)# default-router 10.13.193.254
Multilayer-SW1(dhcp-config)#
```

Рисунок 3.3 – Налаштування DHCP pool

```
SW-RECEPTION(config-if-range)#ip domain-name hotel.local
SW-RECEPTION(config)#ip ssh version 2
Please create RSA keys (of at least 768 bits size) to enable SSH v2.
SW-RECEPTION(config)#ip ssh authentication-retries 2
SW-RECEPTION(config)#ip ssh time-out 15
SW-RECEPTION(config)#username admin privilege 15 secret hoteladmin
```

Рисунок 3.4 – Налаштування SSH доступу

Таким чином можна налаштовувати як комутатори так і маршрутизатори.

Застосування технології VLAN (віртуальних локальних мереж) дозволяє логічно розділити фізичну мережу, об’єднуючи обладнання в окремі групи, не зважаючи на їх фізичне розміщення. Цей підхід забезпечує ефективну організацію мережевої інфраструктури, бо зменшує обсяг широкомовного трафіку та сприяє покращенню управління потоками даних. Більше того, VLAN відіграє значну роль у підвищенні безпеки: завдяки ізоляції між сегментами стає можливим обмежити доступ до ресурсів тільки для авторизованих користувачів,

а також застосовувати диференційовані політики контролю доступу.

Окремі VLAN мають можливість отримувати власні параметри якості обслуговування (QoS), що дає змогу пріоритезувати певні типи трафіку, як-от голосовий чи службовий. Це позитивно впливає на загальну продуктивність мережі та покращує користувацький досвід, незалежно від навантаження в інших частинах інфраструктури [14].

За допомогою наступних команд налаштовується VLAN на обладнані CISCO (рис. 3.5).

```
Multilayer-SW1(config)#interface range GigabitEthernet1/0/1
Multilayer-SW1(config-if-range)# description TRUNK to SW-ARCHIVE
Multilayer-SW1(config-if-range)# switchport mode trunk
Multilayer-SW1(config-if-range)# switchport trunk allowed vlan 101,701
Multilayer-SW1(config-if-range)#!
Multilayer-SW1(config-if-range)#interface GigabitEthernet1/0/2
Multilayer-SW1(config-if)# description TRUNK to SW-RECEPTION
Multilayer-SW1(config-if)# switchport mode trunk
Multilayer-SW1(config-if)# switchport trunk allowed vlan 102,701
Multilayer-SW1(config-if)#!
Multilayer-SW1(config-if)#interface GigabitEthernet1/0/3
Multilayer-SW1(config-if)# description TRUNK to SW-IT
Multilayer-SW1(config-if)# switchport mode trunk
Multilayer-SW1(config-if)# switchport trunk allowed vlan 103
```

Рисунок 3.5 – Налаштування VLAN

Схема розподілу VLAN мережі готелю розписана у таблиці 3.10.

Таблиця 3.10 – Схема розподілу VLAN

Діапазон VLAN	Призначення VLAN
101 - 106	Провідні користувацькі сегменти, корпус 1
107 - 110	Провідні користувацькі сегменти, корпус 2
701	Сегмент бездротового доступу (Wi-Fi)
702	Сегмент серверів загального доступу
703	Сегмент серверів обмеженого доступу
704 - 709	Сегменти з’єднань мережевих пристроїв

Налаштовані VLAN в сегменті мережі корпусу 1 зображено на рисунку 3.6.

```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gig1/0/7, Gig1/0/9, Gig1/0/10, Gig1/0/11
                                                Gig1/0/12, Gig1/0/13, Gig1/0/14, Gig1/0/15
                                                Gig1/0/16, Gig1/0/17, Gig1/0/18, Gig1/0/19
                                                Gig1/0/20, Gig1/0/21, Gig1/0/22, Gig1/0/23
                                                Gig1/1/1, Gig1/1/2, Gig1/1/3, Gig1/1/4
101  ARCHIVE                          active    Gig1/0/1
102  RECEPTION                        active    Gig1/0/2
103  IT                               active    Gig1/0/3
105  DIRECTOR                         active    Gig1/0/4
106  GUEST                            active    Gig1/0/5
110  ADMIN-PC                         active    Gig1/0/6
703  SERVER-LINK                      active    Gig1/0/8
```

Рисунок 3.6 – Налаштовані VLAN 1 корпусу

Налаштовані VLAN в сегменті мережі корпусу 2 зображено на рисунку 3.7.

```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gig1/0/14, Gig1/0/15, Gig1/0/16, Gig1/0/17
                                                Gig1/0/18, Gig1/0/19, Gig1/0/20, Gig1/0/21
                                                Gig1/0/22, Gig1/0/23, Gig1/1/1, Gig1/1/2
                                                Gig1/1/3, Gig1/1/4
110  VLAN0110                         active
120  GUEST_WIFI_2_CORPUS              active    Gig1/0/12
201  ADMIN-2                          active    Gig1/0/6
202  LOGISTICS                        active    Gig1/0/7
203  FINANCE                          active    Gig1/0/8
205  DIRECTOR-2                       active    Gig1/0/9
206  RECEPTION-2                      active    Gig1/0/10
207  INTAKE                           active    Gig1/0/11
701  WIFI                             active    Gig1/0/13
```

Рисунок 3.7 – Налаштовані VLAN 2 корпусу

3.3.2 Налаштування протоколу резервування з’єднань

Для стабільної роботи мережевої інфраструктури у великих будівлях, наприклад, у готельних комплексах, критично важливо передбачити резервні канали зв’язку. Вони автоматично залучаються у випадку збою основних з’єднань. Це дозволяє уникнути перебоїв у роботі та гарантує високу доступність послуг [15].

Враховуючи можливу надлишковість фізичних з’єднань між комутаторами, ключовим є уникнення петель у топології. Для цього

використовують Spanning Tree Protocol (STP). Він автоматично обчислює оптимальний шлях і блокує інші, забезпечуючи безпечну та безперебійну передачу кадрів. Це набуває особливого значення у багатошарових мережах, де кількість комутаторів та з'єднань між ними вважаються значними [16].

Налаштування порту для точки доступу Wi-Fi з увімкненим STP PortFast на комутаторі логістичного відділу (рис. 3.8).

```
SW-LOGISTICS(config-if-range)#! === WiFi Access Point VLAN 701 ===
SW-LOGISTICS(config-if-range)#interface FastEthernet0/6
SW-LOGISTICS(config-if)# description Logistics-WiFi-AP
SW-LOGISTICS(config-if)# switchport mode access
SW-LOGISTICS(config-if)# switchport access vlan 701
SW-LOGISTICS(config-if)# spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface  when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/6 but will only
have effect when the interface is in a non-trunking mode.
SW-LOGISTICS(config-if)# no shutdown
```

Рисунок 3.8 – Використання протоколу STP

3.2 Організація безпровідноного доступу

Бездротові мережі надають бізнесу значні переваги, оптимізуючи операції та підвищуючи гнучкість. Завдяки бездротовим рішенням співробітники можуть підключатися з будь-якої точки офісу, покращуючи продуктивність та співпрацю. Від підвищеної мобільності до економії коштів, бездротові мережі підвищують ефективність бізнесу та сприяють зростанню.

Однією з основних переваг бездротових мереж є можливість підвищення ефективності бізнесу. Завдяки бездротовій мережі співробітники можуть вільно переміщатися по робочому простору, залишаючись підключеними до критично важливих систем і даних. Така мобільність забезпечує швидший зв'язок і співпрацю, оскільки члени команди можуть отримувати доступ до ресурсів, не будучи прив'язаними до конкретного столу чи комп'ютера. Незалежно від того,

чи вони отримують доступ до хмарних програм, чи співпрацюють над спільними документами, чи спілкуються з віддаленими колегами, бездротові мережі оптимізують робочі процеси та зменшують час простою, що підвищує загальну продуктивність [17].

Для підключення точок доступу використовуються L2-комутатори, зокрема SW-GOUST (рис. 3.9), а маршрутизація та керування IP-адресами забезпечується на багаторівневому комутаторі Multilayer-SW2 (рис. 3.10). Для гостьової Wi-Fi мережі було виділено VLAN 120 та IP-підмережу 10.13.224.0/27.

Більшість сучасних точок доступу налаштовуються за допомогою графічного інтерфейсу (веб-сторінки або програми).

Однак нижче подано загальні кроки та команди налаштування, які можуть застосовуватися до більшості точок доступу (рис. 3.9-3.11).

```
Multilayer-SW2>en
Password:
Multilayer-SW2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Multilayer-SW2(config)#vlan 120
Multilayer-SW2(config-vlan)# name GUEST_WIFI_2_CORPUS
Multilayer-SW2(config-vlan)#
Multilayer-SW2(config-vlan)#interface Vlan120
Multilayer-SW2(config-if)# description GUEST_WIFI_SEGMENT
Multilayer-SW2(config-if)# ip address 10.13.224.1 255.255.255.224
Multilayer-SW2(config-if)# ip access-group BLOCK-GUEST in
Multilayer-SW2(config-if)# no shutdown
Multilayer-SW2(config-if)#
Multilayer-SW2(config-if)#ip dhcp pool GUEST_WIFI_2_CORPUS
Multilayer-SW2(dhcp-config)# network 10.13.224.0 255.255.255.224
Multilayer-SW2(dhcp-config)# default-router 10.13.224.1
Multilayer-SW2(dhcp-config)# dns-server 8.8.8.8
Multilayer-SW2(dhcp-config)#
Multilayer-SW2(dhcp-config)#ip access-list extended BLOCK-GUEST
Multilayer-SW2(config-ext-nacl)# deny ip 10.13.0.0 0.0.255.255 any
Multilayer-SW2(config-ext-nacl)# permit ip any any
```

Рисунок 3.9 – Налаштування комутатора Multilayer-SW2

```
SW-GOUST>en
Password:
SW-GOUST#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW-GOUST(config)#vlan 120
SW-GOUST(config-vlan)# name GUEST_WIFI_2_CORPUS
SW-GOUST(config-vlan)#
SW-GOUST(config-vlan)#interface range FastEthernet0/1 - 2
SW-GOUST(config-if-range)# description Guest Wi-Fi APs
SW-GOUST(config-if-range)# switchport mode access
SW-GOUST(config-if-range)# switchport access vlan 120
SW-GOUST(config-if-range)# spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface  when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/1 but will only
have effect when the interface is in a non-trunking mode.
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface  when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/2 but will only
have effect when the interface is in a non-trunking mode.
SW-GOUST(config-if-range)#
SW-GOUST(config-if-range)#interface GigabitEthernet0/1
SW-GOUST(config-if)# description TRUNK to Multilayer-SW2
SW-GOUST(config-if)# switchport mode trunk
SW-GOUST(config-if)# switchport trunk allowed vlan 120,701
```

Рисунок 3.10 – Налаштування комутатора SW-GOUST

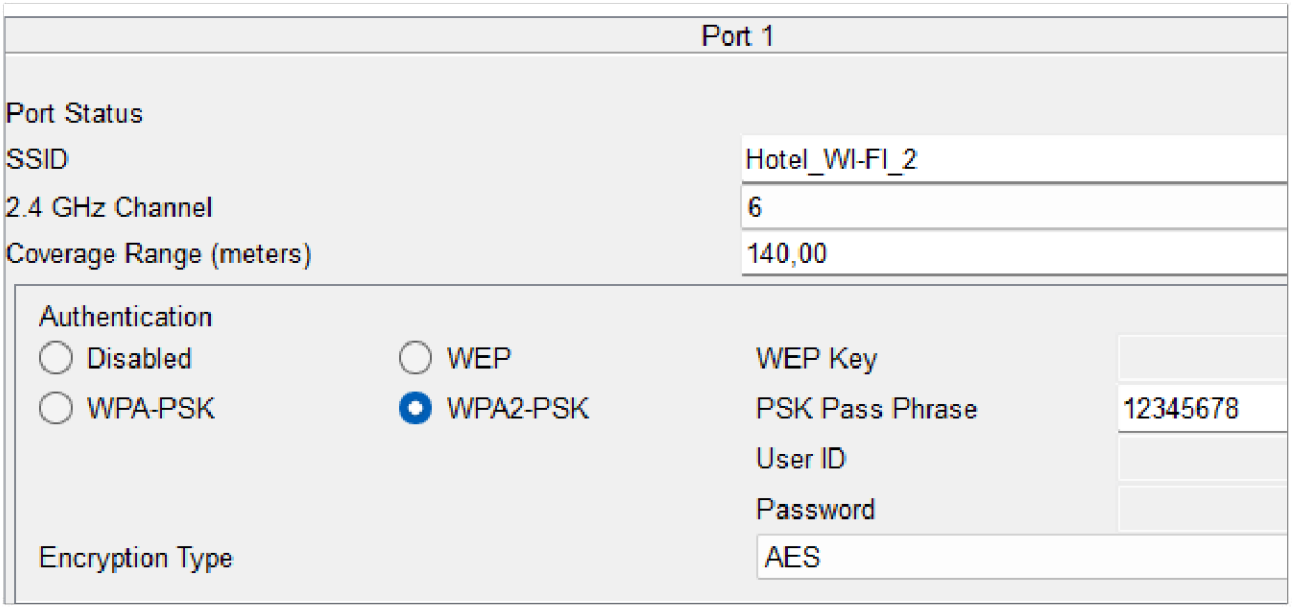

Рисунок 3.11 – Налаштування точки доступу

3.3 Налаштування міжмережевої взаємодії

Для налагодження сполучення між відокремленими логічними частинами комп'ютерної мережі застосовуються маршрутизатори. Вони виконують функцію пересилання даних між підмережами, здійснюючи маршрутизацію IP-пакетів на основі інформації з таблиці маршрутів.

Кожній VLAN у структурі мережі присвоюється віртуальний інтерфейс з унікальною IP-адресою (інтерфейс типу VlanX), що виконує роль шлюзу за замовчуванням для клієнтів цієї VLAN. Для забезпечення маршрутизації між VLAN необхідне увімкнення команди ip routing [18].

У стандартних випадках для комутаторів третього рівня (Multilayer Switch) додатково налаштовуються статичні маршрути (ip route), які дозволяють пересилати пакети до віддалених мереж. Це сприяє зменшенню розміру широкомовних доменів, реалізації сегментації, а також поліпшенню керованості та безпеки трафіку [19].

Нижче представлено приклад налаштування інтерфейсів для Multilayer-SW1 та відповідного маршрутизатора Router0, який забезпечує зв'язок з зовнішніми мережами (рис. 3.12-3.13).

```
Multilayer-SW1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Multilayer-SW1(config)#! ===    Router0 ===
Multilayer-SW1(config)#interface GigabitEthernet1/0/24
Multilayer-SW1(config-if)# description *** Uplink to Building Router ***
Multilayer-SW1(config-if)# no switchport
Multilayer-SW1(config-if)# ip address 10.13.225.10 255.255.255.252
Multilayer-SW1(config-if)# no shutdown
Multilayer-SW1(config-if)#
```

Рисунок 3.12 – Налаштування інтерфейсу комутатора (Корпус 1).

```
Multilayer-SW1(config-if)#ip route 0.0.0.0 0.0.0.0 10.13.225.9
```

Рисунок 3.13 – Статичний маршрут на Multilayer-SW1

Налаштування інтерфейсу між корпусами зображено на рисунку 3.14.

```
Router0>en
Password:
Router0#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router0(config)#interface GigabitEthernet0/0
Router0(config-if)# description *** Link to Multilayer-SW1 ***
Router0(config-if)# ip address 10.13.225.9 255.255.255.252
Router0(config-if)# no shutdown
Router0(config-if)#
08:28:14: %OSPF-5-ADJCHG: Process 10, Nbr 10.13.225.9 on GigabitEthernet0/0 from EXSTART to DOWN,
Neighbor Down: Interface down or detached
```

Рисунок 3.14 – Налаштування інтерфейсу на Router0

Налаштування підключення між маршрутизаторами Router0 ↔ Router1 зображено на рисунках 3.15-3.16.

```
Router1>en
Password:
Password:
Router1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router1(config)#! ===  Router1    Router0 ===
Router1(config)#interface GigabitEthernet0/1
Router1(config-if)# ip address 10.13.225.2 255.255.255.252
Router1(config-if)# no shutdown
```

Рисунок 3.15 – Інтерфейс Router1 для зв’язку з Router0.

```
Router0(config-if)#! ===  Router0    Router1 ===
Router0(config-if)#interface GigabitEthernet0/1
Router0(config-if)# ip address 10.13.225.1 255.255.255.252
Router0(config-if)# no shutdow
```

Рисунок 3.16 – Інтерфейс Router0 для зв’язку з Router1

Налаштування маршрутів між двома корпусами зображено на рисунках 3.17-3.18.

```
Router0(config-if)#! ===  Router0 (    2) ===
Router0(config-if)#ip route 10.13.0.0 255.255.0.0 10.13.225.2
```

Рисунок 3.17 – Шлях до мережі корпусу 2

```
Router1(config-if)#! ===  Router1 (    1) ===
Router1(config-if)#ip route 10.13.0.0 255.255.0.0 10.13.225.1
```

Рисунок 3.18 – Шлях до мереж корпусу 1

Завершену схему комп'ютерної мережі для готельного комплексу зображено на рисунку 3.19.

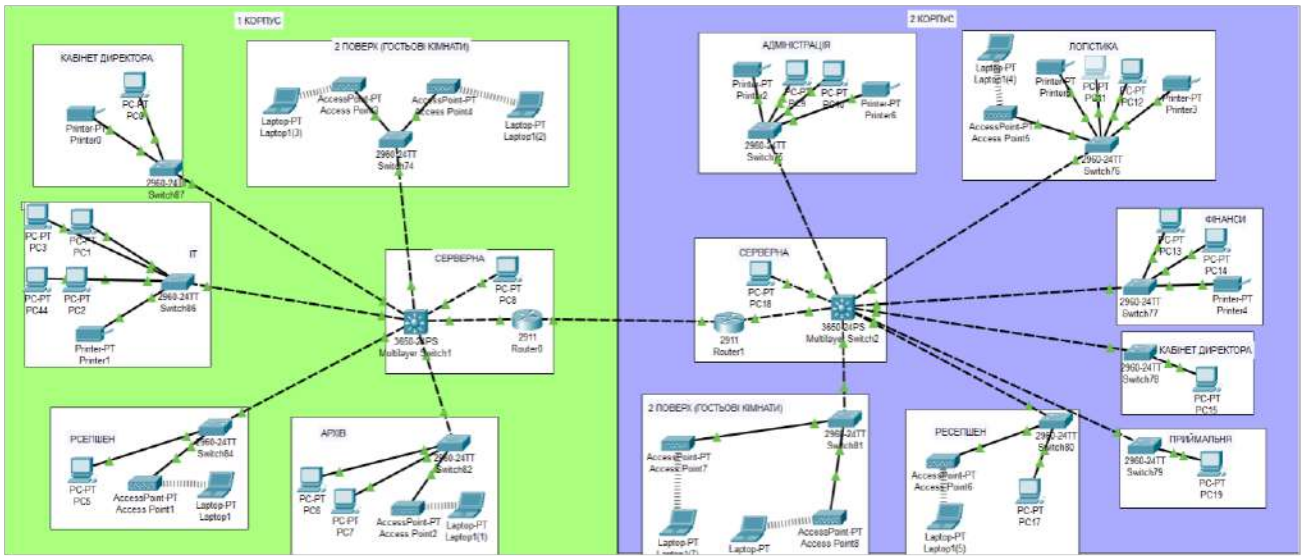

Рисунок 3.19 – Готова схема комп'ютерної мережі

Мережа готова до повноцінного використання: забезпечено фізичне з'єднання всіх підрозділів, налаштовано VLAN для логічного поділу, організовано маршрутизацію між сегментами та впроваджено доступ до сервісів через дротові й бездротові підключення.

ВИСНОВКИ

У процесі виконання кваліфікаційної роботи здійснено детальний аналіз існуючих потреб та можливостей готельного комплексу «Сонячний берег» щодо впровадження сучасної комп'ютерної мережі, визначено ключові технічні аспекти та нюанси топології, враховуючи поділ на два корпуси. Розглянуто особливості розташування обладнання, зон доступу та необхідну кількість клієнтських пристроїв.

Виконано було ось такі завдання:

– виконано детальний аналіз існуючої мережі, що дозволив виявити слабкі місця: відсутність VLAN-сегментації, застарілий парк обладнання, обмежене резервування та недостатній рівень захисту даних;

– сформовано технічні вимоги до оновленої інфраструктури, які враховують потреби всіх підрозділів, вимоги безпеки, централізоване адміністрування та перспективи розвитку;

– проаналізовано інформаційні сервіси й протоколи, визначено критично важливі системи (сервери, Wi-Fi точки доступу і тд.) та описано умови їх підключення;

– обґрунтовано фізичну топологію з резервними каналами, що забезпечує безперервність роботи підрозділів у разі відмови окремих комутаторів;

– розраховано оптимальне розміщення точок доступу Wi-Fi, що гарантує стабільний сигнал у всіх приміщеннях готелю;

– розроблено логічну схему адресації з поділом мережі на VLAN для кожного підрозділу й службового сегмента, із закладеним резервом IP-адрес та ізоляцією трафіку;

– підібрано й налаштовано активне мережеве обладнання з підтримкою VLAN, маршрутів, STP, DHCP та SSH, що підвищило керованість і безпеку;

– реалізовано базові конфігурації для комутаторів 2-го та 3-го рівнів: увімкнено STP, уніфіковано паролі, відключено неактивні порти та забезпечено

захищений доступ;

– організовано бездротовий сегмент із виділеною VLAN, активованим DHCP, що гарантує стабільне й безпечне підключення.

На основі виконаної роботи можна стверджувати, що збудована комп'ютерна мережа відповідає сучасним вимогам до корпоративної інфраструктури та може бути використана як платформа для автоматизації послуг готельного комплексу. Розроблену систему можна застосувати для реального впровадження у готельному закладі середнього або великого розміру зі схожою структурою приміщень та потребами в адмініструванні, безпеці й гнучкості керування мережевими ресурсами.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Cisco. *DHCP Overview.* URL: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_dhcp/configuration/15-sy/dhcp-15-sy-book/dhcp-overview.html (дата звернення: 04.03.2025).

2. Velrajan G. Mastering SSH - A Complete Guide to Secure Shell Protocol. *SocketXP*. URL: https://www.socketxp.com/iot/ssh-secure-shell/ (дата звернення: 08.03.2025).

3. Keary T. Best Network Topologies Explained – Pros & Cons [Includes Diagrams]. *Comparitech.* URL: https://www.comparitech.com/net-admin/network-topologies-advantages-disadvantages/ (дата звернення: 11.03.2025).

4. Spanning Tree Protocol Explained: Eliminating Network Loops. *Cloud Computing Courses | Cyber Security & Ethical Hacking.* URL: https://www.jetking.com/blog/spanning-tree-protocol-explained (дата звернення: 15.03.2025).

5. Хорт Є. Дослідницька робота «Розрахунки оптимального розташування точок доступу Wi-Fi для покриття навчального закладу». *Освітній проект «На Урок» для вчителів.* URL: https://naurok.com.ua/doslidnicka-robota-rozrahunki-optimalnogo-roztashuvannya-tochok-dostupu-wi-fi-dlya-pokrittya-navchalnogo-zakladu-375450.html#__RefHeading__27_293249452 (дата звернення: 19.03.2025).

6. Точка доступу Wi-Fi Ubiquiti UniFi U6 PLUS (U6-PLUS). *Brain – роздрібний інтернет-магазин комп'ютерної техніки та електроніки в Україні.* URL: https://brain.com.ua/ukr/Tochka_dostupu_Wi-Fi_Ubiquiti_UniFi_U6_PLUS_U6-PLUS-p1018392.html?srsltid=AfmBOoo9QNC-BaXW8unFQpIoNrOp1bXijj8dxiEbDC_-qk0htsFtU7a7-_o (дата звернення: 24.03.2025).

7. Layer 3 Switches in Cisco – GeeksforGeeks. *GeeksforGeeks.* URL: https://www.geeksforgeeks.org/layer-3-switches-in-cisco/ (дата звернення: 28.03.2025).

8. Комутатор мережевий Ubiquiti USW-24-POE. *Brain – роздрібний інтернет-магазин комп'ютерної техніки та електроніки в Україні.*

URL: https://brain.com.ua/ukr/Komutator_merejheviy_Ubiquiti_USW-24-POE-p676223.html (дата звернення: 02.04.2025).

9. Deluisio C. Understanding Layer 2 Switches: A Comprehensive Guide. *The Blog of Cody Deluisio*. URL: https://deluisio.com/networking/2024/09/07/understanding-layer-2-switches-a-comprehensive-guide/ (дата звернення: 09.04.2025).

10. Комутатор мережевий TP-Link TL-SG2016P. *Brain – роздрібний інтернет-магазин комп'ютерної техніки та електроніки в Україні*. URL: https://brain.com.ua/ukr/Komutator_merejheviy_TP-Link_TL-SG2016P-p1102610.html?utm_content=new_buyers&gad_source=1&gad_campaignid=20824663912&gclid=Cj0KCQjw0qTCBhCmARIsAAj8C4YDEmbeKpO7wkYv9qmeMVgibLFxPaJnJwe0hSDHbnV0dBAcUbE0uNIaAj2gEALw_wcB (дата звернення: 14.04.2025).

11. Маршрутизатор EdgeRouter 12 (ER-12) купити в Києві та Україні. *Мережеве обладнання купити в Києві, ціна в Україні*. URL: https://nexen.com.ua/uk/goods/edgerouter-12 er-12?gclid=Cj0KCQjwmK_CBhCEARIsAMKwcD7QrUyOkfvmlME_bHxW9sQwDwyAM1sXoXCKxfwxf0_9KoSoQSMTr9gaAuWtEALw_wcB (дата звернення: 16.04.2025).

12. M. Ghobaei-Arani, M. Sookhak, A. Gani, «Network Security in Cloud Computing: Challenges and Solutions,» *Journal of Network and Computer Applications*, Elsevier, Розд. 169, 2020. (дата звернення: 18.04.2025).

13. Network Switching : Types, Differences, Advantages & Its Uses. *ElProCus – Electronic Projects for Engineering Students*. URL: https://www.elprocus.com/network-switching/ (дата звернення: 21.04.2025).

14. Odom W. CCNA 200-301 Official Cert Guide, Volume 1. Розд. 8: Virtual LANs (VLANs). Indianapolis: *Cisco Press*, 2020. 848 с. (дата звернення: 23.04.2025).

15. Tetz, E., & Froom, R. (2021). CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide. *Cisco Press*. (дата звернення: 28.04.2025).

16. Hucaby D. CCNA 200-301 Official Cert Guide, Volume 2. Indianapolis: *Cisco Press*, 2020. Розд. 4: Spanning Tree Protocol (STP). 736 с. (дата звернення: 28.04.2025).

17. Burke B. T. Wireless Networking Benefits: Enhance Business Efficiency & Mobility. Quest *Technology Management*. URL: https://questsys.com/ceo-blog/wireless-networking-benefits-enhance-business-efficiency-and-mobility/ (дата звернення: 29.04.2025).

18. Odom W. CCNA 200-301 Official Cert Guide, Volume 1. Розд. 17: Routing Between VLANs. Indianapolis: *Cisco Press*, 2020. 848 с. (дата звернення: 03.05.2025).

19. Hucaby D. CCNP Enterprise Advanced Routing ENARSI 300-410 Official Cert Guide. Розд. 3: Static Routing. Indianapolis: *Cisco Press*, 2020. 928 с. (дата звернення: 09.05.2025)

ДОДАТКИ

Додаток А

Лістинги конфігураційних файлів

Комутатор Multilayer-SW1:

```
hostname Multilayer-SW1
username admin privilege 15 secret hoteladmin
ip domain-name hotel.local
crypto key generate rsa modulus 1024
ip ssh version 2
line vty 0 4
 login local
 transport input ssh
 exec-timeout 5 0

ip routing
ip flow-export version 9
no service password-encryption

interface Vlan101
 description ARCHIVE
 ip address 10.13.101.1 255.255.255.224
 no shutdown

interface Vlan102
 description RECEPTION
 ip address 10.13.102.1 255.255.255.224
 no shutdown

interface Vlan103
 description IT
 ip address 10.13.103.1 255.255.255.224
 no shutdown

interface Vlan105
 description DIRECTOR
 ip address 10.13.105.1 255.255.255.224
 no shutdown

interface Vlan106
 description GUEST
 ip address 10.13.106.1 255.255.255.224
 no shutdown

interface Vlan110
 description ADMIN
 ip address 10.13.110.1 255.255.255.224
 no shutdown

interface GigabitEthernet0/1
 description *** Uplink to Router0 ***
 no switchport
 ip address 10.13.225.9 255.255.255.252
 no shutdown

ip route 0.0.0.0 0.0.0.0 10.13.225.10

interface GigabitEthernet1/0/1
 description Uplink_to_SW-ARCHIVE
 switchport mode trunk
 switchport trunk allowed vlan 101,701

interface GigabitEthernet1/0/2
 description Uplink_to_SW-RECEPTION
 switchport mode trunk
 switchport trunk allowed vlan 102,701

interface GigabitEthernet1/0/3
 description TRUNK to SW-IT
 switchport mode trunk
 switchport trunk allowed vlan 1-1005

interface GigabitEthernet1/0/4
 description TRUNK to SW-DIRECTOR
 switchport mode trunk
 switchport trunk allowed vlan 1-1005

interface GigabitEthernet1/0/5
 description TRUNK to SW-GUEST
 switchport mode trunk
 switchport trunk allowed vlan 1-1005

interface GigabitEthernet1/0/6
 description Admin PC
 switchport mode access
 switchport access vlan 110

banner motd #
 ДОСТУП ДО Multilayer-SW1 ЗАБОРОНЕНО
НЕАВТОРИЗОВАНИМ КОРИСТУВАЧАМ
#

end
write memory
```

Комутатор Multilayer-SW2:

```
hostname Multilayer-SW1
username admin privilege 15 secret hoteladmin
ip domain-name hotel.local
crypto key generate rsa modulus 1024
ip ssh version 2
line vty 0 4
 login local
 transport input ssh
 exec-timeout 5 0

ip routing
ip flow-export version 9
no service password-encryption

interface Vlan101
 description ADMINISTRATION
 ip address 10.13.32.1 255.255.255.224
 no shutdown

interface Vlan102
 description LOGISTICS
 ip address 10.13.64.1 255.255.255.224
 no shutdown

interface Vlan103
 description FINANCE
 ip address 10.13.96.1 255.255.255.224
 no shutdown

interface Vlan105
 description DIRECTOR
 ip address 10.13.128.1 255.255.255.224
 no shutdown

interface Vlan106
 description GOUST
 ip address 10.13.160.1 255.255.255.224
 no shutdown

interface Vlan110
 description RECEPTION
 ip address 10.13.192.1 255.255.255.224
 no shutdown

interface GigabitEthernet0/1
 description *** Uplink to Router1 ***
 no switchport
 ip address 10.13.225.18 255.255.255.248
 no shutdown

ip route 0.0.0.0 0.0.0.0 10.13.225.17

interface GigabitEthernet1/0/1
 description Uplink_to_SW-ADMINISTRATION
 switchport mode trunk
 switchport trunk allowed vlan 101,701

interface GigabitEthernet1/0/2
 description Uplink_to_SW-LOGISTICS
 switchport mode trunk
 switchport trunk allowed vlan 102,701

interface GigabitEthernet1/0/3
 description TRUNK to SW-FINANCE
 switchport mode trunk
 switchport trunk allowed vlan 1-1005

interface GigabitEthernet1/0/4
 description TRUNK to SW-DIRECTOR
 switchport mode trunk
 switchport trunk allowed vlan 1-1005

interface GigabitEthernet1/0/5
 description TRUNK to SW-GOUST
 switchport mode trunk
 switchport trunk allowed vlan 1-1005

interface GigabitEthernet1/0/6
 description Admin PC
 switchport mode access
  switchport access vlan 110
```

Маршрутизатор Router0:

```
hostname Router0

username admin privilege 15 secret
hoteladmin
ip domain-name hotel.local
crypto key generate rsa modulus 1024
ip ssh version 2
line vty 0 4
 login local
 transport input ssh
 exec-timeout 5 0

interface GigabitEthernet0/0
 description *** To Multilayer-SW1 ***
 ip address 10.13.225.10 255.255.255.252
 ip nat outside
 no shutdown

interface GigabitEthernet0/1
 description *** To Router1 ***
 ip address 10.13.225.60 255.255.255.252
 no shutdown

ip access-list standard 1
 permit 10.13.0.0 0.0.255.255

ip nat inside source list 1 interface
 GigabitEthernet0/0 overload

ip route 10.13.225.16 255.255.255.248
 10.13.225.61

end
write memory
```

Маршрутизатор Router1:

```
hostname Router1

username admin privilege 15 secret hoteladmin
ip domain-name hotel.local
crypto key generate rsa modulus 1024
ip ssh version 2
line vty 0 4
 login local
 transport input ssh
 exec-timeout 5 0

interface GigabitEthernet0/0
 description *** To Router0 ***
 ip address 10.13.225.61 255.255.255.252
 no shutdown

interface GigabitEthernet0/1
 description *** To Multilayer-SW2 ***
 ip address 10.13.225.17 255.255.255.248
 no shutdown

ip route 0.0.0.0 0.0.0.0 10.13.225.61
ip route 10.13.225.8 255.255.255.252
 10.13.225.61

end
write memory
```