

Міністерство освіти і науки України  
Національний технічний університет  
«Дніпровська політехніка»

Навчально-науковий  
інститут електроенергетики  
(інститут)  
Факультет інформаційних технологій  
(факультет)  
Кафедра інформаційних технологій та комп'ютерної інженерії  
(повна назва)

**ПОЯСНЮВАЛЬНА ЗАПИСКА**  
**кваліфікаційної роботи ступеня бакалавра**

студента Мухіна Владислава Дмитровича  
(ПІБ)

академічної групи 123-21ск-1  
(шифр)

спеціальності 123 Комп'ютерна інженерія  
(код і назва спеціальності)

за освітньо-професійною програмою 123 Комп'ютерна інженерія  
(офіційна назва)

на тему «Комп'ютерна система приватного підприємства «River Travels» з  
детальним опрацюванням побудови, налаштування та безпеки  
корпоративної мережі»

(назва за наказом ректора)

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	доц. Кожевніков А.В.			
спеціальної частини				
розділів:				
розробка апаратної частини	доц. Бешта Д.О.			
розробка корпоративної мережі	ас. Панферова Я.В.			
Рецензент	доц. Логвін В.М.			
Нормоконтролер	проф. Цвіркун Л.І.			

Дніпро  
2024

**ЗАТВЕРДЖЕНО:**

завідувач кафедри  
інформаційних технологій  
та комп'ютерної інженерії

(повна назва)

\_\_\_\_\_ Гнатушенко В.В.  
(підпис) (прізвище, ініціали)

« \_\_\_\_\_ » \_\_\_\_\_ 2024 року

**ЗАВДАННЯ**  
**на кваліфікаційну роботу**  
**ступеня бакалавр**

студента Мухіна В.Д. академічної групи 123-21ск-1  
(прізвище та ініціали) (шифр)

спеціальності 123 Комп'ютерна інженерія  
за освітньо-професійною програмою 123 Комп'ютерна інженерія  
(офіційна назва)

на тему «Комп'ютерна система приватного підприємства «River Travels» з  
детальним опрацюванням побудови, налаштування та безпеки  
корпоративної мережі»

затверджену наказом ректора НТУ «Дніпровська політехніка» 23.05.2024 № 469-с

Розділ	Зміст	Термін виконання
Стан питання та постановка завдання	На основі матеріалів виробничих практик, інших науково-технічних джерел розглянути призначення та завдання для розробки та налаштування комп'ютерної мережі для приватного підприємства «River Travels».	01.04.2024
Розробка апаратної частини	Розробити вимоги до функцій, виконуваними системою та провести розробку та аналіз загальної архітектури мережі, з подальшим створенням структурної схеми та вибором апаратних засобів та її реалізації.	27.04.2024
Розробка корпоративної мережі	Побудувати в Packet Tracer модель корпоративної мережі компанії, виконати налаштування та перевірку роботи системи.	25.05.2024
Розробка компонента системи	Розробити спеціальної частини корпоративної мережі з використанням технології інтернету речей з подальшим аналізом та перевіркою системи.	13.06.2024

**Завдання видано**

доц. Кожевніков А.В.

\_\_\_\_\_ (підпис керівника)

\_\_\_\_\_ (прізвище, ініціали)

**Дата видачі** 01.05.2024

**Дата подання до екзаменаційної комісії** 17.06.2024

**Прийнято до виконання**

Мухін В.Д.

\_\_\_\_\_ (підпис студента)

\_\_\_\_\_ (прізвище, ініціали)

## РЕФЕРАТ

Пояснювальна записка: 82 с., 24 рис., 7 табл., 1 додатків, 7 джерела.

**КЛЮЧОВІ СЛОВА:** віртуальна мережа, кібербезпека, комп'ютерна система, оптимізація, програмне забезпечення, річкові тури, управління даними.

Об'єкт розробки – комп'ютерна система компанії «River Travels».

Мета роботи – побудова комп'ютерної система приватного підприємства «River Travels» з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі.

Методи дослідження та апаратура – використання сучасних методів системного аналізу, а також застосування комп'ютерної інженерії для розробки системи.

Результати та їх новизна – створено корпоративну мережу компанії яка включає оптимізацію їх процесами безпеку даних та контролювання доступу.

Основні конструктивні, технологічні й техніко-експлуатаційні характеристики – система включає передові рішення у сфері безпеки даних, оптимізації робочих процесів та інтерфейсу, зручного для користувачів

## ЗМІСТ

Перелік умовних позначень, символів, одиниць, скорочень і термінів .....	7
Вступ .....	8
1 Стан питання і постановка завдання .....	9
1.1 Стисла характеристика галузі та умов застосування мережі.....	9
1.2 Характеристика підприємства та умов застосування КС.....	10
1.3 Принципи, технічні способи та математичні методи інформаційного забезпечення підприємства .....	11
1.4 Огляд існуючих інженерних рішень КС в галузі та визначення можливих напрямків рішення поставлених завдань .....	12
1.5 Розробка схеми організаційної структури підприємства .....	14
1.6 Завдання і мета роботи.....	15
1.7 Визначення можливих напрямків рішення поставлених завдань .....	16
1.8 Обґрунтування вибраного напрямку інженерного рішення.....	17
2 Розробка апаратної частини комп'ютерної або кіберфізичної системи.....	18
2.1 Технічні вимоги до комп'ютерної системи приватного підприємства «River Travels» .....	18
2.1.1 Вимоги до системи в цілому .....	18
2.1.1.1 Вимоги до структури і функціонуванню системи .....	18
2.1.1.1.1 Перелік підсистем, їхнє призначення й основні характеристики, вимоги до числа рівнів ієрархії та ступені централізації Системи.....	18
2.1.1.1.2 Вимоги до способів і засобів зв'язку між компонентами комп'ютерної системи .....	19
2.1.1.1.3 Вимоги до характеристик взаємозв'язків створюваної системи із суміжними системами.....	20
2.1.1.1.4 Вимоги до режимів функціонування системи .....	21
2.1.1.1.5 Вимоги до діагностування системи .....	21
2.1.1.1.6 Перспективи розвитку, модернізації системи .....	21
2.1.1.2 Вимоги до показників призначення .....	22

2.1.1.3	Вимоги до патентної чистоти.....	23
2.1.1.4	Додаткові вимоги.....	23
2.1.2	Вимоги функцій, виконуваним системою.....	24
2.1.3	Вимоги до видів забезпечення комп'ютерної системи.....	26
2.1.3.1	Вимоги до математичного забезпечення .....	26
2.1.3.2	Вимоги до інформаційного забезпечення.....	26
2.1.3.3	Вимоги до лінгвістичного забезпечення.....	28
2.1.3.4	Вимоги до технічного забезпечення.....	28
2.1.3.5	Вимоги до організаційного забезпечення.....	29
2.1.3.6	Вимоги до методичного забезпечення .....	29
2.2	Розробка апаратної частини комп'ютерної системи.....	29
2.2.1	Розробка загальної архітектури мережі підприємства .....	29
2.2.2	Вибір і обґрунтування структурної схеми комплексу технічних засобів комп'ютерної системи.....	30
2.2.3	Розробка специфікації апаратних засобів комп'ютерної системи.....	31
2.2.4	Розрахунок інтенсивності трафіку вихідного трафіку найбільшої локальної мережі підприємства .....	33
3	Розробка корпоративної мережі .....	36
3.1	Проектування логічної топології мережі .....	36
3.2	Вибір та опис мережного обладнання.....	38
3.3	Розрахунок схеми адресації корпоративної мережі .....	38
3.4	Вибір та налаштування способу маршрутизації .....	42
3.4.1	Базове налаштування конфігурації пристроїв.....	42
3.4.2	Налаштування протоколу OSPF та DHCP для маршрутизаторів корпоративної мережі .....	43
3.4.3	Налаштування роботи Інтернет .....	45
3.5	Налаштування мереж VLAN, маршрутизації між VLAN .....	46
3.6	Захист інформації в комп'ютерній системі від несанкціонованого доступу.....	49
3.6.1	Налаштування віртуальної приватної мережі VPN .....	49
3.6.2	Налаштування маршрутизаторів на підтримку служби AAA .....	50

3.7	Перевірка комп'ютерної Системи підприємства .....	52
4	Розробка компонента безпеки та клімат контролю .....	57
4.1	Інженерне рішення по розробці компонента Системи .....	57
4.2	Налаштування обладнання та сервісів системи IoT .....	58
4.3	Перевірка роботи компонента Системи .....	62
	Висновки .....	66
	Список використаних джерел .....	67
	Додаток А. Текст налаштування пристроїв та загальна архітектура мережі .....	68

## **ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ**

БД — База даних.

ВП — Веб-портал.

КС — Комп'ютерна система.

НСІ — Національна система інформації.

ОС — Операційна система.

ПЗ — Програмне забезпечення.

РТ — River Travels.

СКБД — Система керування базами даних.

СУБД — Система управління базами даних.

ТЗ — Технічне завдання.

ЦП — Центральний процесор.

IP — Інтернет-протокол.

VLAN — Віртуальна локальна обчислювальна мережа.

OSPF — Протокол коротшого шляху першого вибору (Open Shortest Path First).

VPN — Віртуальна приватна мережа.

AAA — Аутентифікація, Авторизація та Облік (Authentication, Authorization, and Accounting).

NAT — Мережева адресна трансляція.

ACL — Список контролю доступу.

## ВСТУП

У сьогоднішньому світі технології розвиваються стрімко, і важливість належного впровадження та адміністрування інформаційних систем у корпоративному середовищі значно зростає. Оптимізація робочих процесів через використання комп'ютерних систем відіграє ключову роль у підвищенні ефективності підприємств та наданні якісних послуг. Саме тому тема роботи побудова комп'ютерної система приватного підприємства «River Travels» з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі є актуальною та заслуговує на детальне вивчення.

Підприємство «River Travels» спеціалізується на наданні послуг з оренди каяків та SUP дошок, а також проведенні річкових турів у місті Дніпро. Ця сфера вимагає чіткої організації роботи, ефективного управління ресурсами та швидку відповідь на зміни в попиті та ринкових умовах. Інформаційна система, яка була спроектована та реалізована у рамках даної роботи, відіграє ключову роль у досягненні цих цілей.

Основним завданням дипломної роботи є аналіз поточного стану інформаційної інфраструктури підприємства, розробка та впровадження вдосконаленої комп'ютерної системи, яка забезпечує ефективне управління діяльністю компанії, зокрема бронюванням обладнання, організацією турів та обліком. Також значна увага приділяється питанням кібербезпеки, що є критичним аспектом у захисті даних та інформаційних ресурсів підприємства.

Впровадження цієї системи дозволить «River Travels» підвищити рівень задоволеності клієнтів, оптимізувати внутрішні процеси та забезпечити стійкий розвиток підприємства у конкурентному ринковому середовищі.



## 1 СТАН ПИТАННЯ І ПОСТАНОВКА ЗАВДАННЯ

### 1.1 Стисла характеристика галузі та умов застосування мережі

Приватне підприємство «River Travels» спеціалізується на наданні послуг з оренди каяків та SUP дощок, а також проведенні екскурсійних турів річками Дніпра. Зростання популярності водного туризму та активного відпочинку серед населення спонукає до розширення ринку послуг, зокрема через інтеграцію сучасних технологій у процеси бронювання, обслуговування клієнтів та управління ресурсами.

Впровадження комп'ютерної системи в діяльність підприємства «River Travels» вимагає врахування особливостей галузі, таких як висока залежність від сезонності, динамічність попиту, а також необхідність забезпечення високого рівня безпеки і надійності сервісу. Система орієнтована на підвищення ефективності обробки замовлень, оптимізацію планування турів та забезпечення зручності користувачів через інтерфейс для онлайн-бронювання та управління особистими резерваціями.

Система також розробляється з урахуванням необхідності інтеграції з геолокаційними сервісами для точного відстеження місцезнаходження водного транспорту в режимі реального часу, що забезпечує додаткову безпеку клієнтів під час водних подорожей та оптимізує роботу сервісної служби. Включення цієї функціональності дозволяє також аналізувати маршрути руху, частоту використання певних напрямків та планувати стратегічні напрямки розвитку послуг.

Для забезпечення високого рівня обслуговування та індивідуалізації досвіду клієнтів, система передбачає функцію збору та аналізу зворотного зв'язку від користувачів, що дозволяє підприємству оперативно реагувати на потреби та побажання клієнтів, а також вдосконалювати якість послуг. Ця інформація буде корисною для формування маркетингових стратегій та промоційних кампаній, спрямованих на підвищення лояльності клієнтів та залучення нових відвідувачів.

Окрім того, система обладнана інструментами для ефективного управління внутрішніми ресурсами підприємства, такими як управління запасами, логістика та облік, що дозволяє оптимізувати внутрішні процеси та знижувати операційні витрати. Автоматизація цих процесів спрямована на підвищення ефективності загальної роботи підприємства та забезпечення сталого розвитку.

Основною вимогою до системи є її масштабованість та адаптивність до змінюваних умов ринку, можливість інтеграції з існуючими платформами соціальних мереж для просування послуг, а також висока ступінь захищеності даних клієнтів, що досягається за допомогою розгорнутих технологій шифрування та ідентифікації.

## **1.2 Характеристика підприємства та умов застосування КС**

Приватне підприємство «River Travels» виконує свою діяльність на ринку водного туризму, надаючи послуги оренди каяків, SUP дощок та організації річкових турів. Основною цільовою аудиторією є активні молоді люди та сім'ї, які цікавляться здоровим способом життя та пригодами на природі. Підприємство знаходиться в місті Дніпро, що забезпечує легкий доступ до річки Дніпро, що є ключовою локацією для водних активностей.

Комп'ютерна система (КС), розроблена для «River Travels», спрямована на підтримку та автоматизацію основних бізнес-процесів, зокрема бронювання обладнання, планування турів, управління клієнтськими даними та зворотнім зв'язком.

Система також інтегрована з модулями для збору аналітичних даних для вивчення попиту та вподобань клієнтів, що дозволяє підприємству адаптуватися до ринкових умов та оптимізувати пропозицію послуг.

Умови застосування КС включають забезпечення безперервності служби, високий рівень безпеки даних клієнтів, здатність системи швидко адаптуватися до змінних умов роботи, наприклад, у випадках зміни погодних умов або змін у планах клієнтів. Важливою є також інтеграція з мобільними додатками та соціальними мережами для промоції послуг і спілкування з клієнтами.

КС «River Travels» має бути розроблена з урахуванням потреб сучасного ринку водного туризму та забезпечує комплексне рішення, яке допомагає підвищити якість обслуговування клієнтів та ефективність внутрішніх операцій підприємства.

### **1.3 Принципи, технічні способи та математичні методи інформаційного забезпечення підприємства**

Принципи інформаційного забезпечення:

інтегрованість: Система розробляється таким чином, щоб забезпечити єдиний центр управління даними, що дозволяє інтеграцію різних модулів (бронювання, облік, логістика, зворотній зв'язок);

масштабованість: Система проектується з можливістю легкого розширення функціоналу та збільшення обсягу оброблюваних даних без втрати продуктивності;

гнучкість: Адаптивність до змін у бізнес-процесах і ринкових умовах;

безпека: Впровадження сучасних методів шифрування та ідентифікації для захисту інформації.

Технічні способи:

використання хмарних технологій для забезпечення доступності системи з будь-якої точки з доступом до інтернету та високого рівня даних;

модульна архітектура дозволяє легко модифікувати або додавати нові компоненти без перебудови всієї системи;

автоматизація процесів з використанням бізнес-логіки для внутрішніх операцій, зокрема управління запасами та логістика;

реалізація API для інтеграції з зовнішніми сервісами, такими як соціальні мережі та геолокаційні сервіси.

Математичні методи:

статистичний аналіз даних для визначення тенденцій попиту та планування ресурсів;

методи оптимізації для планування маршрутів турів та логістики, використовуючи алгоритми мінімізації витрат та максимізації покриття;

прогнозування з використанням машинного навчання для адаптації пропозицій послуг під змінювані умови ринку та переваги клієнтів;

алгоритми кластеризації для сегментації клієнтів на основі поведінкових та демографічних характеристик для цільового маркетингу та персоналізації пропозицій.

Ці принципи, способи та методи забезпечують створення ефективної, безпечної та гнучкої системи, що дозволяє підприємству «River Travels» підвищувати конкурентоспроможність та задовольняти потреби клієнтів на високому рівні.

#### **1.4 Огляд існуючих інженерних рішень КС в галузі та визначення можливих напрямків рішення поставлених завдань**

Існує кілька провідних компаній, які займаються розробкою та імплементацією комп'ютерних мереж та їх інфраструктур. Ці компанії пропонують широкий спектр рішень, які використовуються у багатьох галузях, включаючи туризм:

1) Cisco Systems — лідер у розробці та імплементації мережевих рішень. Cisco пропонує обладнання для створення масштабованих, надійних та безпечних мереж, таке як маршрутизатори, комутатори, точки доступу Wi-Fi та безпекове обладнання.

2) Juniper Networks — спеціалізується на виробництві мережевого обладнання для створення високопродуктивних комп'ютерних мереж. Їх продукція включає маршрутизатори, комутатори та продукти безпеки, які використовуються в корпоративних мережах та провайдерами інтернет-послуг.

3) Hewlett Packard Enterprise (HPE) — пропонує рішення для побудови мережевих інфраструктур, включаючи комутатори, маршрутизатори, бездротове обладнання та рішення з управління мережею, здатні задовольнити потреби великих підприємств і дрібних організацій.

4) Aruba Networks (частина HPE) — фокусується на розробці бездротових рішень та мережевої безпеки, що забезпечує інтеграцію мобільних та IoT-пристроїв у корпоративні мережі.

5) Dell Technologies — пропонує рішення для мережевих інфраструктур, включаючи комутатори, маршрутизатори та рішення для зберігання даних, що дозволяє створювати масштабовані та ефективні мережеві середовища.

Ці компанії та їхні технології забезпечують фундамент для створення міцної інфраструктури, яка є критично важливою для надійного та безпечного доступу до інформаційних ресурсів в галузі туризму та активного відпочинку, а також може бути використана для розширення можливостей комп'ютерної системи підприємства "River Travels".

Та також що до програм які інтегруються до системи для полегшення ведення бізнесу, ринку існує кілька зразків комп'ютерних систем, що забезпечують ефективне управління ресурсами та клієнтськими відносинами у сфері туризму та активного відпочинку. Серед них:

– системи онлайн-бронювання (наприклад, Booking.com, Airbnb) забезпечують гнучке управління резерваціями і легко інтегруються з веб-сайтами та мобільними додатками;

– CRM-системи (наприклад, Salesforce, HubSpot) спрямовані на управління взаємовідносинами з клієнтами, збір і аналіз даних про клієнтів, що сприяє підвищенню якості обслуговування та ефективності маркетингових кампаній;

– ERP-системи (наприклад, SAP, Oracle) інтегрують всі основні бізнес-процеси компанії, включаючи логістику, облік та управління запасами.

– спеціалізовані галузеві рішення для туристичних агенцій та операторів активного відпочинку, що включають модулі для управління маршрутами, планування турів і ведення статистики.

Можливі напрямки рішення поставлених завдань: Для підвищення ефективності управління "River Travels", можливі такі напрямки розвитку комп'ютерної системи:

– адаптація та кастомізація існуючих CRM і ERP систем для забезпечення індивідуальних потреб підприємства, зокрема інтеграція з модулями бронювання та планування турів;

– розробка власного рішення, зосередженого на специфіці водного туризму, що включатиме додаткові функції, як-от геолокаційне відстежування, управління безпекою та адаптація до екологічних ініціатив;

– інтеграція з мобільними додатками та соціальними мережами для поліпшення взаємодії з клієнтами та просування послуг;

– впровадження інноваційних технологій, таких як машинне навчання для аналізу даних та штучний інтелект для автоматизації рішень, що підвищить точність прогнозування попиту та оптимізації ресурсів.

Такий підхід дозволить "River Travels" не лише ефективно управляти поточними потребами, але й гнучко адаптуватися до мінливих умов ринку та очікувань клієнтів, забезпечуючи стійке зростання та розвиток підприємства.

### **1.5 Розробка схеми організаційної структури підприємства**

Організаційна структура підприємства включає наступні ключові підрозділи:

Верховне керівництво:

– Директор: Відповідає за стратегічне планування та загальне керівництво діяльністю підприємства.

Адміністративний відділ:

– Менеджер з адміністративних питань: Координує всі внутрішні операції, включаючи управління персоналом, офісом та юридичні питання.

Фінансовий відділ:

– Головний бухгалтер: Відповідає за управління фінансами, бухгалтерський облік та податкову звітність.

Відділ маркетингу та продажів:

– Менеджер з маркетингу: Розробляє та впроваджує стратегії просування послуг підприємства.

– Менеджер з продажів: Відповідає за прями продажі, взаємодію з клієнтами та організацію турів.

ІТ-відділ:

– ІТ-директор: Відповідає за розробку, впровадження та підтримку комп'ютерної системи.

– Технічний спеціаліст: Підтримує стабільну роботу мережевої інфраструктури та програмного забезпечення.

Відділ обслуговування клієнтів:

– Менеджер з обслуговування клієнтів: Відповідає за взаємодію з клієнтами, обробку замовлень та вирішення проблем клієнтів.

Логістичний відділ:

– Логіст: Координує рух обладнання та забезпечення необхідними ресурсами для проведення турів.

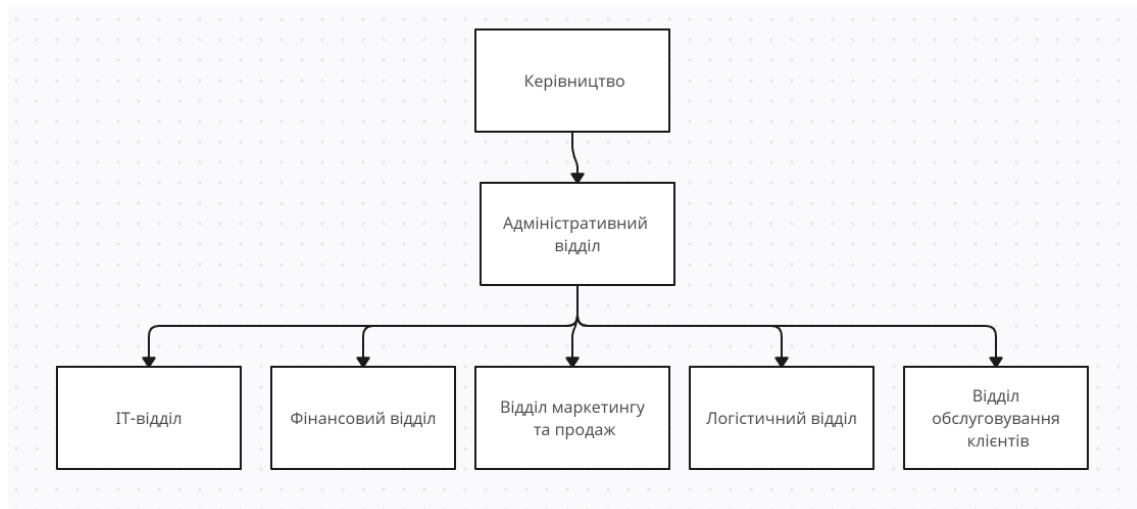


Рисунок 1.1 – Схема організаційної структури компанії

## 1.6 Завдання і мета роботи

Головна мета даної роботи полягає у розробці та впровадженні комп'ютерної системи для підприємства «River Travels», яка забезпечуватиме ефективне управління ресурсами, оптимізацію процесів обслуговування клієнтів та підвищення загальної продуктивності бізнесу. Система спрямована на

автоматизацію ключових бізнес-процесів, поліпшення взаємодії з клієнтами та забезпечення безпеки даних.

Завдання роботи: Для досягнення поставленої мети, робота передбачає виконання наступних завдань:

- аналіз об'єкта впровадження;
- сформулювати технічні вимоги до об'єкта;
- обґрунтувати вибір мережевої архітектури та обладнання для майбутньої системи;
- розробити специфікацію апаратних засобів;
- провести аналіз мережевого трафіку;
- провести тестування мережі в цілому та кожного компонента мережі окремо.

### **1.7 Визначення можливих напрямків рішення поставлених завдань**

Розглянемо ключові напрямки, які дозволять забезпечити надійність, безпеку та ефективність мережевої інфраструктури:

Створення масштабованої та модульної мережевої архітектури:

- Розробка мережевої структури, що забезпечить легке масштабування відповідно до росту підприємства та збільшення кількості користувачів.

Впровадження централізованого управління мережею:

- Використання систем управління мережею для моніторингу, діагностики та вирішення проблем у реальному часі, забезпечуючи високий рівень доступності послуг.

Застосування передових методів захисту даних та мережевої безпеки:

- Імплементация надійних рішень для захисту від зовнішніх та внутрішніх загроз, включно з вогняними стінами, антивірусним захистом, системами виявлення та запобігання вторгненням.

Організація бездротової інфраструктури для гнучкого доступу:

- Розгортання Wi-Fi мережі для забезпечення доступу до корпоративних ресурсів з будь-якої точки офісу або бази відпочинку.

Інтеграція з хмарними сервісами для підвищення ефективності:



– Використання хмарних платформ для резервного копіювання даних, колаборативної роботи та інших корпоративних додатків.

Впровадження VPN-доступу для забезпечення конфіденційності:

– Налаштування віртуальних приватних мереж для безпечного з'єднання співробітників, що працюють віддалено або з мобільних пристроїв.

Реалізація системи управління та моніторингу мережевого трафіку:

– Застосування рішень для аналізу мережевого трафіку, що дозволяє оптимізувати використання мережевих ресурсів та попереджувати перевантаження.

Ці напрямки допоможуть забезпечити високу ефективність та надійність корпоративної мережі «River Travels», а також дозволять гнучко реагувати на мінливі вимоги сучасного бізнес-середовища та зростаючі потреби клієнтів.

## **1.8 Обґрунтування вибраного напрямку інженерного рішення**

Для підприємства «River Travels», яке спеціалізується на наданні послуг з оренди каяків і SUP дощок та проведенні екскурсійних турів річками, важливо мати надійну, безпечну та ефективну корпоративну мережу. З огляду на специфіку діяльності та потреби підприємства, вибір напрямку для інженерного рішення зосереджується на розгортанні масштабованої мережевої інфраструктури.

Розгортання масштабованої мережевої інфраструктури:

Надійність: Стабільна мережева інфраструктура є ключовою для безперервної роботи онлайн-платформ бронювання та управління клієнтськими даними. Масштабованість мережі дозволяє забезпечити надійність та безперебійність служб навіть при високому навантаженні.

Безпека: Розгортання фізичних та віртуальних засобів безпеки на рівні мережі, включно з вогняними стінами, інтрузивними системами виявлення та запобігання, забезпечує захист від атак і несанкціонованого доступу до корпоративних ресурсів.

## **2 РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ КОМП'ЮТЕРНОЇ АБО КІБЕРФІЗИЧНОЇ СИСТЕМИ**

### **2.1 Технічні вимоги до комп'ютерної системи приватного підприємства «River Travels»**

#### **2.1.1 Вимоги до системи в цілому**

##### **2.1.1.1 Вимоги до структури і функціонуванню системи**

##### **2.1.1.1.1 Перелік підсистем, їхнє призначення й основні характеристики, вимоги до числа рівнів ієрархії та ступені централізації Системи**

Для ефективного функціонування та управління бізнес-процесами в "River Travels", комп'ютерна система (КС) має бути структурована на декілька ключових підсистем, кожна з яких відіграє важливу роль у загальній архітектурі системи. Ось перелік основних підсистем і їх призначень:

Підсистема бронювання та управління резерваціями:

- призначення: Обробка замовлень клієнтів, управління доступністю інвентарю, резервації та планування маршрутів;
- характеристики: Інтуїтивно зрозумілий інтерфейс користувача, інтеграція з платіжними системами, звітність у реальному часі.

Клієнтська підсистема (CRM):

- призначення: Управління відносинами з клієнтами, збір та аналіз даних про клієнтів, історія звернень і взаємодій;
- характеристики: Підтримка бази даних клієнтів, інструменти для маркетингу та зв'язку з клієнтами, аналітика поведінки клієнтів.

Фінансова підсистема:

- призначення: Управління фінансовими потоками, бухгалтерський облік, звітність;
- характеристики: Автоматизація фінансових операцій, інтеграція з бухгалтерськими програмами, забезпечення відповідності податковим нормам.

Логістична підсистема:

– призначення: Управління логістикою обладнання, оптимізація маршрутів, планування доставки;

– характеристики: Моніторинг розташування обладнання, інтеграція з GPS-слідкуванням, автоматизація логістичних процесів.

Вимоги до числа рівнів ієрархії та ступені централізації: КС "River Travels" має бути розроблена з використанням централізованої архітектури з можливістю децентралізації окремих компонентів при необхідності:

Централізована архітектура забезпечує єдиний точок доступу до даних, поліпшене управління ресурсами і легше впровадження змін у систему.

Модульний дизайн дозволяє відокремлення функціональних блоків для локальної адаптації та оптимізації без впливу на загальну систему.

Дворівнева архітектура: Перший рівень - це центральний сервер з основною базою даних і логікою системи. Другий рівень - це клієнтські додатки та мобільні додатки, що забезпечують інтерфейс до центральної системи.

Ця структура забезпечить ефективну координацію між різними підрозділами підприємства, поліпшить управління даними та забезпечить високий рівень обслуговування клієнтів.

#### **2.1.1.1.2 Вимоги до способів і засобів зв'язку між компонентами комп'ютерної системи**

Для забезпечення ефективного функціонування комп'ютерної системи «River Travels», важливо встановити високі вимоги до способів і засобів зв'язку між її компонентами. Це забезпечить надійне, безпечне і швидке обмін даними всередині системи. Основні аспекти цих вимог включають:

Типи зв'язку:

Широкосмуговий доступ до Інтернету для забезпечення постійного зв'язку між всіма компонентами системи, включаючи віддалені локації.

Внутрішня локальна мережа (LAN) для забезпечення високошвидкісного зв'язку між компонентами, розташованими в одному фізичному просторі.

Віртуальна приватна мережа (VPN) для забезпечення безпечного зв'язку між компонентами, що знаходяться у різних локаціях.

Протоколи передачі даних:

HTTP/HTTPS для веб-запитів і веб-сервісів, забезпечуючи сумісність з веб-браузерами та мобільними додатками.

TCP/IP для надійної передачі даних між серверами та клієнтськими системами.

WebSocket для забезпечення двостороннього комунікаційного зв'язку у реальному часі, що є важливим для додатків, які вимагають швидкої реакції, таких як системи бронювання та чат-боти.

Засоби забезпечення безпеки:

Шифрування даних через SSL/TLS для забезпечення конфіденційності та цілісності даних під час їх передачі.

Ідентифікація та аутентифікація користувачів та систем через використання сертифікатів та ключів безпеки.

Міжмережеві екрани (firewalls) і системи виявлення та запобігання вторгненням (IDS/IPS) для захисту від несанкціонованих доступів та атак.

Вимоги до апаратного забезпечення:

Маршрутизатори та комутатори мають бути відповідної потужності для підтримки необхідного обсягу даних і кількості підключень.

Сервери мають бути оснащені достатнім рівнем обчислювальних ресурсів для обробки запитів у режимі реального часу без затримок.

### **2.1.1.1.3 Вимоги до характеристик взаємозв'язків створюваної системи із суміжними системами**

Для забезпечення ефективної інтеграції створюваної комп'ютерної системи «River Travels» із суміжними системами, важливо дотримуватися вимог до сумісності та взаємодії. Це включає налаштування стабільних і безпечних інтерфейсів для обміну даними, використання стандартних протоколів для інтеграції та забезпечення надійного захисту даних що передаються. Також система

має підтримувати актуальні версії API для забезпечення взаємодії із зовнішніми сервісами, які можуть включати платіжні системи, соціальні мережі та аналітичні інструменти. Важливо також враховувати потребу в гнучкості для майбутніх модернізацій та оновлень, що дозволить системі адаптуватися до змін у технологіях та бізнес-процесах.

#### **2.1.1.1.4 Вимоги до режимів функціонування системи**

Система «River Travels» повинна забезпечувати стабільне та безперервне функціонування в різних режимах для задоволення потреб підприємства. Важливо враховувати вимоги до автономності роботи системи під час відсутності інтернет-з'єднання та забезпечити режими реального часу для обробки запитів бронювання. Система має бути здатною до швидкого відновлення після збоїв із мінімальною втратою даних. Також необхідно передбачити можливість масштабування системи для обробки піків навантажень, що є типовим для туристичного сектору в сезонні періоди.

#### **2.1.1.1.5 Вимоги до діагностування системи**

Важливо забезпечити наявність автоматизованих засобів для перевірки стану всіх компонентів системи, включаючи сервери, мережі та прикладні програми. Система повинна надавати детальні логи та звіти про виконання операцій, які допоможуть в ідентифікації та аналізі збоїв або неправильної роботи компонентів. Також необхідно розробити процедури регулярних перевірок та тестувань системи для попередження потенційних проблем.

#### **2.1.1.1.6 Перспективи розвитку, модернізації системи**

Для забезпечення тривалої ефективності та відповідності до сучасних технологічних стандартів, система "River Travels" повинна мати чітко визначені перспективи розвитку та можливості модернізації. План розвитку має включати інтеграцію новітніх технологій, таких як штучний інтелект і машинне навчання, для покращення аналізу даних та персоналізації сервісів. Важливо передбачити

адаптацію системи до зростаючих обсягів даних та користувачів через вдосконалення масштабованості та процесів обробки даних.

Також слід розглянути можливість розширення функціональності системи з введенням додаткових сервісів, які можуть включати інтеграцію з віртуальною та доповненою реальністю для збагачення клієнтського досвіду. Регулярне оновлення безпекових протоколів та впровадження сучасних методів захисту даних повинні бути невід'ємною частиною стратегії розвитку системи.

### **2.1.1.2 Вимоги до показників призначення**

**Надійність:** Забезпечення стабільної роботи системи з мінімальною кількістю збоїв. Показник надійності може бути виражений через час між відмовами (MTBF, Mean Time Between Failures), який повинен становити не менше ніж 10,000 годин.

**Час відгуку:** Система повинна обробляти запити користувачів швидко, ідеально в межах 1-2 секунд для 95% запитів, що гарантує високий рівень користувацького досвіду.

**Масштабованість:** Система повинна бути здатна обслуговувати зростаючу кількість користувачів та обсяги даних. Показник масштабованості може бути вимірний через здатність системи підтримувати збільшення кількості одночасних користувачів на 50% без деградації продуктивності.

**Доступність:** Система має бути доступною для користувачів протягом мінімум 99,5% часу, що включає планові технічні перерви.

**Безпека:** Система має забезпечувати високий рівень захисту даних, з вимогами до шифрування, аутентифікації та контролю доступу. Показники безпеки повинні включати здатність виявляти та реагувати на 99% відомих загроз у реальному часі.

**Функціональність:** Система має повністю відповідати заявленим функціональним вимогам, забезпечуючи всі необхідні операції для управління резерваціями, клієнтськими відносинами, логістикою, фінансами та іншими відповідними процесами.

### **2.1.1.3 Вимоги до патентної чистоти**

Перевірка існуючих патентів та ліцензій: Перед розробкою та імплементацією системи необхідно провести детальний аналіз існуючих патентів та ліцензійних угод для виявлення потенційних порушень патентних прав.

Консультації з юристами: Співпраця з кваліфікованими патентними юристами для забезпечення відповідності всіх аспектів системи чинному законодавству про інтелектуальну власність.

Використання відкритого програмного забезпечення: Там, де це можливо, використовувати відкрите програмне забезпечення з відповідними ліцензіями, що дозволяють комерційне використання без порушення патентних прав.

Розробка власних рішень: Уникнення використання патентованих технологій шляхом розробки власних унікальних рішень та інновацій у рамках системи.

Ліцензування необхідних технологій: У випадку неминучості використання патентованих технологій необхідно забезпечити законне придбання ліцензій та дотримання умов їх використання.

### **2.1.1.4 Додаткові вимоги**

Для забезпечення надійної роботи та ефективної експлуатації комп'ютерної системи "River Travels", потрібно врахувати низку додаткових вимог:

Особливі умови експлуатації:

Система повинна бути адаптована до високих вимог щодо зносостійкості та стійкості до змін кліматичних умов, оскільки обладнання може використовуватися у різних локаціях.

Активне обладнання:

Необхідно забезпечити достатню кількість портів у комутаційному обладнанні з урахуванням потенційного розширення системи. Рекомендується передбачити запас портів на 20% більше поточних потреб.

Обладнання повинно підтримувати монтаж у стандартні стійки та мати можливість легкого доступу для обслуговування.

Кабель-канали та розетки:

Використання стандартизованих кабель-каналів, інформаційних та електричних розеток для забезпечення універсальності та легкості монтажу.

Кабель-канали мають бути достатньо міцними для захисту кабелів від фізичних пошкоджень.

Комунікаційне обладнання:

Розташування обладнання в приміщенні має враховувати легкий доступ для технічного обслуговування та достатнє вентилявання.

Тип шаф і методи кабельного підводу повинні забезпечувати організованість та захист кабельних трас.

Однорідність системи:

Використання єдиного типу кабелів, роз'ємів та інших компонентів для забезпечення сумісності та спрощення обслуговування.

Резервування:

Належне резервування критичних компонентів таких як комутатори та маршрутизатори та з'єднань для забезпечення безперервності роботи системи у випадку відмов.

Спеціальні вимоги:

Відповідно до вимог розробника чи замовника, можуть бути включені додаткові специфікації, наприклад, вимоги до енергоефективності чи компактності обладнання.

### **2.1.2 Вимоги функцій, виконуваним системою**

Підсистема бронювання та управління резерваціями:

Функції: Обробка замовлень, управління доступністю обладнання, автоматизація підтверджень резервацій.

Часовий регламент: Відповіді на запити користувачів мають надходити протягом 2 секунд.

Вимоги до якості: Висока надійність під час піків навантаження, точність даних резервації на 99.9%.



Вихідна інформація: Електронні квитки та підтвердження бронювання у PDF форматі.

Клієнтська підсистема (CRM):

Функції: Збір даних клієнтів, управління відносинами, аналіз поведінки клієнтів.

Часовий регламент: Оновлення даних клієнта у системі має відбуватися в реальному часі.

Вимоги до якості: Забезпечення конфіденційності даних клієнтів, точність аналітики на рівні 95%.

Вихідна інформація: Звіти щодо взаємодії з клієнтами, доступні в режимах CSV і Excel.

Фінансова підсистема:

Функції: Ведення бухгалтерського обліку, генерація фінансових звітів.

Часовий регламент: Звіти повинні бути готові до кінця наступного робочого дня після запиту.

Вимоги до якості: Забезпечення точності фінансових записів на рівні 99.9%.

Вихідна інформація: Фінансові звіти у форматах PDF та Excel.

Логістична підсистема:

Функції: Моніторинг місцезнаходження обладнання, оптимізація маршрутів доставки.

Часовий регламент: Оновлення статусу обладнання кожні 10 хвилин.

Вимоги до якості: Точність відстеження місцезнаходження на 98%.

Вихідна інформація: Інтерактивні карти та логістичні звіти.

Загальні вимоги:

Одночасність виконання: Система має бути здатна одночасно обробляти запити від усіх підсистем без втрати продуктивності.

Вірогідність видачі результатів: Має бути забезпечено високий рівень вірогідності видачі результатів, незалежно від кількості одночасно оброблюваних задач.

### **2.1.3 Вимоги до видів забезпечення комп'ютерної системи**

#### **2.1.3.1 Вимоги до математичного забезпечення**

Склад математичного забезпечення:

Математичні методи та моделі: Моделі оптимізації розкладу річкових турів.

Статистичні моделі для аналізу попиту та прогнозування. Економіко-математичні моделі для ціноутворення і бюджетування.

Типові алгоритми: Алгоритми кластеризації для сегментації клієнтів. Алгоритми навігації та маршрутизації для організації турів. Оптимізаційні алгоритми для планування ресурсів.

Алгоритми, що підлягають розробці: Розробка алгоритму динамічного ціноутворення відповідно до змін у попиті та пропозиції. Розробка алгоритмів для автоматизованого виявлення фроду в транзакціях.

Область застосування та обмеження: Математичні моделі та алгоритми будуть застосовуватися в управлінській системі для оптимізації внутрішніх процесів та підвищення якості обслуговування клієнтів. Обмеження застосування цих методів та моделей включають доступність та якість даних, юридичні та етичні аспекти обробки інформації.

Способи використання: Всі математичні методи та моделі мають бути інтегровані у корпоративну інформаційну систему через модулі бронювання та планування. Для ефективного впровадження алгоритмів необхідно забезпечити постійне оновлення даних та вдосконалення алгоритмічних рішень відповідно до змін у операційному середовищі підприємства.

#### **2.1.3.2 Вимоги до інформаційного забезпечення**

Склад, структура та способи організації даних у Системі:

Структура даних має бути оптимізована для швидкого доступу та ефективної обробки, з чітко визначеними схемами для всіх ключових сутностей, таких як клієнти, резервації, транзакції, тощо.

Нормалізація баз даних здійснюється для уникнення дублікації даних та підвищення інтегритету.

Інформаційний обмін між компонентами Системи:

Інтерфейси API повинні забезпечувати безпечний та ефективний обмін даними між компонентами, використовуючи сучасні протоколи, такі як REST або GraphQL.

Інформаційна сумісність із суміжними Системами:

Стандарти даних (наприклад, XML, JSON) і протоколи (наприклад, SOAP, REST) повинні бути уніфіковані для забезпечення сумісності з іншими системами та легкої інтеграції.

Застосування Систем керування базами даних:

Системи управління базами даних (СУБД), такі як MySQL, PostgreSQL або MongoDB, повинні бути налаштовані для забезпечення високої продуктивності, надійності та масштабованості.

Структура процесу збору, обробки, передачі даних у Системі і представлення даних:

Автоматизація збору даних з різних джерел і їх інтеграція в систему, забезпечення точності та актуальності інформації.

Методи обробки даних повинні включати валідацію, фільтрацію та трансформацію для відповідності бізнес-потребам.

Відображення даних має бути зрозумілим і зручним для кінцевих користувачів, забезпечуючи доступність важливої інформації через звіти, панелі керування тощо.

Контроль, збереження і відновлення даних:

Заходи безпеки для захисту даних від несанкціонованого доступу, включно з шифруванням, аутентифікацією та контролем доступу.

Резервне копіювання та відновлення даних мають бути частиною регулярних процедур для забезпечення відновлення системи після збоїв.

Аудит та моніторинг повинні використовуватися для постійного нагляду за станом даних та виявлення потенційних проблем з безпекою.

### **2.1.3.3 Вимоги до лінгвістичного забезпечення**

Лінгвістичне забезпечення системи "River Travels" має враховувати мовні та культурні аспекти взаємодії з клієнтами. Важливо забезпечити, щоб система була зрозумілою та доступною для користувачів різних мовних груп. Нижче наведені основні вимоги:

Мовна підтримка:

Багатомовність: Система має підтримувати кілька основних мов, зокрема українську, англійську, та інші мови, залежно від цільової аудиторії. Це дозволяє залучати більш широку клієнтську базу та поліпшувати користувацький досвід.

Локалізація інтерфейсу та документації: Всі інтерфейси користувача та документація мають бути перекладені та локалізовані з урахуванням культурних та мовних особливостей користувачів.

Технічні вимоги до лінгвістичної підтримки:

Підтримка Unicode: Для правильного відображення та обробки текстів на різних мовах система має використовувати Unicode. Це гарантує коректну роботу з символами всіх мовних алфавітів.

Використання мовних пакетів: Забезпечення можливості легкої зміни та оновлення мовних пакетів для адаптації до нових мовних ринків.

Адаптація під мовні звички: Система має враховувати лінгвістичні нюанси, такі як формати дат, чисел, адрес та інших локалізованих даних.

### **2.1.3.4 Вимоги до технічного забезпечення**

Система «River Travels» повинна використовувати тільки сучасні та сертифіковані технічні засоби, включаючи програмно-технічні комплекси та інші комплектуючі, що відповідають високим стандартам безпеки та продуктивності. Важливо забезпечити, щоб всі технічні засоби відповідали функціональним, конструктивним і експлуатаційним вимогам для надійної та безперервної роботи системи.

### 2.1.3.5 Вимоги до організаційного забезпечення

функціонування системи, мають бути чітко визначені з детальним описом процедур взаємодії між персоналом системи та персоналом на місцях впровадження. Організаційне забезпечення має також включати заходи для захисту системи від помилкових дій персоналу, що можуть призвести до збоїв чи аварій.

### 2.1.3.6 Вимоги до методичного забезпечення

Для системи "River Travels" повинна бути розроблена повна набір нормативно-технічної документації, включаючи застосовані стандарти, нормативи та методики, які регулюють її функціонування. Це забезпечить юридичну та технічну основу для її експлуатації та дозволить систематично підходити до управління та підтримки системи.

## 2.2 Розробка апаратної частини комп'ютерної системи

### 2.2.1 Розробка загальної архітектури мережі підприємства

Враховуючи загальну характеристику компанії, її архітектуру, кількість підмереж та специфічні вимоги, була розроблена структурна схема комплексу технічних засобів комп'ютерної системи, яка представлена на рисунку 2.1.

З'єднання між маршрутизаторами має бути реалізована за допомогою Serial DTE кабелів або крос-кабелів, а зв'язок між маршрутизаторами та комутаторами має здійснюватися через прямі кабелі, також як і підключення комп'ютерів до комутаторів. Для з'єднання комутаторів між собою мають бути використані крос-кабелі.

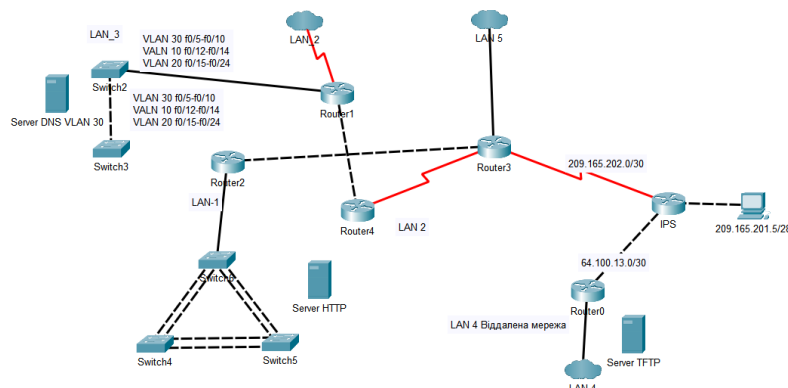


Рисунок 2.2 – Структурна схема комплексу технічних засобів комп'ютерної системи

### **2.2.2 Вибір і обґрунтування структурної схеми комплексу технічних засобів комп'ютерної системи**

Маршрутизатори та комутатори умовно розділяють мережу на кілька сегментів, забезпечуючи оптимальний потік даних та ізоляцію мережевого трафіку в рамках кожного VLAN. Таке розподілення сприяє зниженню мережевих заток і покращує безпеку за рахунок розділення різних типів трафіку.

Схема включає такі елементи:

Маршрутизатори, що з'єднують різні локальні мережі (LAN) та керують трафіком між ними.

Комутатори, які забезпечують підключення кінцевих пристроїв, таких як комп'ютери та сервери, та дозволяють їм комунікувати в межах однієї підмережі.

Сервери, що надають різні мережеві сервіси, включно з HTTP для веб-запитів та FTP для передачі файлів.

Кожен маршрутизатор та комутатор налаштований на певні VLAN, що дозволяє контролювати доступ до ресурсів та керувати пропускнуою спроможністю. Кабельні з'єднання між пристроями, такі як прямі та крос-кабелі, підібрані з урахуванням стандартів та фізичних вимог мережевої архітектури.

Структурна схема також показує, що система розрахована на забезпечення масштабованості. Додаткові порти на комутаторах та вільні інтерфейси на маршрутизаторах дозволяють легко розширити мережу в майбутньому без необхідності заміни основного обладнання. Схема на рисунку 2.2 забезпечує зрозумілість управління мережею, полегшує діагностику та технічне обслуговування.

### 2.2.3 Розробка специфікації апаратних засобів комп'ютерної системи

Маршрутизатор Cisco AXR2054+ став вибором для корпоративної мережі завдяки своїй високій продуктивності та здатності ефективно обробляти великі об'єми мережевих даних. Обладнаний двома WAN портами та дев'ятьма портами для підключення комутаторів із пропускною здатністю до 1 Gbps це як раз відповідає вимогам топологія на зараз та у разі масштабування системи, а також мережевим екраном, що підтримує до 5 Gbps, цей маршрутизатор забезпечує стабільне та безпечне з'єднання між мережевими пристроями, відповідаючи вимогам до швидкості та безпеки корпоративної інфраструктури.

Комутатор Cisco Catalyst 2960X-24TS-L використовується для побудови локальної мережі і оснащений 24 портами Fast Ethernet та двома портами із швидкістю до 1 Gbps, що дозволяє ефективно підключати робочі станції, сервери та інші мережеві пристрої. Підтримка VLAN, Quality of Service (QoS), Spanning Tree Protocol (STP) та Access Control Lists (ACLs) дозволяє гнучко налаштовувати мережеве обладнання, забезпечуючи високу швидкість передачі даних та великі можливості управління, безпеки та масштабування мережі.

Таблиця 2.1 – Специфікація обладнання

Позиція	Найменування і технічна характеристика	Тип, марка, позначення документа	Одиниці виміру	Кількість
1	2	3	4	5
1	Cisco AXR2054 System, Crypto, 4 built-in GE, Dual P/S, 20Gbit, 6x1000Base-X (SFP), 2x10G SFP+ інтегровані RP, SIP та ESP, 1xNIM, 1xSPA, RAM 8Gb, 2xAC	Cisco ASR1001-X Myxin_R1 Myxin_R2 Myxin_R3 Myxin_R4 Myxin_R5	Од.	5

## Продовження таблиці 2.1

2	Комутатор 24 x Ethernet 10/100/1000 Мбіт/сек, RIP v1, RIP v2, OSPF, USB-порт, LAN Base, 4 SFP слоти	Cisco Catalyst 2960X-24TS-L Cheredbychenko_SW1-23	Од.	23
4	Сервер оснащений двома процесорами Intel Xeon E5-2650L v2 з тактовою частотою 1.70-2.10 GHz, 8 GB оперативної пам'яті DDR3, двома портами Ethernet зі швидкістю 1 Gb, та контролером управління Cisco Integrated Management Controller (CIMC).	Cisco UCS C220 M3 LFF	Од.	3
5	Комп'ютер оснащений процесором AMD Ryzen 5 5600G з тактовою частотою від 3.9 до 4.4 ГГц, 16 GB оперативної пам'яті DDR4, накопичувачем SSD об'ємом 1 ТБ та графічним процесором AMD Radeon.	ARTLINE Business B38v08Win	Од.	331



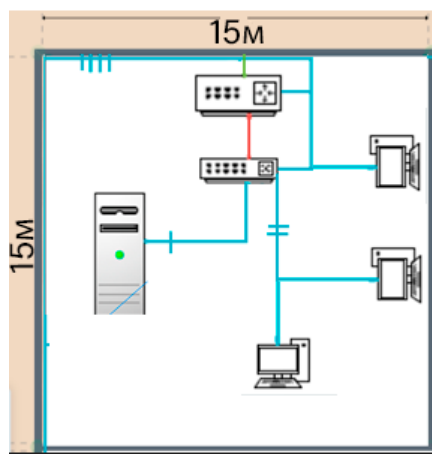


Рисунок 2.3 – Схема кабельної мережі LAN3

Таблиця 2.2 – Специфікація структурованої кабельної мережі

Позиція	Найменування	Тип, марка, позначення документа, опитувального листа	Одиниці	Кількість
1.	2.	3.	4.	5.
1.	Кабельний канал 40×25 мм	«ЭЛЕКОР»	м.	30
2.	Розетка комп'ютерна RJ-45 UTP подвійна	Hypernet MB-UTP	од.	89
3.	Lan кабель UTP КПВ-ВП cat.5E 4x2x0,51	Одескабель	м.	50
4.	Розетка із заземленням подвійна	Hypernet	од.	179
5.	Кабель живлення ПВС 3*2,5	Одескабель	м.	30
7.	Комутаційна коробка	E.NEXT	од.	1

#### 2.2.4 Розрахунок інтенсивності трафіку вихідного трафіку найбільшої локальної мережі підприємства

В підмережі встановлений комутатор Cisco2960, що об'єднує 179 ПК працівників. Вихідний трафік з комутатора SW1 надсилається до роутера R1 в лінію з пропускною здатністю, що становить 1000 Мбіт/с.

Для того, щоб комутатор не був перенасичений, швидкість надходження пакетів не повинна перевищувати швидкості їх відправлення. Вважаємо, що послугами одночасно користуються 100% користувачів. Середня інтенсивність трафіку  $\mu=198$  (кадрів/с), а середня довжина повідомлення – 1150 байт.

Теоретично припустимо, що всі користувачі найбільшої підмережі DLS одночасно використовують мережу. В такому разі, пропускна здатність на рівні доступу буде дорівнювати:

$$P_{p.p.} = \mu * L_{пов} * N * 8 = 198 * 1150 * 20 * 8 = 36.4 \text{ Мбіт/с} \quad (2.1)$$

де  $L_{пов}$  – середня довжина повідомлення;

$N$  – кількість вузлів в мережі.

Отриманий результат не перевищуватиме заданих параметрів мережі по вихідному каналу, отже перенавантажень не трапиться.

Комутатор SW1 також передає трафік до маршрутизатора зі швидкістю 1000 Мбіт/с. Отже, загальне навантаження на комутатор не повинно перевищувати:

$$\mu_{вих} = 109 / (1150 * 8) = 108\,696 \text{ пакетів/с} \quad (2.2)$$

Оскільки в середньому, кожне джерело виробляє 198 пакетів/с, то маршрутизатор обмежений кількістю приєднань, яку ми можемо дізнатись наступним чином:

$$N = \mu_{вих} / \mu = 108\,696 / 198 \approx 548 \text{ джерела} \quad (2.3)$$

Ця кількість задовольняє кількості вузлів у найбільшій нашій локальній мережі, до якої входить 179 ПК.

Кожен з 179 ПК посилає потік заявок з інтенсивністю у 196 кадрів/с. Звідси, можемо розрахувати інтенсивність вихідного трафіку:

$$\lambda = N * \mu = 179 * 196 = 35084 \text{ пакетів/с.} \quad (2.4)$$

Коефіцієнт затримки:

$$\rho = \frac{\lambda}{\mu_{вих}} = \frac{35084}{108696} = 0,32 \quad (2.5)$$

Коефіцієнт зайнятості маршрутизатора:

$$\frac{\rho}{1-\rho} = \frac{0,32}{1-0,32} = 0,47 \quad (2.6)$$

Середня затримка кадру, пов'язана з чергою М/М/1, дорівнює:

$$T = \frac{1}{(\mu-\lambda)} = \frac{1}{(108696 - 35084)} = 1,33 \text{ мкс} \quad (2.7)$$

Середня довжина черги:

$$L_{\text{чер}} = \frac{\rho^2}{1-\rho} = \frac{0,32^2}{1-0,32} = 0,15 \quad (2.8)$$

Середній час перебування пакета у черзі:

$$T_{\text{оч}} = \frac{L_{\text{чер}}}{\lambda} = \frac{0,15}{35084} = 0,48 \text{ мкс} \quad (2.9)$$

Це значення задовольняє вимогам до затримки в ЛМ.

## **3 РОЗРОБКА КОРПОРАТИВНОЇ МЕРЕЖІ**

### **3.1 Проектування логічної топології мережі**

Топологія організована з використанням комутаторів та маршрутизаторів, що забезпечують з'єднання між різними відділами та мережевими сегментами. Ключовим елементом є інтеграція VLAN, яка дозволяє ефективно розділити мережеві ресурси на основі функціональних потреб без зміни фізичної структури мережі. Це забезпечує високий рівень безпеки та оптимізацію трафіку, що особливо важливо для корпоративних мереж великих масштабів.

На рисунку 3.1 показана структура корпоративної мережі. Вона включає основну і віддалену мережі, а також мережу провайдера. Ці мережі з'єднані між собою за допомогою SerialEthernet та GigabitEthernet кабелів.

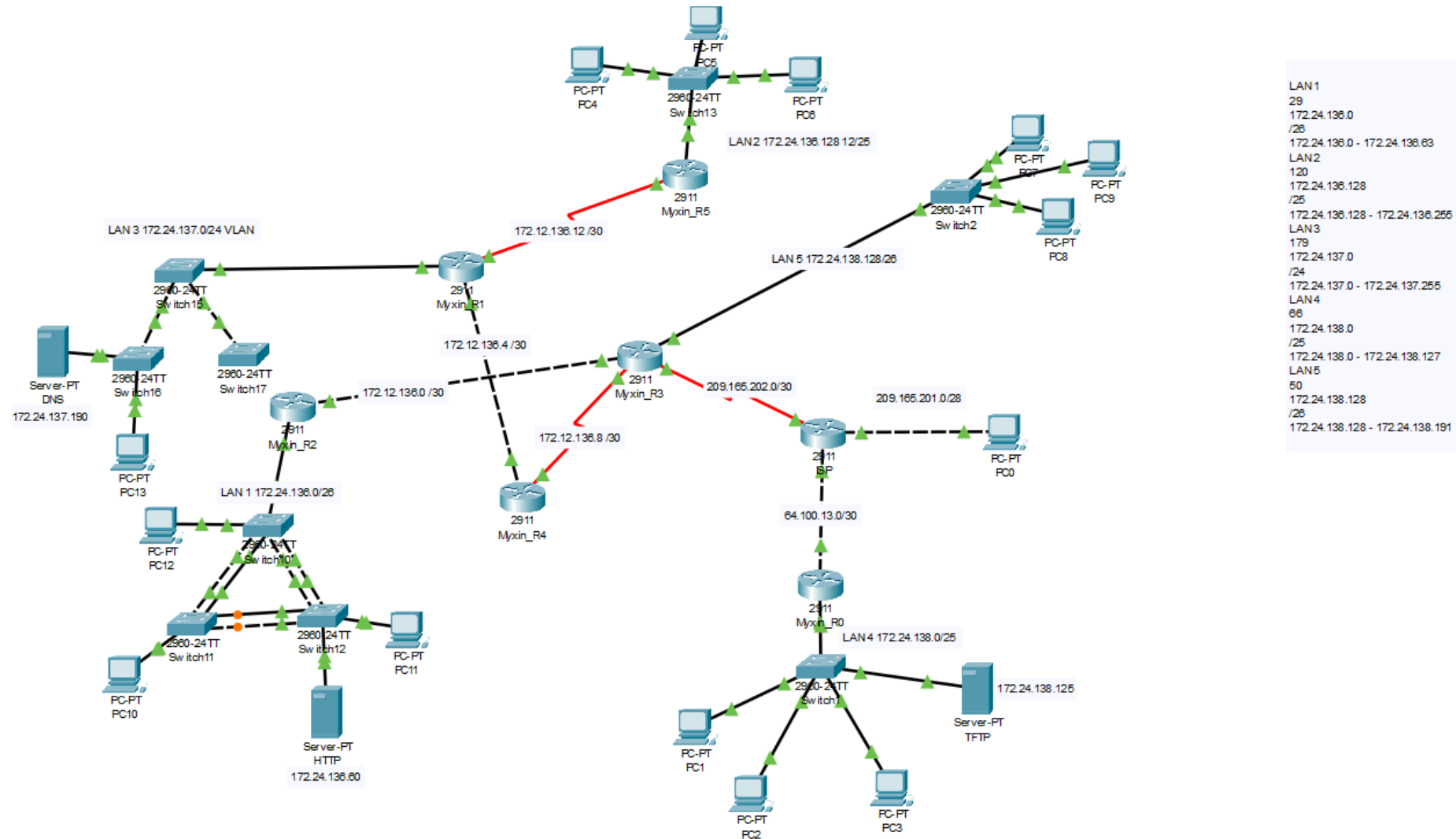


Рисунок 3.4 – Топологічна схема корпоративної мережі

### **3.2 Вибір та опис мережного обладнання**

Для проектування мережі компанії «River Travels» було обрано комутатори та маршрутизатори від відомого виробника Cisco, що забезпечують високу надійність та продуктивність роботи мережі.

Комутатори Cisco 2960: Ці комутатори є частиною Cisco Catalyst серії, які підтримують технології Power over Ethernet (PoE), що дозволяє жити кінцеве обладнання, таке як VoIP телефони або IP камери, без потреби в окремому джерелі живлення. Така функціональність сприяє зменшенню витрат на проводку та спрощенню управління мережевим обладнанням. Комутатори Cisco 2960 підтримують різні конфігурації портів, включаючи Gigabit Ethernet, що забезпечує високу пропускну здатність для обробки мережевого трафіку в корпоративних мережах.

Маршрутизатори Cisco 2911: Ці маршрутизатори відносяться до серії Cisco ISR (Integrated Services Routers) і призначені для забезпечення високої продуктивності при роботі в складних мережах з великою кількістю мережевих сервісів. Модель 2911 підтримує модульність, що дозволяє додавати нові інтерфейси та сервіси без необхідності заміни обладнання. Маршрутизатори забезпечують високу безпеку передачі даних завдяки вбудованим засобам шифрування та підтримці VPN, що критично важливо для забезпечення захищеного зв'язку між різними локаціями компанії.

Вибір такого обладнання для мережі «River Travels» виправданий їх високою надійністю, легкістю управління та можливістю розширення функціональності, що дозволяє компанії ефективно масштабувати мережеві ресурси згідно зі зростанням бізнесу та новими вимогами.

### **3.3 Розрахунок схеми адресації корпоративної мережі**

Поділ мережі на підмережі полягає у розподілі великого блоку IP-адрес на менші, ізольовані сегменти. У таблиці 3.1 представлено адресний блок мережі разом із кількістю вузлів для кожної підмережі.

Таблиця 3.3 – Блок адрес мережі та кількість вузлів в кожній підмережі

№	Блок адрес	LAN1	LAN2	LAN3	LAN4	LAN5
12	172.24.136.0/24	29	120	179	66	50

Задача полягає у створенні п'яти підмереж для 331 користувача, використовуючи технологію VLSM (Variable Length Subnet Masking), яка дозволяє створювати підмережі з різними довжинами масок. Цей метод надає можливість адаптивного поділу IP-адресного простору на великі чи малі блоки залежно від потреб користувачів, що підвищує ефективність використання ресурсів та збереження IP-адрес. Завдяки VLSM покращуються масштабованість та управління мережею.

1) Підмережа LAN1 для 29 хостів

– Потрібна кількість хостів: 29

– Маска підмережі: /26

– Діапазон адрес: 172.24.136.0 - 172.24.136.63

– Розрахунок маски: Маска /26 означає, що перші 26 бітів маски підмережі використовуються для адресації мережі, а решта 6 бітів — для хостів. Бітова адресація: 11111111.11111111.11111111.11000000

Це в двійковому вигляді відповідає 255.255.255.192 у десятковій системі.

2) Підмережа LAN2 для 120 хостів

– Потрібна кількість хостів: 120

– Маска підмережі: /25

– Діапазон адрес: 172.24.136.128 - 172.24.136.255

– Розрахунок маски: Маска /25 означає, що перші 25 бітів маски підмережі використовуються для адресації мережі, а решта 7 бітів — для хостів. Бітова адресація: 11111111.11111111.11111111.10000000

Це в двійковому вигляді 255.255.255.128 у десятковій системі.

3) Підмережа LAN3 для 179 хостів

– Потрібна кількість хостів: 179

– Маска підмережі: /24

– Діапазон адрес: 172.24.137.0 - 172.24.137.255

– Розрахунок маски: Маска /24 означає, що перші 24 біти маски підмережі використовуються для адресації мережі, а решта 8 бітів — для хостів. Бітова адресація: 11111111.11111111.11111111.00000000

Це в двійковому вигляді 255.255.255.0 у десятковій системі.

4) Підмережа LAN4 для 66 хостів

– Потрібна кількість хостів: 66

– Маска підмережі: /25

– Діапазон адрес: 172.24.138.0 - 172.24.138.127

– Розрахунок маски: Аналогічно до другої підмережі, маска /25 має бітову адресацію: 11111111.11111111.11111111.10000000

255.255.255.128 у десятковій системі.

5) Підмережа LAN5 для 50 хостів

– Потрібна кількість хостів: 50

– Маска підмережі: /26

– Діапазон адрес: 172.24.138.128 - 172.24.138.191

– Розрахунок маски: Маска /26, як і для першої підмережі, має бітову адресацію: 11111111.11111111.11111111.11000000

255.255.255.192 у десятковій системі.

Це аналіз та розрахунок масок і бітових адрес для підмереж використовуючи технологію VLSM.

Таблиця 3.4 – Схема адресації мережі

Назва підмережі	Необхідна к-ть вузлів	Адреса підмережі	Маска Підмережі у Десятковому	Діапазон допустимих IP-адрес вузлів
LAN1	29	172.24.136.0	/26	172.24.136.0 - 172.24.136.63
LAN2	120	172.24.136.128	/25	172.24.136.128 - 172.24.136.255
LAN3	179	172.24.137.0	/24	172.24.137.0 - 172.24.137.255
LAN4	66	172.24.138.0	/25	172.24.138.0 - 172.24.138.127
LAN5	50	172.24.138.128	/26	172.24.138.128 - 172.24.138.191



Для зв'язку між маршрутизаторами буде використано адресний блок 172.12.136.0/24. Також застосуємо метод VLSM для розбиття цієї мережі на п'ять підмереж з двома вузлами у кожній. У таблиці 3.3 наведено схему адресації каналів між маршрутизаторами.

Таблиця 3.5 – Схема адресації каналів між маршрутизаторами

Назва мережі	Кількість вузлів	Номер мережі	Маска мережі	Початкове значення діапазону	Кінцеве значення діапазону
WAN1	2	172.12.136.0	/30	172.1.128.1	172.1.128.2
WAN2	2	172.12.136.4	/30	172.1.128.5	172.1.128.6
WAN3	2	172.12.136.8	/30	172.1.128.9	172.1.128.10
WAN4	2	172.12.136.12	/30	172.1.128.13	172.1.128.14

У таблиці 3.6 наведена адресація всіх маршрутизаторів мережі.

Таблиця 3.6 – Схема адресації пристроїв

Пристрій	Інтерфейс	IP-адреса	Маска
Myxin_R1	Se0/0/0	172.12.136.13	255.255.255.252
	Gig0/0	172.12.136.5	255.255.255.252
	Gig0/1	172.24.137.1	255.255.255.255
Myxin_R2	Gig0/1	172.24.136.1	255.255.255.128
	Gig0/0	172.12.136.1	255.255.255.252
Myxin_R3	Gig0/0	172.12.136.2	255.255.255.252
	Gig0/1	172.24.138.129	255.255.255.128
	Se0/0/0	209.165.202.1	255.255.255.252
	Se0/0/1	172.12.136.9	255.255.255.252
Myxin_R4	Se0/0/0	172.12.136.10	255.255.255.252
	Gig0/0	172.12.136.6	255.255.255.252

Продовження таблиці 3.6

Muxin_R5	Gig0/0	172.24.136.129	255.255.255.192
	Se0/0/0	172.12.136.14	255.255.255.252
Muxin_R0	Gig0/0	64.100.13.1	255.255.255.252
	Gig0/1	172.24.138.1	255.255.255.192

### 3.4 Вибір та налаштування способу маршрутизації

#### 3.4.1 Базове налаштування конфігурації пристроїв

Базове налаштування конфігурації пристроїв на прикладі Muxin\_R3:

hostname Muxin\_R3 // призначення назви пристрою

line console 0 // вхід в конфігураційний режим лінії консолі

password cisco // призначення паролю до консолі

login // вимикання анонімного доступу

line vty 0 15 // вхід в конфігураційний режим лінії VTY

password cisco // призначення паролю до лінії VTY

login // вимикання анонімного доступу

enable secret class // встановлення зашифрованого паролю для привілейного режиму

service password-encryption // шифрування паролів

banner motd #Muxin\_R3# // налаштування банера MOTD

line vty 0 15 // вхід в конфігураційний режим лінії VTY

transport input ssh // назначення використання протоколу SSH

login local // налаштування локальної аутентифікації

username 12321ck1\_Muxin password admincisco // призначення імені користувача

та паролю

ip domain-name Muxin\_R3 // налаштування імені домена

crypto key generate rsa // створення ключа шифрування

1024 // вибір довжини ключа шифрування

int se0/0/0 // вибір DCE-інтерфейсу

clock rate 128000 // встановлення значення тактової частоти

В LAN\_1 використовується технологія Etherchannel, яка дозволяє об'єднати декілька фізичних інтерфейсів мережевого пристрою в один логічний канал. Налаштування Etherchannel на прикладі комутатора з мережі:

```
interface range fa0/1-2 // вибір інтерфейсів
channel-group 1 mode active // налаштування режиму портової групи
interface port-channel 1 // вибір інтерфейсу портової групи
switchport mode trunk // налаштування портової групи в режим транку
switchport trunk allowed vlan all // встановлення всіх VLAN як дозволених для
проходження даних через транковий порт
interface range fa0/3-4
channel-group 2 mode active
interface port-channel 2
switchport mode trunk
switchport trunk allowed vlan all
```

Ці команди треба повторити на кожному комутаторі з підмережі де реалізовано Etherchannel.

### **3.4.2 Налаштування протоколу OSPF та DHCP для маршрутизаторів корпоративної мережі**

Протокол DHCP використовується для автоматичного призначення IP-адрес комп'ютерам у мережі. Це значно полегшує не лише адміністрування мережі та налаштування пристроїв, але й забезпечує більш ефективне використання ресурсів мережі. Автоматизація процесу призначення адрес дозволяє зберігати час та зменшувати ймовірність помилок під час конфігурації комп'ютерних пристроїв у мережі.

Налаштування DHCP на прикладі маршрутизатора Muxin\_R5:

```
ip dhcp excluded-address 172.24.136.129 172.24.136.134 // виключення вказаних
адрес з dhcp пулів
ip dhcp excluded-address 172.24.136.255
ip dhcp excluded-address 172.24.136.254
```

```
ip dhcp pool LAN-2 // створення та вказання адреси dhcp пулу
network 172.24.136.128 255.255.255.128 // вказання IP-адреси мережі
default-router 172.24.136.129 // вказання IP-адреси шлюзу
dns-server 172.24.137.190 // вказання IP-адреси dns сервера
```

Для забезпечення взаємодії користувачів з різних підмереж потрібно налаштувати маршрутизацію між цими мережами. Існують два основні підходи до цього процесу: статична і динамічна маршрутизація. У статичній маршрутизації маршрути встановлюються вручну, тоді як у динамічній вони автоматично оновлюються, що забезпечує більш гнучкий та автоматизований підхід до конфігурації мережі.

У нашому проекті ми плануємо використовувати протокол динамічної маршрутизації OSPF, який є одним з найпопулярніших у сучасних мережах. OSPF використовує алгоритм SPF для пошуку найкоротших маршрутів, що значно підвищує швидкість мережі. Крім того, серед переваг OSPF варто відзначити його високий рівень безпеки, масштабованість, підтримку VLSM та здатність інтеграції з обладнанням різних виробників.

Використання OSPF дозволить ефективно керувати мережевим трафіком, забезпечить стабільність та підвищить продуктивність нашої мережі.

Налаштування протоколу OSPF на прикладі маршрутизатора Muxin\_R3:

```
router ospf 1 // увімкнення протоколу
network 172.24.138.128 0.0.0.63 area 0 // анонсування всіх необхідних для
маршрутизації мереж
network 209.165.202.0 0.0.0.3 area 0
network 172.12.136.8 0.0.0.3 area 0
network 172.12.136.0 0.0.0.3 area 0
passive-interface default // відключення поширення оновлень за
замовчуванням на всіх портах
```

no passive-interface Serial0/0/0 // увімкнення поширення оновлень на портах  
через які будуть передаватись дані щодо підключених мереж

```
no passive-interface GigabitEthernet0/0
no passive-interface GigabitEthernet0/1
no passive-interface Serial0/0/1
```

На граничному маршрутизаторі Мухін\_Р3 налаштовуємо маршрут за замовчуванням до маршрутизатора ISP (інтернет-провайдер) і виконуємо його розповсюдження:

```
ip route 0.0.0.0 0.0.0.0 209.165.202.2 // налаштовуємо маршрут за замовчуванням
router ospf 1 // увімкнення протоколу
redistribute static subnets // увімкнення розповсюдження статичних маршрутів
```

через протокол OSPF

Додаємо статичний маршрут до мережі провайдера ISP:

```
ip route 209.165.201.0 255.255.255.240 209.165.202.2
```

### 3.4.3 Налаштування роботи Інтернет

Для того, щоб система отримала доступ до Інтернету, необхідно налаштувати технологію перетворення мережевих адрес NAT (Network Address Translation). Ця технологія забезпечує перетворення внутрішніх IP-адрес на публічні та навпаки, а також перетворення номерів портів, що дозволяє багатьом пристроям одночасно користуватися Інтернетом через обмежений набір публічних IP-адрес.

Для реалізації NAT-трансляції необхідно створити пул адрес NAT, який буде включати в себе діапазон публічних IP-адрес. Наприклад, пул адрес NAT може включати адреси від 209.165.202.5 до 209.165.202.30. Цей діапазон буде використовуватись для трансляції внутрішніх адрес у публічні при зверненні до Інтернету та навпаки.

Переглянемо налаштування NAT на прикладі прикордонного маршрутизатора Мухін\_Р3:

```
ip access-list extended NAT12
deny ip 172.24.136.0 0.0.0.63 172.24.138.0 0.0.0.127
deny ip 172.24.136.128 0.0.0.127 172.24.138.0 0.0.0.127
deny ip 172.24.137.0 0.0.0.255 172.24.138.0 0.0.0.127
```

```

deny ip 172.24.138.128 0.0.0.63 172.24.138.0 0.0.0.127
deny ip 172.12.136.0 0.0.0.255 172.24.138.0 0.0.0.127
permit ip 172.24.136.0 0.0.0.63 any
permit ip 172.24.136.128 0.0.0.127 any
permit ip 172.24.137.0 0.0.0.255 any
permit ip 172.24.138.128 0.0.0.63 any
permit ip 172.12.136.0 0.0.0.255 any
permit ip 172.24.0.0 0.0.255.255 any
ip nat pool Internet 209.165.200.6 209.165.200.30 netmask 255.255.255.224
ip nat inside source list NAT12 pool Internet
ip nat inside source static 172.24.138.125 209.165.200.3
ip nat inside source static 172.24.136.60 209.165.200.3
ip nat inside source static 172.24.137.190 209.165.200.3
interface Serial0/0/0
ip nat outside
interface Serial0/0/1
ip nat inside
interface GigabitEthernet0/0
ip nat inside
interface GigabitEthernet0/1
ip nat inside

```

### 3.5 Налаштування мереж VLAN, маршрутизації між VLAN

Використання VLAN забезпечує ефективне керування трафіком, враховуючи потреби різних груп користувачів чи пристроїв у мережі. Кожна VLAN може мати свої власні правила доступу та політики безпеки, що дозволяє забезпечити високий рівень захисту мережі в цілому.

Однією з ключових переваг використання технології VLAN є зменшення фізичного розташування пристроїв та кабелів. Замість того, щоб мати окремі фізичні мережні сегменти для кожної групи користувачів, VLAN дозволяє розділити мережу

логічно, що спрощує управління та підтримку мережі, а також зменшує витрати на обладнання та кабелі.

Крім того, використання VLAN підвищує рівень безпеки мережі, оскільки він дозволяє ізолювати трафік між різними групами користувачів. Це зменшує ризик несанкціонованого доступу до чутливої інформації та можливість атак від внутрішніх джерел. Таким чином, використання технології VLAN є важливим елементом для покращення ефективності, безпеки та контролю в сучасних комп'ютерних мережах.

Таблиця 3.7 – Адресація мереж VLAN

Назва	Мережева адреса	Маска	Діапазон використання
VLAN10	172.24.137.0	/26	172.24.137.0 - 172.24.137.63
VLAN20	172.24.137.64	/26	172.24.137.64 - 172.24.137.127
VLAN30	172.24.137.128	/26	172.24.137.128 - 172.24.137.191
VLAN99	172.24.137.192	/28	172.24.137.192 - 172.24.137.207

Налаштування VLAN на прикладі комутатора з мережі LAN3:

```
int range fa0/5-10 // вибір портів
```

```
switchport mode access // налаштування портів
```

```
switchport access vlan 10 // присвоювання портам влану
```

```
int range fa0/11-16
```

```
switchport mode access
```

```
switchport access vlan 20
```

```
int range fa0/17-24
```

```
switchport mode access
```

```
switchport access vlan 30
```

```
int range fa0/1-4
```

```
switchport mode trunk // налаштування портів в режим транку
```

```
switchport trunk native vlan 100 // налаштування власної мережі на транковому
```

порті

```
switchport trunk allowed vlan 42,22,32,99-100 //налаштування списку
```

дозволеніх VLAN на транковому порті

```
int vlan 99 // вибір VLAN
```

```
ip address 172.24.137.194 255.255.255.240 // призначення IP-адреси
ip default-gateway 172.24.137.193 // вказання IP-адреси шлюзу за замовчуванням
```

Налаштовуємо підінтерфейси на маршрутизаторі Мухін\_Р1, що будуть

виступати в ролі шлюзу для вказаних VLAN:

```
int g0/1.10 // вибір підінтерфейсу
encapsulation dot1Q 10 // встановлення мітки для вибраного порту
ip address 172.24.137.0 255.255.255.192 // вказання IP-адреси підінтерфейсу
int g0/1.20
encapsulation dot1Q 20
ip address 172.24.137.64 255.255.255.192
int g0/1.30
encapsulation dot1Q 30
ip address 172.24.137.128 255.255.255.192
int g0/1.99
encapsulation dot1Q 99
ip address 172.24.137.192 255.255.255.240
```

Для автоматичного призначення IP-адрес вузлам в різних VLAN буде використовуватись протокол DHCP.

Налаштування DHCP на маршрутизаторі Мухін\_Р1, який буде виступати в ролі DHCP-сервера:

```
ip dhcp excluded-address 172.24.137.1 172.24.137.5
ip dhcp excluded-address 172.24.137.65 172.24.137.70
ip dhcp excluded-address 172.24.137.129 172.24.137.133
ip dhcp pool LAN3-VLAN10
network 172.24.137.0 255.255.255.192
default-router 172.24.137.1
dns-server 172.24.137.190
ip dhcp pool LAN3-VLAN20
network 172.24.137.64 255.255.255.192
default-router 172.24.137.65
```



```
dns-server 172.24.137.190
ip dhcp pool LAN3-VLAN30
network 172.24.137.128 255.255.255.192
default-router 172.24.137.129
dns-server 172.24.137.190
```

### **3.6 Захист інформації в комп'ютерній системі від несанкціонованого доступу**

#### **3.6.1 Налаштування віртуальної приватної мережі VPN**

VPN - це технологія, що застосовується для створення безпечного тунелювання в незахищених мережах, таких як Інтернет. Використовуючи VPN, дані передаються через зашифроване з'єднання, що забезпечує конфіденційність та цілісність інформації, що передається між вузлами мережі. У нашому конкретному випадку, ми плануємо використовувати VPN для забезпечення безпечного підключення з віддаленої мережі до основної мережі.

Один з основних аспектів використання VPN - це забезпечення конфіденційності і безпеки даних під час їх трансляції через небезпечні мережі, такі як Інтернет. Шляхом шифрування даних та створення захищеного тунелю між віддаленими точками, VPN дозволяє користувачам передавати інформацію без ризику її перехоплення або модифікації третіми сторонами.

Окрім забезпечення безпеки, VPN дозволяє здійснювати з'єднання між віддаленими мережами або пристроями, які знаходяться у різних географічних регіонах. Це робить його ідеальним рішенням для організацій з розподіленими командами або філіалами, які потребують безпечного зв'язку між своїми мережами.

При використанні VPN, важливо правильно налаштувати і керувати доступом до мережевих ресурсів. Це включає в себе належне аутентифікування користувачів, контроль доступу та моніторинг активності в мережі, щоб забезпечити безпеку та прозорість використання мережевих ресурсів.

Налаштування VPN розглянемо на прикладі Muxin\_R0:

```
license boot module c2900 technology-package securityk9 // активація модуля securityk9
```

```
ip access-list extended VPN12 // створення ACL-списку VPN12, щоб визначити трафік з основної мережі до віддаленої
```

```
permit ip 172.24.138.0 0.0.0.63 172.24.136.0 0.0.0.63 // надання доступу на проходження пакетів з основної на віддалену мережу
```

```
permit ip 172.24.138.0 0.0.0.63 172.24.136.128 0.0.0.128
```

```
permit ip 172.24.138.0 0.0.0.63 172.24.137.0 0.0.0.0
```

```
permit ip 172.24.138.0 0.0.0.63 172.24.138.128 0.0.0.63
```

```
permit ip 172.24.138.0 0.0.0.63 172.12.136.0 0.0.0.255
```

```
crypto isakmp policy 10 // створення криптографічної політики
```

```
encr 3des // вибір алгоритму шифрування
```

```
hash md5 // вибір алгоритму створення геш-суми
```

```
authentication pre-share // вибір методу аутентифікації пірів
```

```
group 2
```

```
crypto isakmp key cisco address 209.165.202.1 // створення ключа для взаємодії з обраним партнером
```

```
crypto ipsec transform-set TS esp-3des esp-md5-hmac // створення набору перетворень
```

```
crypto map MAP 10 ipsec-isakmp // створення криптографічного зіставлення
```

```
set peer 209.165.202.1 // створення піра
```

```
set transform-set TS // вибір набору перетворень
```

```
match address VPN12 // прив'язка до списку VPN12
```

```
int GigabitEthernet0/1 // вибір інтерфейсу
```

```
crypto map MAP // прив'язка криптографічного зіставлення MAP до вихідного інтерфейсу
```

### 3.6.2 Налаштування маршрутизаторів на підтримку служби AAA

AAA, або Authentication, Authorization, and Accounting, є моделлю, що використовується для забезпечення керування доступом та контролю над мережевими

ресурсами. Ця модель включає в себе процеси авторизації, аутентифікації та обліку, які гарантують безпеку та ефективно використання мережі. Шляхом встановлення правильних політик доступу, AAA забезпечує контроль над тим, хто має доступ до ресурсів мережі і як вони можуть їх використовувати.

Одним з ключових компонентів моделі AAA є RADIUS-сервер. RADIUS (Remote Authentication Dial-In User Service) надає централізовану систему аутентифікації та авторизації для користувачів, що намагаються отримати доступ до мережевих ресурсів. Цей сервер виконує перевірку ідентифікаційних даних користувачів та встановлює їх права доступу на основі визначених політик безпеки.

Ще одним важливим аспектом моделі AAA є облік. Облік дозволяє вести журнал дій користувачів у мережі, включаючи інформацію про їх входи, вихідні ресурси та час, що вони витрачають у мережі. Ця інформація не лише допомагає відслідковувати активність користувачів, але й виявляти можливі проблеми безпеки або невідповідності політикам мережі.

Завдяки використанню моделі AAA з RADIUS-сервером, організації можуть забезпечити високий рівень безпеки та контролю над доступом до своїх мережевих ресурсів. Це особливо важливо в умовах розподіленої мережі або при роботі з великою кількістю користувачів, де керування доступом стає складним завданням.

Налаштовуємо всі маршрутизаторів на підтримку служби AAA на прикладі Мухін\_R3:

```
aaa new-model // увімкнення служби AAA
radius-server host 172.24.136.60 auth-port 1645 key radius123 // вказання IPадреси
RADIUS-серверу, порту підключення та ключа аутентифікації
aaa authentication login console group radius local // налаштування аутентифікації
для консольного доступу до мережевого пристрою з використанням RADIUS-сервера
line console 0 // вхід в режим конфігурації лінії консолі
login authentication console // встановлення методу аутентифікації для доступу
до консольного порту
aaa authentication login default local // створення локальної бази даних
користувачів
```

```
username Muxin password admin123 // налаштування логіну та паролю у
локальній базі
```

```
line vty 0 15 // вхід в режим конфігурації ліній віртуального терміналу
```

```
login authentication default // встановлення за замовчуванням методу
аутентифікації для доступу через VTY-порти
```

### 3.7 Перевірка комп'ютерної Системи підприємства

Проведено перевірку базових налаштувань обладнання за допомогою маршрутизатора Muxin\_R5 як прикладу. За допомогою команди `show running-config` у привілейованому режимі аналізується ряд параметрів, таких як ім'я пристрою, налаштування паролів для доступу до консолі та ліній vty, їх конфігурація для використання протоколу ssh, пароль для доступу до привілейованого режиму, налаштування банера MOTD і ім'я домену.

```
!
hostname Muxin_R5
!!
```

Рисунок 3.5 – Показ назви пристрою

```
|line con 0
|password 7 0822455D0A16
|login
|,
```

Рисунок 3.6 – Консольний доступ: пароль

```
line vty 0 4
password 7 0822455D0A16
login local
transport input ssh
line vty 5 15
password 7 0822455D0A16
login local
transport input ssh
!
```

Рисунок 3.7 – vty пароль та SSH

```
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCil
,
```

Рисунок 3.8 – Привілейований режим: пароль

```

!
banner motd ^CMyxin_R5^C
!
!

```

Рисунок 3.9 – Повідомлення MOTD

```

!
!
ip domain-name Myxin_R5
!

```

Рисунок 3.10 – Ім'я домену

```

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

Number of channel-groups in use: 2
Number of aggregators:          2

Group  Port-channel  Protocol    Ports
-----+-----+-----+-----
1      Po1(SU)        LACP       Fa0/1(P) Fa0/2(P)
2      Po2(SU)        LACP       Fa0/3(P) Fa0/4(P)

```

Рисунок 3.11 – Технологія EtherChannel

```

router ospf 1
log-adjacency-changes
passive-interface default
no passive-interface GigabitEthernet0/0
no passive-interface Serial0/0/0
network 172.12.136.12 0.0.0.3 area 0
network 172.24.136.128 0.0.0.127 area 0

```

Рисунок 3.12 – Налаштування OSPF

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC3	PC9	ICMP		0.000	N	0	(edit)	(delete)
	Successful	TFTP	PC9	ICMP		0.000	N	1	(edit)	(delete)

Рисунок 3.13 – Зв'язок між LAN\_4 та LAN\_5

```

209.165.201.0/28 is subnetted, 1 subnets
S    209.165.201.0 [1/0] via 209.165.202.2
S*  0.0.0.0/0 [1/0] via 209.165.202.2

```

Рисунок 3.14 – Маршрут за замовчуванням

```

User Access Verification

Username: myxin12321ck1
Password:
Myxin_R3>

```

Рисунок 3.15 – Служба AAA на маршрутизаторі

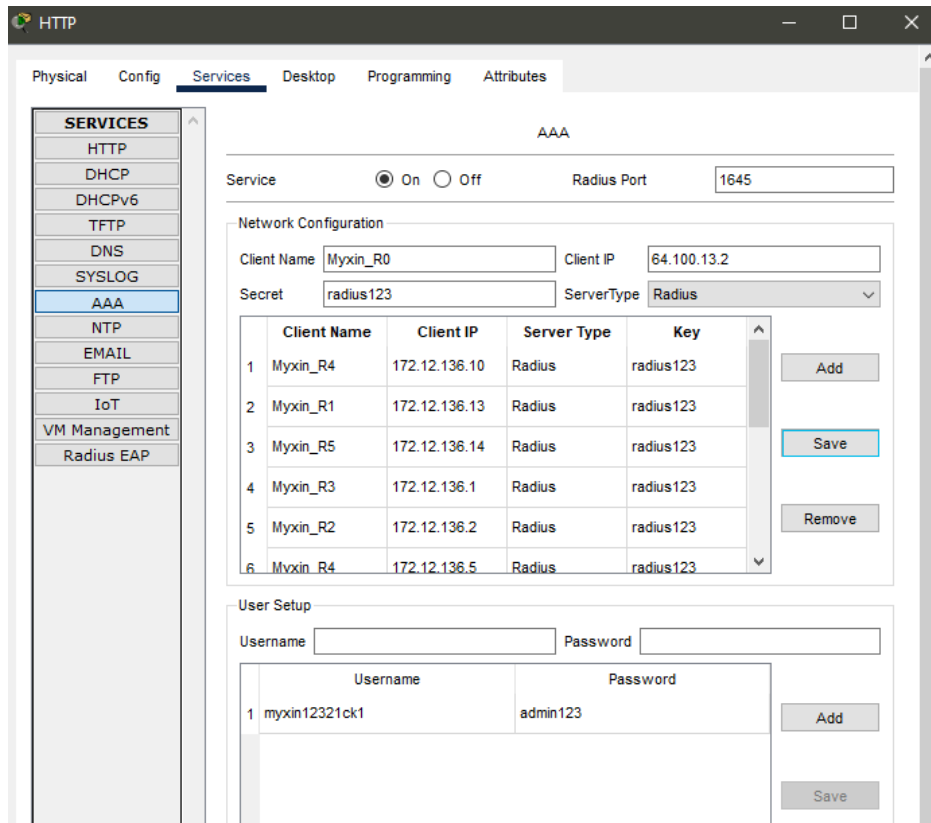


Рисунок 3.16 – Налаштування RADIUS-сервера

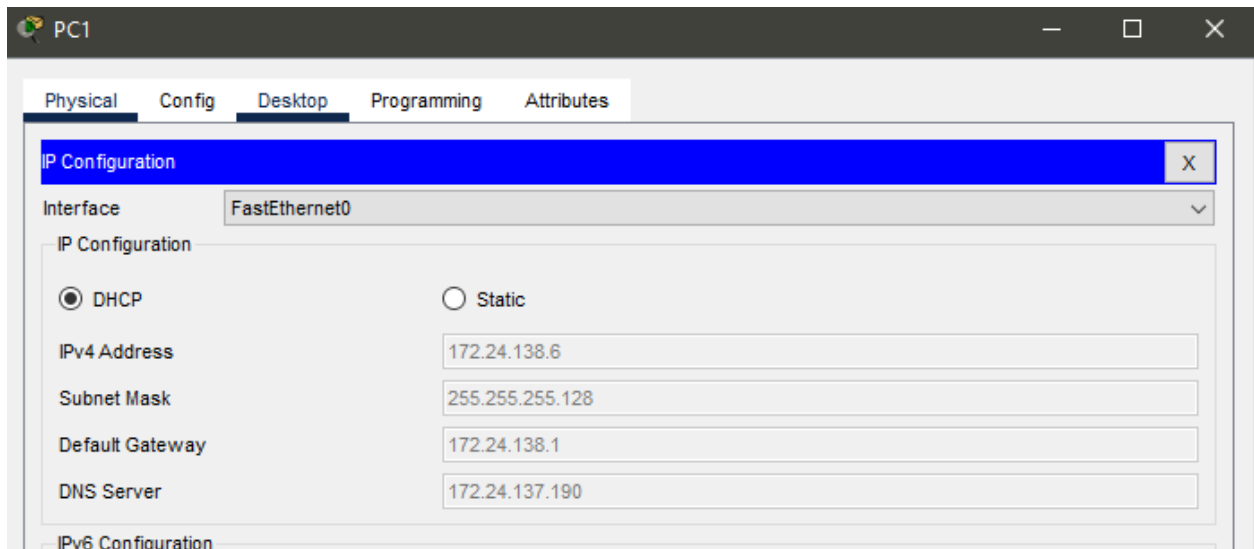


Рисунок 3.17 – IP-адреса комп'ютера PC1

```
Myxin_R3#show ip interface brief
Interface          IP-Address      OK? Method Status  Protocol
GigabitEthernet0/0 172.12.136.1   YES manual up      up
GigabitEthernet0/1 172.24.138.129 YES manual up      up
GigabitEthernet0/2 unassigned     YES unset  up      down
Serial0/0/0        209.165.202.1 YES manual up      up
Serial0/0/1        172.12.136.9   YES manual up      up
Vlan1              unassigned     YES unset  administratively down down
```

Рисунок 3.18 – IP-адреси маршрутизатора

VLAN Name	Status	Ports
1 default	active	Fa0/4, Fa0/5, Gig0/1, Gig0/2
10 VLAN0010	active	Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/10
20 VLAN0020	active	Fa0/11, Fa0/12, Fa0/13, Fa0/14 Fa0/15, Fa0/16
30 VLAN0030	active	Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0
10	enet	100010	1500	-	-	-	-	-	0	0
20	enet	100020	1500	-	-	-	-	-	0	0
30	enet	100030	1500	-	-	-	-	-	0	0
1002	fddi	101002	1500	-	-	-	-	-	0	0
1003	tr	101003	1500	-	-	-	-	-	0	0
1004	fdnet	101004	1500	-	-	-	ieee	-	0	0
1005	trnet	101005	1500	-	-	-	ibm	-	0	0

VLAN Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
Remote SPAN VLANs									

Primary	Secondary	Type	Ports

Рисунок 3.19 – Імена та порти VLAN

```
Switch#show interfaces tr
Switch#show interfaces trunk
Port      Mode      Encapsulation  Status      Native vlan
Fa0/1     on        802.1q         trunking    1
Fa0/2     on        802.1q         trunking    1
Fa0/3     on        802.1q         trunking    1

Port      Vlans allowed on trunk
Fa0/1     1-1005
Fa0/2     1-1005
Fa0/3     1-1005

Port      Vlans allowed and active in management domain
Fa0/1     1,10,20,30
Fa0/2     1,10,20,30
Fa0/3     1,10,20,30

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1     1,10,20,30
Fa0/2     1,10,20,30
Fa0/3     1,10,20,30
```

Рисунок 3.20 – Транкові порти

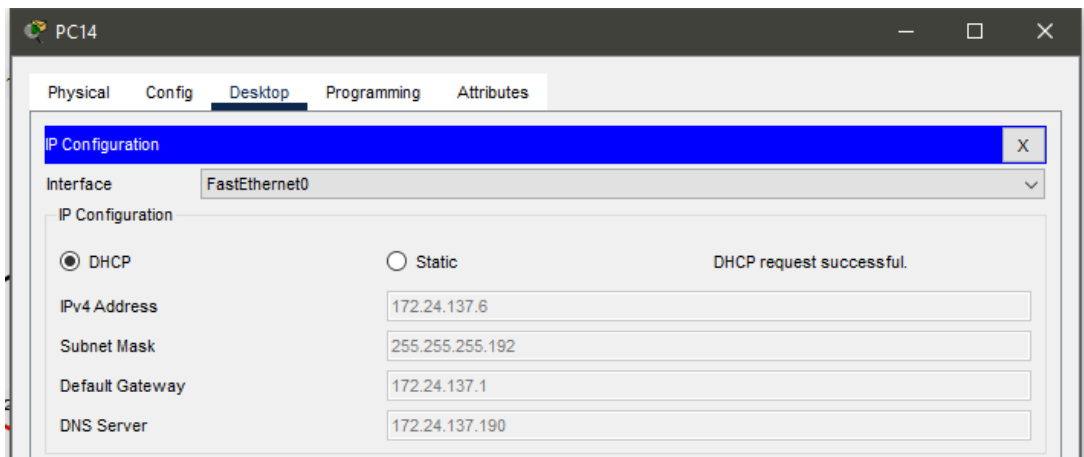


Рисунок 3.21 – IP-адреса PC14 VLAN

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC13	PC14	ICMP		0.000	N	0	(edit)	(delete)
	Successful	PC14	PC13	ICMP		0.000	N	1	(edit)	(delete)

Рисунок 3.22 – Зв'язок між VLAN10 та VLAN20

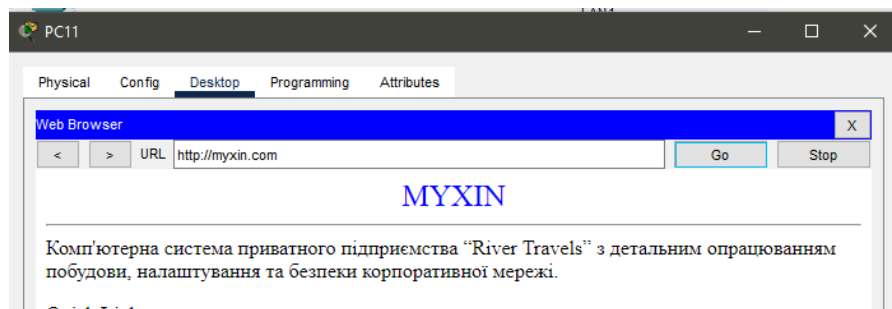


Рисунок 3.23 – Відкритий веб-сайт з відомостями про тему та завдання на кваліфікаційну роботу студента



## 4 РОЗРОБКА КОМПОНЕНТА БЕЗПЕКИ ТА КЛІМАТ КОНТРОЛЮ

### 4.1 Інженерне рішення по розробці компонента Системи

Інтернет речей представляє собою мережу взаємопов'язаних фізичних об'єктів, здатних до підключення до Інтернету та взаємодії між собою. Система Інтернету речей зазвичай включає в себе датчики, що неперервно моніторять умови зовнішнього середовища, і пристрої, які активуються або деактивуються залежно від даних цих датчиків та налаштувань, заданих користувачем. Це дозволяє автоматизувати такі процеси, як управління освітленням, регулювання температури чи вологості та інші.

Замовник модернізації комп'ютерної мережі побажав додати IoT пристрої на віддалену мережу тому що це підмережа прокату компанії та вона повинна виконувати такі функції

- При виявленні вогню активується сирена;
- При реєстрації руху включається веб-камера;
- При температурі вище 24 вмикається кондиціонер та при меншій ніж 22 вимикається;
- При успішному скануванні ID-картки відчиняються двері.

Зв'язок між компонентами Інтернету речей та центральним шлюзом HomeGateway реалізовано за допомогою бездротового з'єднання Wi-Fi, що відповідає стандарту IEEE 802.11. Це дозволяє забезпечити стабільне та швидке підключення між пристроями, не обмежуючись фізичними з'єднаннями. Управління всіма компонентами системи Інтернету речей здійснюється через мобільний додаток на смартфоні, що синхронізований з HomeGateway, надаючи користувачу можливість контролювати різноманітні функції дистанційно.

Інтеграція системи Інтернету речей включає різноманітне розміщення датчиків у головній та віддаленій мережах.

## 4.2 Налаштування обладнання та сервісів системи IoT

Початковий етап впровадження системи Інтернету речей для забезпечення безпеки віддаленої мережі включає інсталяцію різних IoT-пристроїв та датчиків, а також інтеграцію смартфона для управління системою. Все обладнання підключається через центральний шлюз — HomeGateway, який слугує як основний вузол для координації та обміну даними між усіма компонентами системи. Це дозволяє централізувати управління безпекою та спростити моніторинг стану об'єкту.

На шлюзі HomeGateway, що знаходиться в межах віддаленої мережі клініки, налаштовується бездротова точка доступу з унікальним ідентифікатором SSID «Muxin» та паролем «Muxin12321sk», що забезпечує захищене з'єднання за допомогою протоколу безпеки WPA2-PSK з використанням алгоритму шифрування AES. Ці параметри гарантують високий рівень безпеки переданих даних. Кожен IoT-пристрій налаштовується на підключення до Home Gateway, вводячи вказані SSID та пароль, що сприяє їхній інтеграції в єдину мережу. Відповідну топологічну схему корпоративної мережі клініки з ілюстрацією розміщення IoT-пристроїв можна знайти на рисунку 4, що допомагає візуалізувати і оптимізувати всю конфігурацію системи.

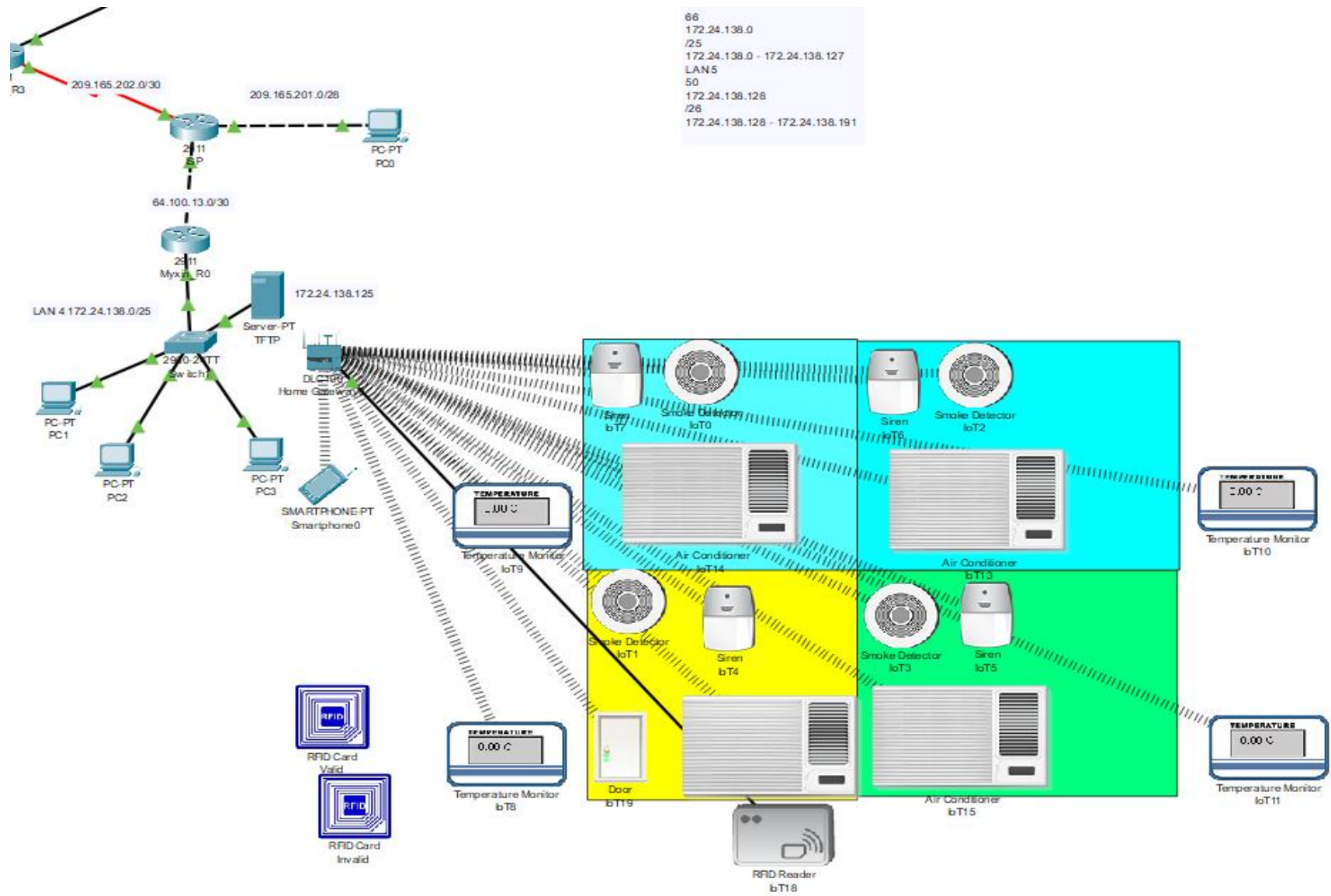


Рисунок 4.1 – Топологічна схема корпоративної мережі

Для налаштування роботи IoT-системи на смартфоні відкриваємо програму IoT Monitor, вводимо адресу шлюзу і виконуємо вхід за допомогою логіна та пароля. Після цього на екрані з'являється сторінка зі списком усіх підключених IoT-пристроїв, яка показана на рисунку 4.2. Потім переходимо до вкладки "Conditions" і натискаємо кнопку "Додати", щоб налаштувати нові умови для роботи пристроїв.

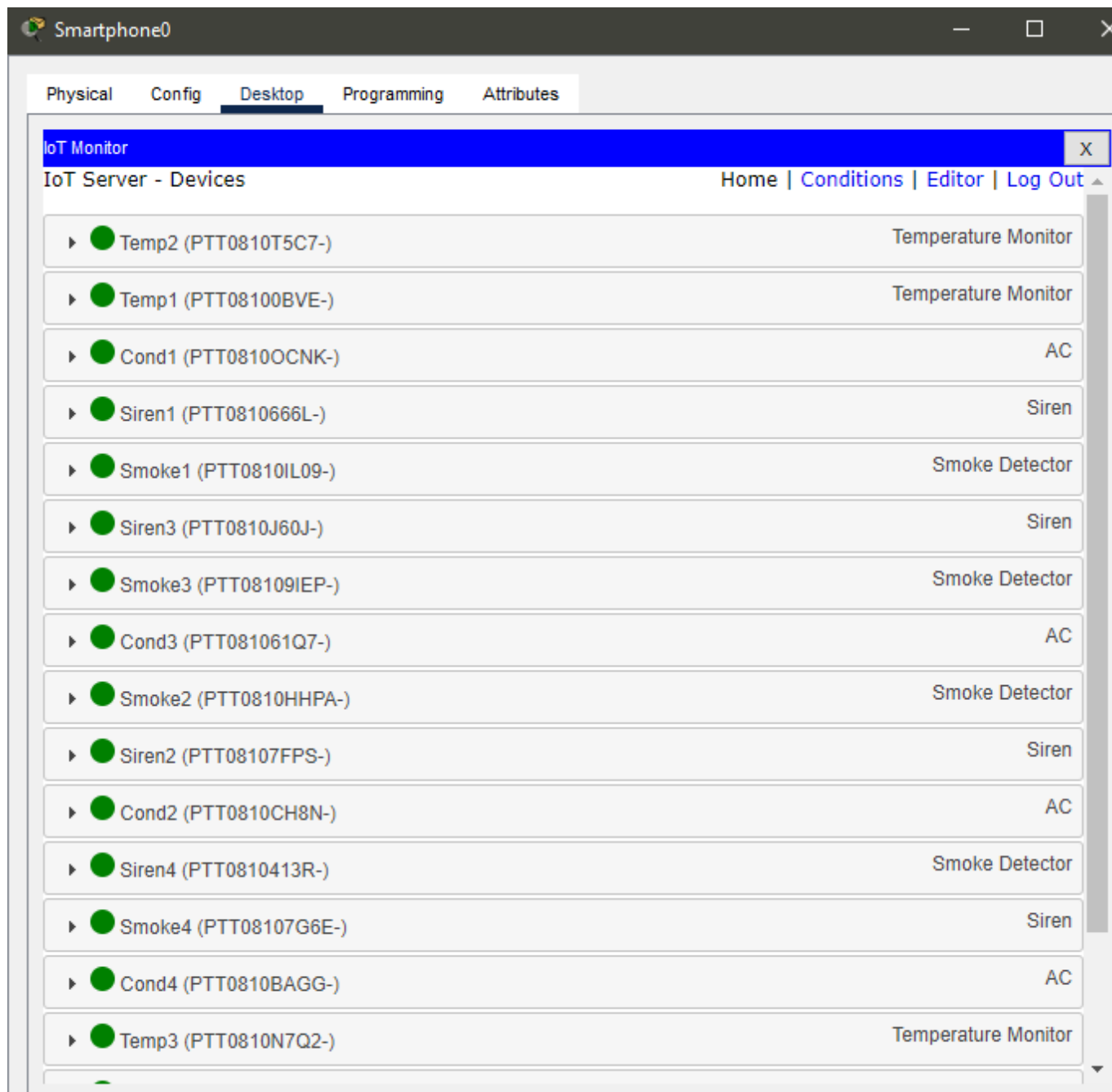


Рисунок 4.2 – Під'єднані IoT-пристрої мережі

Створення правила для детекторів диму, при спрацюванні будь-якого вмикається сирена у всій будівлі та відчиняються двері а при передачі що на всіх датчиках нормальний рівень вуглекислого газу то сирена вимикається та будівля переходить у нормальне функціонування. Налаштування правил показані на рисунках 4.3-4.4.

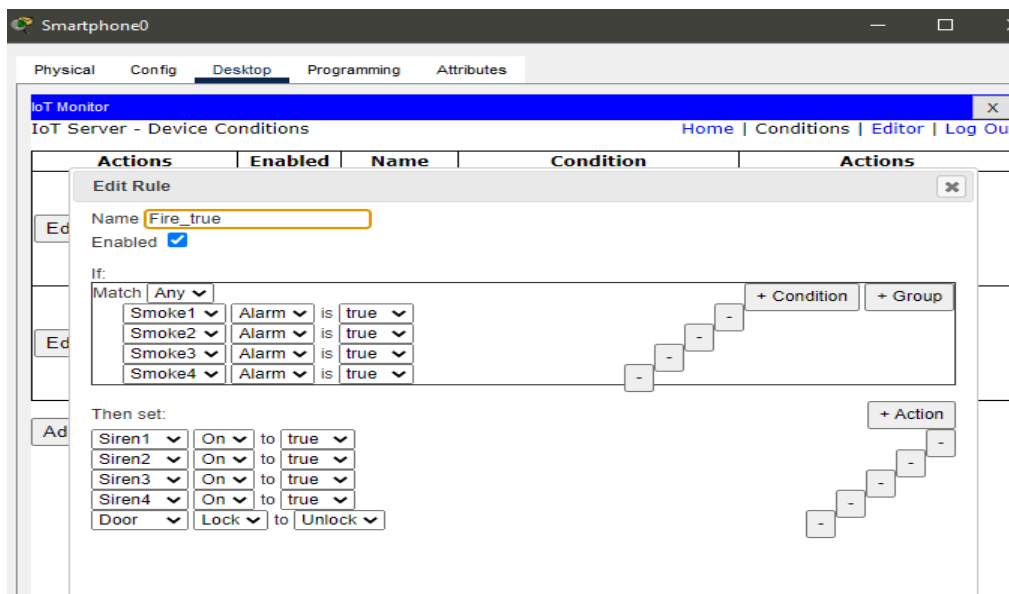


Рисунок 4.3 – Правила при умові виявлення диму

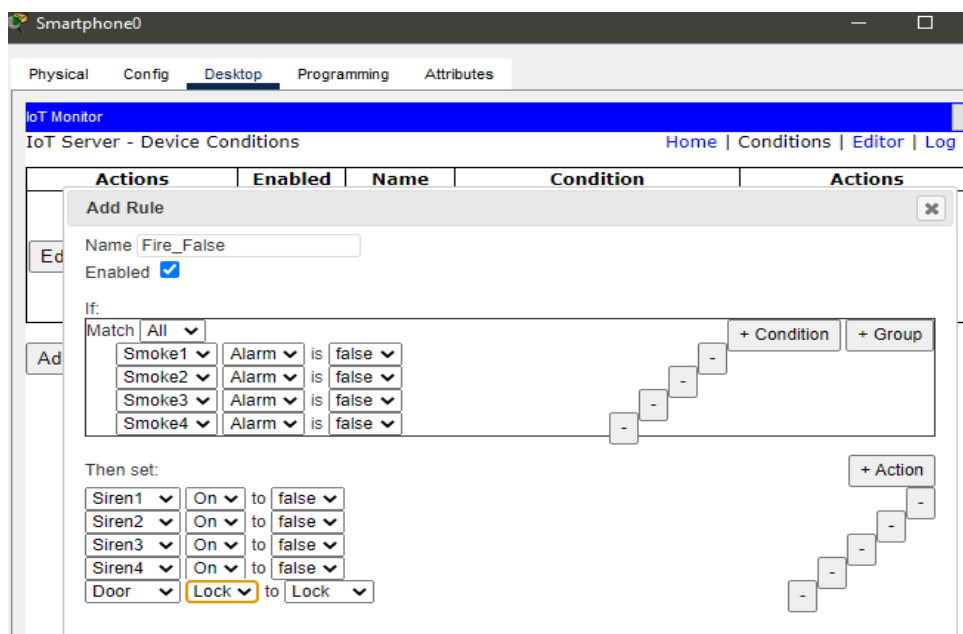


Рисунок 4.4 – Правила при умові не виявлення диму

Наступним етапом є написання правила для розумного клімат контролю з використанням кондиціонерів, для кожної кімнати своє правило яке наведено на рисунку 4.5.

Edit	Remove	Yes	Temp1ON	Temp1 Temperature $\geq$ 24.0 °C	Set Cond1 On to true
Edit	Remove	Yes	Temp1OFF	Temp1 Temperature $<$ 22.0 °C	Set Cond1 On to false
Edit	Remove	Yes	Temp2ON	Temp2 Temperature $\geq$ 24.0 °C	Set Cond2 On to true
Edit	Remove	Yes	Temp2OFF	Temp2 Temperature $<$ 22.0 °C	Set Cond2 On to false
Edit	Remove	Yes	Temp3ON	Temp3 Temperature $\geq$ 24.0 °C	Set Cond3 On to true
Edit	Remove	Yes	Temp3OFF	Temp3 Temperature $<$ 2.0 °C	Set Cond3 On to false
Edit	Remove	Yes	Temp4ON	Temp4 Temperature $\geq$ 24.0 °C	Set Cond4 On to true
Edit	Remove	Yes	Temp4OFF	Temp4 Temperature $<$ 22.0 °C	Set Cond4 On to false

Рисунок 4.5 – Правила для розумного клімат контролю

Правило для входу в будівлю за допомогою ключ карти наведено на рисунку 4.6.

Edit	Remove	Yes	KEY_VALID	REader Card ID = 1	Set REader Status to Valid
Edit	Remove	Yes	KEY_INVALID	REader Card ID $\neq$ 1	Set REader Status to Waiting
Edit	Remove	Yes	Door_open	REader Status is Valid	Set Door Lock to Unlock
Edit	Remove	Yes	Door_lock	REader Status is Waiting	Set Door Lock to Lock

Рисунок 4.6 – Правило для входу в будівлю

### 4.3 Перевірка роботи компонента Системи

Для перевірки функціональності зчитувача ID-карток було додано карти з номерами 1 і 1001 для випадків спрацювання і невідповідно. Проводимо перевірку роботи зчитувача за допомогою цих карток (див. рисунки 4.7-8).

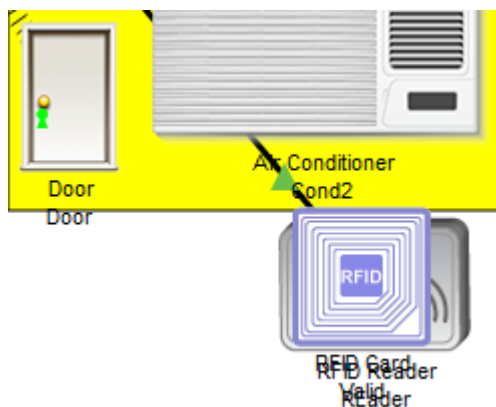


Рисунок 4.7 – Піднесення валідної картки

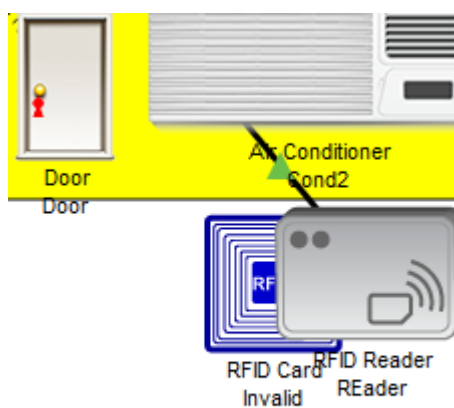


Рисунок 4.8 – Піднесення не дійсної картки

Перевіряємо роботу детекторів диму при спрацюванні та у звичайній ситуації (рис. 4.9-10).

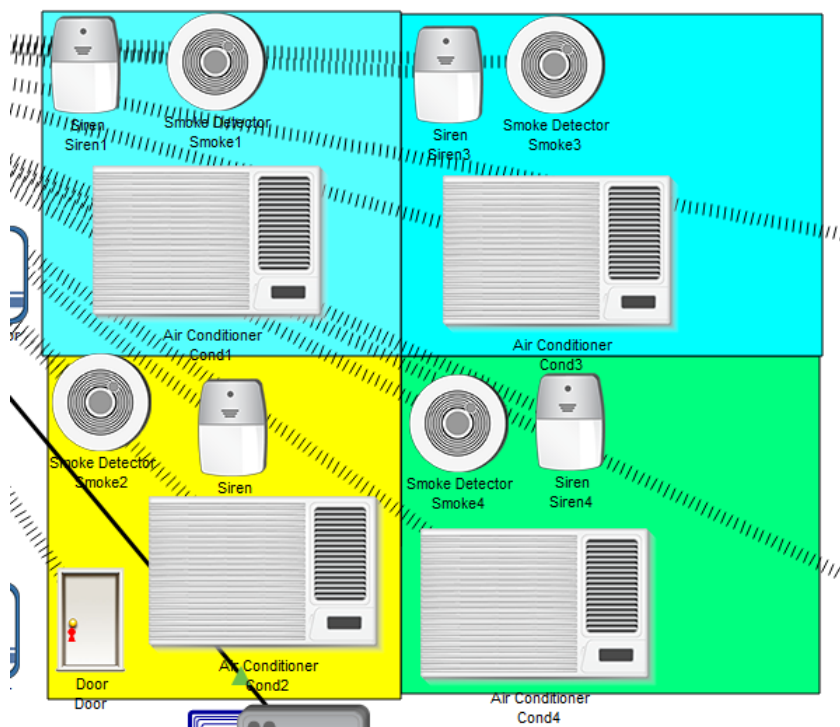


Рисунок 4.9 – Звичайна ситуація

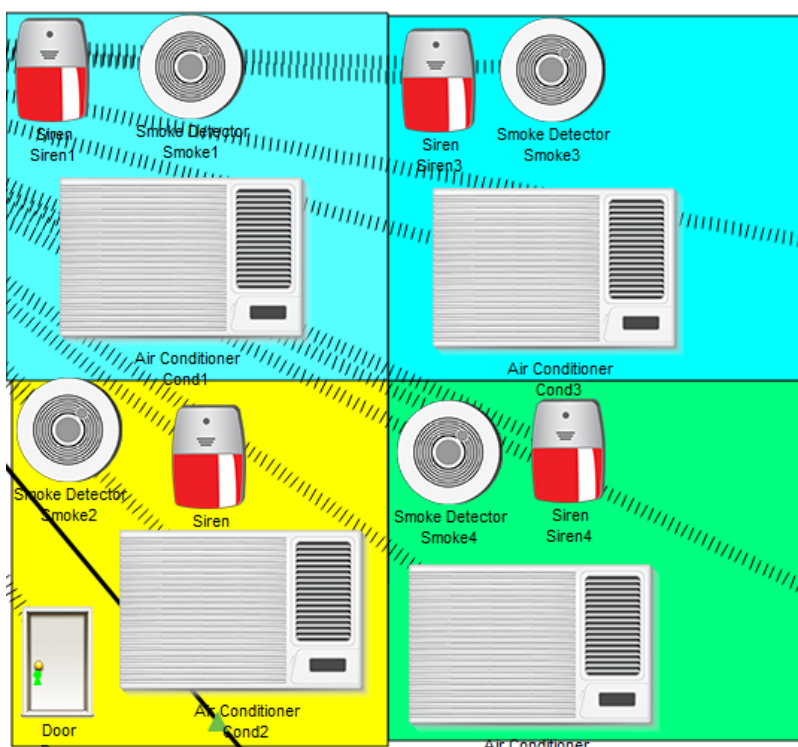


Рисунок 4.10 – При наявності диму



Перевірка спрацювання розумного клімат контролю при більше 24 градусів вмикається система кондиціонерів при меншому за 22 вмикається на рисунках 4.11-12.

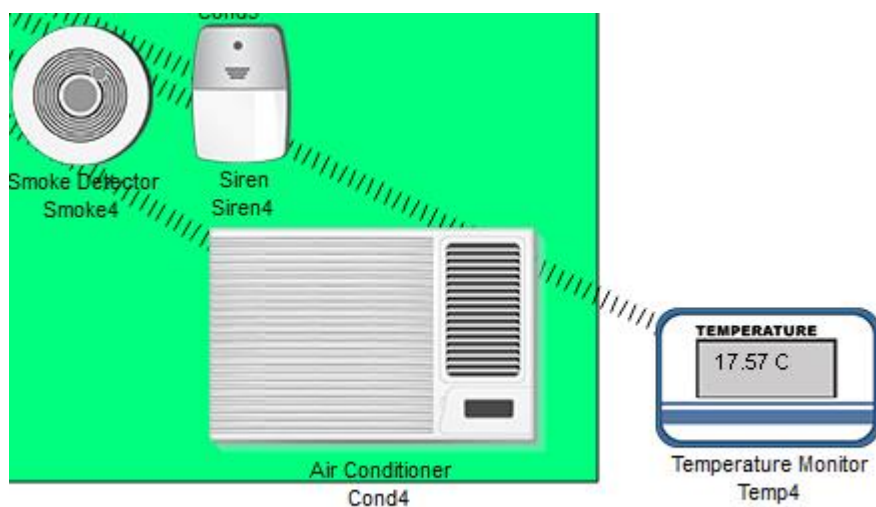


Рисунок 4.11 – Поведінка клімату при 17 градусах

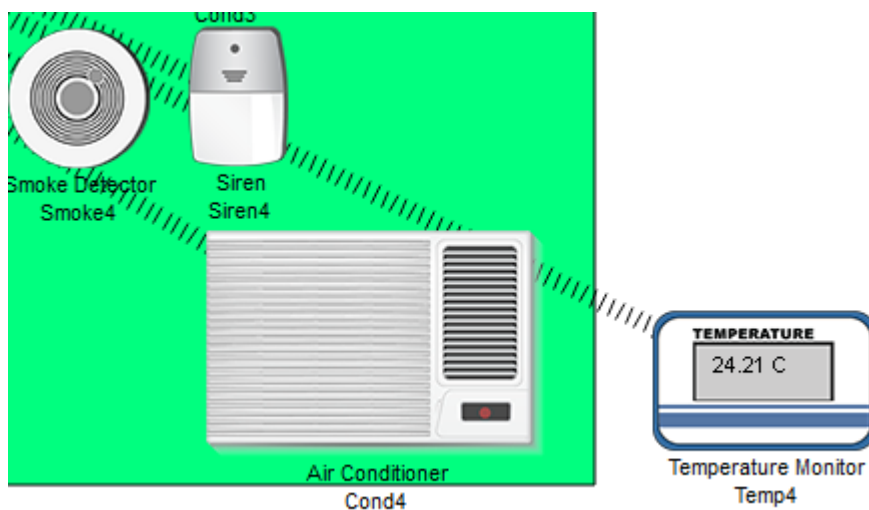


Рисунок 4.12 – При 24 градусах вмикається охолодження

## ВИСНОВКИ

У рамках виконання роботи побудована комп'ютерна система приватного підприємства «River Travels», яка зосереджена на конструкції, налаштуванні та безпеці корпоративної мережі, було досягнуто значних результатів. Протягом реалізації проекту вдалося впровадити стійку та ефективну мережеву інфраструктуру, яка забезпечує надійний обмін даними між структурними підрозділами підприємства і підтримує високий рівень безпеки інформації.

В процесі роботи було розроблено сценарії для ефективної роботи IoT модулів для покращення функціонування працівників в цій підмережі.

Було також реалізовано комплекс заходів щодо забезпечення кібербезпеки, включаючи шифрування даних, регулярне оновлення захисного програмного забезпечення та проведення тренінгів для персоналу з питань безпеки інформації. Ці заходи сприяли підвищенню загального рівня захисту корпоративної інформації.

Завдяки цілеспрямованій роботі та впровадженню сучасних технологій компанія «River Travels» отримала надійну та ефективну комп'ютерну систему, яка відповідає всім сучасним вимогам до корпоративних мереж. Це дозволяє підприємству підвищити рівень обслуговування клієнтів та оптимізувати внутрішні процеси, що, безумовно, сприяє його розвитку та зростанню на ринку.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Методичні рекомендації до виконання кваліфікаційної роботи бакалавра студентами галузі знань 12 Інформаційні технології спеціальності 123 Комп'ютерна інженерія / Л.І. Цвіркун, С.М. Ткаченко, Я.В. Панферова, Д.О. Бешта, Л.В. Бешта. – Д.: НТУ «ДП», 2023-2024. – 62 с. (дата звернення 15.05.2023р.)
2. Корпоративних мереж – Education [Електронний ресурс] – Режим доступу до ресурсу: <https://www.cisco.com/c/en/us/solutions/enterprise-networks/index.html> (дата звернення 20.05.2023р.)
3. Інтернет речей – Education [Електронний ресурс] – Режим доступу до ресурсу: <http://surl.li/dcsqu> (дата звернення 31.05.2023р.)
4. Технології IoT: засоби та методи управління мережами / В.М. Гончаренко, О.І. Мельник. – Київ: НТУУ "КПІ", 2023. – 96 с.
5. Практичні аспекти впровадження IoT в корпоративній сфері: виклики і рішення / А.С. Петров, Л.І. Сидоренко. – Харків: Видавництво ХНУ ім. В.Н. Каразіна, 2023. – 84 с.
6. Системи управління мережами у корпоративному середовищі: сучасні тенденції і перспективи розвитку / Є.О. Григорович, М.П. Литвинов. – Київ: Науковий світ, 2022. – 120 с.
7. IoT технології та їх застосування в управлінні корпоративними мережами / Європейський центр досліджень IoT. – Берлін: ECRIoT, 2023. – 70 с.

## Додаток А

### Текст налаштування пристроїв та загальна архітектура мережі

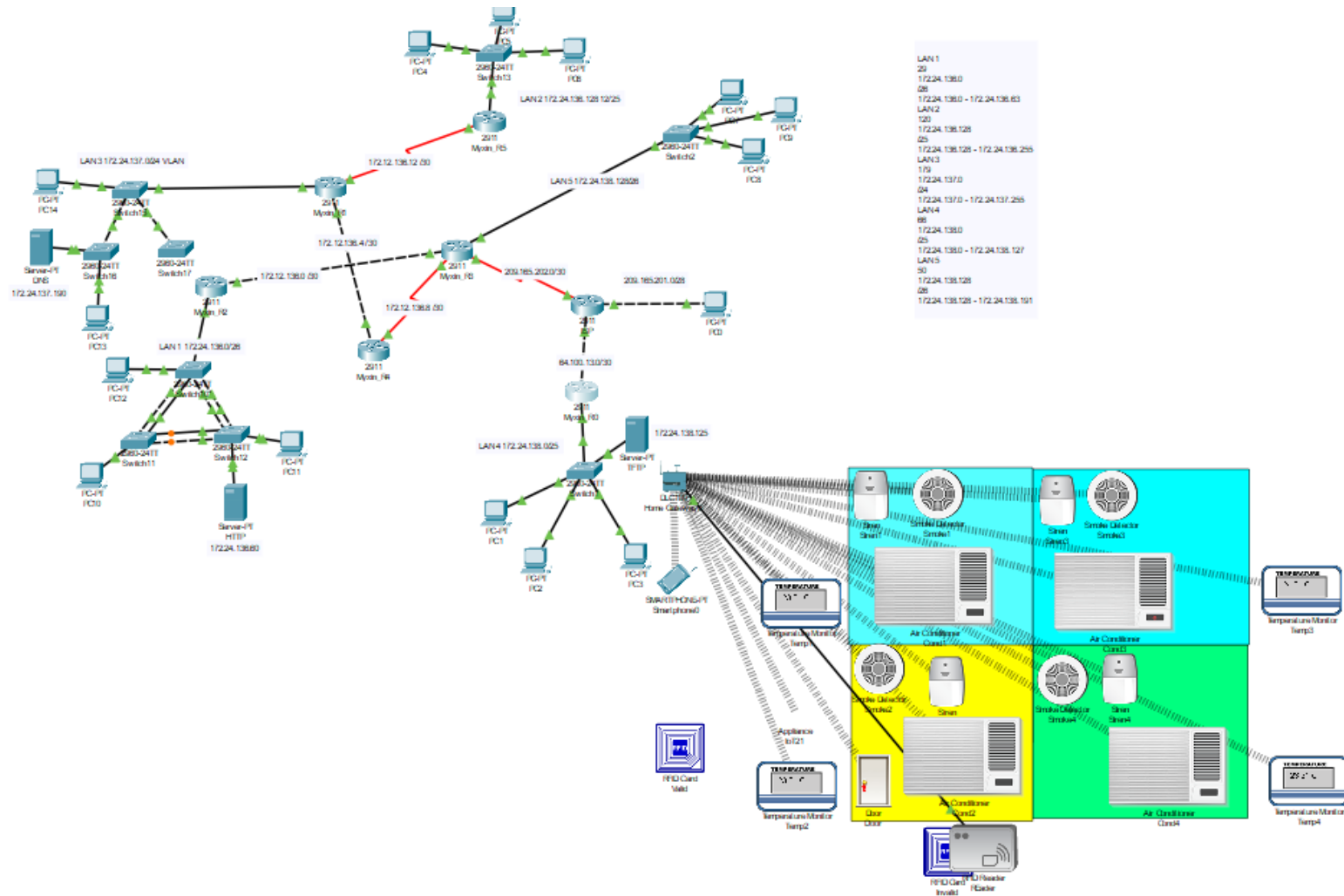


Рисунок ДА.1 – Загальна архітектура мережі

**Міністерство освіти і науки України и  
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ  
“ДНІПРОВСЬКА ПОЛІТЕХНІКА”**

**ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ  
НАЛАШТУВАННЯ МЕРЕЖІ КОМП'ЮТЕРНОЇ СИСТЕМИ**

Текст програми

804.02070743.24011-01 12 01

Листів 16

## АНОТАЦІЯ

Дана програма містить в собі команди для налаштування маршрутизаторів та комутаторів корпоративної мережі. Команди призначені для налаштування IP-адрес, базового налаштування пристроїв, налаштування DHCP, NAT, VPN, AAA, OSPF, VLAN, статичних маршрутів, EtherChannel та безпеки портів.

**3MICT**

1. Myxin_R1 .....	4
2. Myxin_R3 .....	8
3. Myxin_R0 .....	11
4. switch15 .....	14
5. switch10 .....	17

## 1. Myxin\_R1

Current configuration : 2675 bytes

```
!  
version 15.1  
no service timestamps log datetime msec  
no service timestamps debug datetime msec  
service password-encryption  
  
hostname Myxin_R1  
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1  
!  
ip dhcp excluded-address 172.24.137.1 172.24.137.5  
ip dhcp excluded-address 172.24.137.65 172.24.137.70  
ip dhcp excluded-address 172.24.137.129 172.24.137.133  
!  
ip dhcp pool LAN3-VLAN10  
network 172.24.137.0 255.255.255.192  
default-router 172.24.137.1  
dns-server 172.24.137.190  
ip dhcp pool LAN3-VLAN20  
network 172.24.137.64 255.255.255.192  
default-router 172.24.137.65  
dns-server 172.24.137.190  
ip dhcp pool LAN3-VLAN30  
network 172.24.137.128 255.255.255.192  
default-router 172.24.137.129  
dns-server 172.24.137.190  
!  
!  
!  
no ip cef  
no ipv6 cef  
username 12321ck1_Myxin password 7 082048430017061E010803  
license udi pid CISCO2911/K9 sn FTX15248B1Z-  
!  
ip domain-name Myxin_R1  
!  
!  
spanning-tree mode pvst  
!  
interface GigabitEthernet0/0  
ip address 172.12.136.6 255.255.255.252  
duplex auto  
speed auto  
!  
interface GigabitEthernet0/1  
no ip address
```



```
duplex auto
speed auto
!
interface GigabitEthernet0/1.10
encapsulation dot1Q 10
ip address 172.24.137.1 255.255.255.192
!
interface GigabitEthernet0/1.20
encapsulation dot1Q 20
ip address 172.24.137.65 255.255.255.192
!
interface GigabitEthernet0/1.30
encapsulation dot1Q 30
ip address 172.24.137.129 255.255.255.192
!
interface GigabitEthernet0/1.99
encapsulation dot1Q 99
ip address 172.24.137.193 255.255.255.240
!
interface GigabitEthernet0/2
no ip address
duplex auto
speed auto
!
interface Serial0/0/0
ip address 172.12.136.13 255.255.255.252
!
interface Serial0/0/1
no ip address
clock rate 2000000
!
interface Vlan1
no ip address
shutdown
!
router ospf 1
log-adjacency-changes
passive-interface default
no passive-interface GigabitEthernet0/0
no passive-interface GigabitEthernet0/1
no passive-interface Serial0/0/0
no passive-interface GigabitEthernet0/1.10
no passive-interface GigabitEthernet0/1.20
no passive-interface GigabitEthernet0/1.30
no passive-interface GigabitEthernet0/1.99
network 172.12.136.12 0.0.0.3 area 0
network 172.12.136.4 0.0.0.3 area 0
network 172.24.137.0 0.0.0.0 area 0
```

```
network 172.24.137.64 0.0.0.63 area 0
network 172.24.137.0 0.0.0.63 area 0
network 172.24.137.128 0.0.0.63 area 0
network 172.24.137.192 0.0.0.15 area 0
!
ip classless
!
ip flow-export version 9
banner motd ^CMyxin_R1^C
!
line con 0
password 7 0822455D0A16
login
!
line aux 0
!
line vty 0 4
password 7 0822455D0A16
login local
transport input ssh
line vty 5 15
password 7 0822455D0A16
login local
transport input ssh
end
```

## 2. Myxin\_R3

```
Current configuration : 2740 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Myxin_R3
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
ip dhcp excluded-address 172.24.138.129 172.24.138.134
ip dhcp excluded-address 172.24.138.190
ip dhcp excluded-address 172.24.138.191
!
ip dhcp pool LAN-5
network 172.24.138.128 255.255.255.192
default-router 172.24.138.129
dns-server 172.24.137.190
no ip cef
no ipv6 cef
```

```
username 12321ck1_Myxin password 7 082048430017061E010803
license udi pid CISCO2911/K9 sn FTX15245S80-
ip domain-name Myxin_R3
spanning-tree mode pvst
interface GigabitEthernet0/0
ip address 172.12.136.1 255.255.255.252
ip nat inside
duplex auto
speed auto
!
interface GigabitEthernet0/1
ip address 172.24.138.129 255.255.255.192
ip nat inside
duplex auto
speed auto
!
interface GigabitEthernet0/2
no ip address
duplex auto
speed auto
!
interface Serial0/0/0
ip address 209.165.202.1 255.255.255.252
ip nat outside
!
interface Serial0/0/1
ip address 172.12.136.9 255.255.255.252
ip nat inside
!
interface Vlan1
no ip address
shutdown
!
router ospf 1
log-adjacency-changes
redistribute static subnets
passive-interface default
no passive-interface GigabitEthernet0/0
no passive-interface GigabitEthernet0/1
no passive-interface Serial0/0/0
no passive-interface Serial0/0/1
network 172.24.138.128 0.0.0.63 area 0
network 209.165.202.0 0.0.0.3 area 0
network 172.12.136.8 0.0.0.3 area 0
network 172.12.136.0 0.0.0.3 area 0
!
ip nat pool Internet 209.165.200.6 209.165.200.30 netmask 255.255.255.224
ip nat inside source list NAT12 pool Internet
```

```

ip nat inside source static 172.24.138.125 209.165.200.3
ip nat inside source static 172.24.136.60 209.165.200.3
ip nat inside source static 172.24.137.190 209.165.200.3
ip classless
ip route 0.0.0.0 0.0.0.0 209.165.202.2
!
ip flow-export version 9
!
!
ip access-list extended NAT12
deny ip 172.24.136.0 0.0.0.63 172.24.138.0 0.0.0.127
deny ip 172.24.136.128 0.0.0.127 172.24.138.0 0.0.0.127
deny ip 172.24.137.0 0.0.0.255 172.24.138.0 0.0.0.127
deny ip 172.24.138.128 0.0.0.63 172.24.138.0 0.0.0.127
deny ip 172.12.136.0 0.0.0.255 172.24.138.0 0.0.0.127
permit ip 172.24.136.0 0.0.0.63 any
permit ip 172.24.136.128 0.0.0.127 any
permit ip 172.24.137.0 0.0.0.255 any
permit ip 172.24.138.128 0.0.0.63 any
permit ip 172.24.0.0 0.0.255.255 any
permit ip 172.12.136.0 0.0.0.255 any
banner motd ^CMyxin_R3^C
line con 0
password 7 0822455D0A16
login
!
line aux 0
!
line vty 0 4
password 7 0822455D0A16
login local
transport input ssh
line vty 5 15
password 7 0822455D0A16
login local
transport input ssh
end

```

### 3. Myxin\_R0

Building configuration...

Current configuration : 1489 bytes

!

version 15.1

no service timestamps log datetime msec

no service timestamps debug datetime msec

```
service password-encryption
!
hostname Myxin_R0
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
ip dhcp excluded-address 172.24.138.1 172.24.138.5
ip dhcp excluded-address 172.24.138.127
ip dhcp excluded-address 172.24.138.126
!
ip dhcp pool LAN-4
network 172.24.138.0 255.255.255.128
default-router 172.24.138.1
dns-server 172.24.137.190
ip cef
no ipv6 cef
username 12321ck1_Myxin password 7 082048430017061E010803
license udi pid CISCO2911/K9 sn FTX1524AJ8Z-
ip domain-name Myxin_R0
spanning-tree mode pvst
interface GigabitEthernet0/0
ip address 64.100.13.2 255.255.255.252
duplex auto
speed auto
!
interface GigabitEthernet0/1
ip address 172.24.138.1 255.255.255.128
duplex auto
speed auto
!
interface GigabitEthernet0/2
no ip address
duplex auto
speed auto
!
interface Vlan1
no ip address
shutdown
!
router ospf 1
log-adjacency-changes
passive-interface default
no passive-interface GigabitEthernet0/0
no passive-interface GigabitEthernet0/1
network 64.100.13.0 0.0.0.3 area 0
network 172.24.138.0 0.0.0.127 area 0
ip classless
ip flow-export version 9
banner motd ^CMyxin_R0^C
line con 0
```

```
password 7 0822455D0A16
login
!
line aux 0
!
line vty 0 4
password 7 0822455D0A16
login local
transport input ssh
line vty 5 15
password 7 0822455D0A16
login local
transport input ssh

end
```

#### **4.switch15**

```
Current configuration : 1828 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
switchport mode trunk
!
interface FastEthernet0/2
switchport mode trunk
!
interface FastEthernet0/3
switchport mode trunk
!
interface FastEthernet0/4
switchport mode trunk
!
interface FastEthernet0/5
switchport mode trunk
!
interface FastEthernet0/6
switchport access vlan 10
```

```
switchport mode access
!  
interface FastEthernet0/7  
switchport access vlan 10  
switchport mode access  
!  
interface FastEthernet0/8  
switchport access vlan 10  
switchport mode access  
!  
interface FastEthernet0/9  
switchport access vlan 10  
switchport mode access  
!  
interface FastEthernet0/10  
switchport access vlan 10  
switchport mode access  
!  
interface FastEthernet0/11  
switchport access vlan 20  
!  
interface FastEthernet0/12  
switchport access vlan 20  
!  
interface FastEthernet0/13  
switchport access vlan 20  
!  
interface FastEthernet0/14  
switchport access vlan 20  
!  
interface FastEthernet0/15  
switchport access vlan 20  
!  
interface FastEthernet0/16  
switchport access vlan 20  
!  
interface FastEthernet0/17  
switchport access vlan 30  
!  
interface FastEthernet0/18  
switchport access vlan 30  
!  
interface FastEthernet0/19  
switchport access vlan 30  
!  
interface FastEthernet0/20  
switchport access vlan 30  
!
```

```
interface FastEthernet0/21
switchport access vlan 30
!
interface FastEthernet0/22
switchport access vlan 30
!
interface FastEthernet0/23
switchport access vlan 30
!
interface FastEthernet0/24
switchport access vlan 30
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
shutdown
line con 0
!
line vty 0 4
login
line vty 5 15
login
```

## 5.switch10

```
Current configuration : 1420 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
spanning-tree mode pvst
spanning-tree extend system-id
!
interface Port-channel1
description Link to Other Switch
switchport mode trunk
!
interface Port-channel2
switchport mode trunk
!
interface FastEthernet0/1
```



```
switchport mode trunk
channel-group 1 mode active
!
interface FastEthernet0/2
switchport mode trunk
channel-group 1 mode active
!
interface FastEthernet0/3
switchport mode trunk
channel-group 2 mode active
!
interface FastEthernet0/4
switchport mode trunk
channel-group 2 mode active
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
```

```
!  
interface FastEthernet0/22  
!  
interface FastEthernet0/23  
!  
interface FastEthernet0/24  
!  
interface GigabitEthernet0/1  
!  
interface GigabitEthernet0/2  
!  
interface Vlan1  
no ip address  
shutdown  
!  
line con 0  
!  
line vty 0 4  
login  
line vty 5 15  
login  
end
```