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 **Машкова М.А**
(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 для ТОВ "Sentosa" 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. .Шедловський І.А			
спеціальної частини	доц. Шедловський І.А			
розділів:				
розробка апаратної частини	доц. Бешта Д.О			
розробка корпоративної мережі	ас. Панферова Я.В			

Рецензент				

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 Машкова М.А **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 для ТОВ "Sentosa" з детальним опрацюванням побудови та безпеки корпоративної мережі»

затверджену наказом ректора НТУ «Дніпровська політехніка» від 29.04.2024 № 375-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 ТОВ «Sentosa»	10.05.2024
Розробка апаратної частини	Розробити вимоги до функцій, виконуваними системою та провести розробку та аналіз загальної архітектури мережі, з подальшим створенням структурної схеми мережі підприємства.	17.05.2024
Розробка корпоративної мереж	Побудувати в Packet Tracer модель корпоративної мережі компанії, виконати налаштування та перевірку роботи системи	24.05.2024
Розробка компонента системи	Розробити спеціальної частини корпоративної мережі з використанням технології інтернету речей з подальшим аналізом та перевіркою системи	31.05.2024

Завдання видано _____ доц. Шедловський І.А
(підпис керівника) (прізвище, ініціали)

Дата видачі 10.03.24

Дата подання до екзаменаційної комісії 08.06.24

Прийнято до виконання _____ Машков М.А
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 76 с., 26 рис., 5 табл., 1 додаток, 7 джерела. КЛЮЧОВІ СЛОВА: корпоративні мережі, безпека , масштабованість, мережева архітектура, мережеві протоколи, хмарні обчислення.

Об’єкт розробки – комп'ютерна система для ТОВ «Sentosa». Мета роботи – розробка надійної та ефективної мережевої інфраструктури, яка забезпечує високий рівень безпеки та оптимальну продуктивність для корпоративних потреб.

Здійснено розробку інтегрованої мережевої системи, включаючи детальний аналіз вимог, проектування архітектури, впровадження та тестування.

Дослідження базувалися на сучасних методах системного аналізу, використанні програмного забезпечення для моделювання мережевих процесів та апаратури для моніторингу мережі. Отримані результати свідчать про високий рівень відповідності запропонованих рішень сучасним технічним вимогам та можливостям їхнього застосування для оптимізації корпоративних процесів.

Розроблена система володіє такими техніко-експлуатаційними характеристиками, як висока надійність, масштабованість та безпека. Впровадження системи дозволило забезпечити стабільне та ефективне функціонування корпоративної мережі, значно знизити ризики пов'язані з даними.

Рекомендації щодо використання результатів включають розширення мережевої інфраструктури з використанням модульного підходу та введення додаткових заходів безпеки, включаючи застосування сучасних криптографічних методів.

Результати роботи можуть бути використані в інших компаніях, які зацікавлені в підвищенні ефективності та безпеки своїх мережевих систем, а також для подальших наукових досліджень у цій галузі.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

LAN	–	Локальна мережа
WAN	–	Глобальна мережа
VLAN	–	Віртуальна локальна обчислювальна мережа (Virtual LAN)
NAT	–	Мережева адресна трансляція (Network Address Translation)
ACL	–	Список контролю доступу (Access Control List)
SSID	–	Ідентифікатор набору служб бездротового зв'язку (Service Set Identifier)
WPA2-PSK	–	Wi-Fi Protected Access 2 - Pre-Shared Key
IoT	–	Інтернет речей (Internet of Things)

ВСТУП

У контексті швидкоплинного розвитку інформаційних технологій, роль ефективної та надійної комп'ютерної системи стає дедалі важливішою для успішної діяльності будь-якої організації. В цьому аспекті, задача створення та оптимізації корпоративної мережі для ТОВ «Sentosa», компанії, що спеціалізується на наданні послуг у галузі туризму та подорожей, виринає як ключова. Цей процес передбачає глибокий аналіз потреб бізнесу, вибір оптимальної архітектури мережі, а також імплементацію передових технологій для забезпечення її ефективності, безпеки та стабільності.

З огляду на стрімке зростання обсягів даних та необхідність високошвидкісного обміну інформацією всередині компанії, налаштування корпоративної мережі стає непростим завданням, яке вимагає індивідуального підходу. ТОВ «Sentosa» прагне до оптимізації своїх бізнес-процесів через розгортання сучасної комп'ютерної інфраструктури, що включає реалізацію високопродуктивних серверів, надійних засобів зберігання даних, а також ефективних комунікаційних мереж.

Ключовим елементом цієї інфраструктури є корпоративна мережа, яка забезпечує взаємодію між різними підрозділами компанії та інтеграцію всіх необхідних IT-сервісів. Розробка адекватної мережевої структури передбачає вибір такої топології, яка зможе задовольнити поточні потреби організації та бути готовою до масштабування відповідно до майбутнього росту. В цьому контексті, велика увага приділяється вибору мережевого обладнання, здатного забезпечити необхідну пропускну здатність, надійність та захист від можливих загроз.

Особливу увагу під час проектування мережевої інфраструктури ТОВ «Sentosa» слід приділити аспектам безпеки. Враховуючи високу чутливість інформації, якою оперує компанія, застосування комплексних мережевих безпекових рішень, включаючи фаєрволи, системи виявлення та запобігання вторгненням, а також використання віртуальних приватних мереж (VPN) для захищеного з'єднання між офісами, стає критично важливим. Ефективне управління доступом та авторизацією користувачів, регулярне оновлення програмного забезпечення та впровадження

політик інформаційної безпеки забезпечують високий рівень захисту корпоративних даних.

В результаті, комплексний підхід до побудови та налаштування корпоративної мережі для ТОВ «Sentosa», що включає детальне планування, застосування сучасних технологій та строге дотримання мережевих безпекових протоколів, стане основою для створення ефективної, безпечної та масштабованої ІТ-інфраструктури, спроможної підтримати динамічний розвиток компанії в сучасному цифровому світі.

1 СТАН ПИТАННЯ І ПОСТАНОВКА ЗАВДАННЯ

1.1 Стисла характеристика галузі та умов застосування системи

Обрана галузь застосування для проектованої комп'ютерної системи охоплює індустрію туризму. Цей сегмент економіки агрегує широкий спектр послуг, орієнтованих на задоволення потреб мандрівників, включно з туристичними агенціями, операторами пакетних турів, гостинними закладами, авіалініями, закладами харчування та іншими. Динамічний розвиток цієї галузі спонукається неперервним підвищенням інтересу до подорожей і рекреації, підкреслюючи її значний потенціал для зростання[1].

Комп'ютерна система, призначена для розробки в інтересах ТОВ «Sentosa», має бути зорієнтована на оптимізацію процесів управління резервацією турів, обробку клієнтських даних, ведення фінансового обліку та виконання маркетингових стратегій. Особлива увага буде приділена інтеграції функціональності онлайн-бронювання, ефективної комунікації з клієнтами через цифрові канали, включаючи офіційний веб-сайт та соціальні мережі, а також розробці інструментів аналізу даних для глибшого розуміння та управління бізнес-процесами. Важливим аспектом системи є її здатність забезпечити високий рівень безпеки, надійність роботи та можливість масштабування для відповідності майбутнім потребам та викликам, з якими може зіткнутися компанія.

1.2 Характеристика підприємства та умов застосування КС

Об’єкт впровадження – ТОВ «Sentosa»

ТОВ «Sentosa» ключовий гравець у сфері туристичних послуг та гостинності, відомий своєю відданістю забезпеченню висококласного сервісу, інноваційними методами управління та увагою до кожної потреби клієнтів. Компанія "Sentosa" має за мету не лише задовольнити очікування своїх гостей, а й перевершити їх, створюючи неперевершені умови для відпочинку.

Заснована з ідеєю надання бездоганного сервісу, «Sentosa» пропагує філософію, що в кожному аспекті їх діяльності - від вибору місць для відпочинку до деталей

обслуговування - має бути втілена ця місія. Такий підхід втілюється завдяки керівництву компанії, де кожен член команди є висококваліфікованим професіоналом, зосередженим на підвищенні якості послуг та розширенні бізнес-горизонтів «Sentosa».

Керівництво «Sentosa» ставить перед собою стратегічні завдання, які відображають прагнення до лідерства та утримання конкурентних переваг у туристичній індустрії. Організаційна структура компанії розроблена таким чином, щоб забезпечити ефективну взаємодію між відділами - від маркетингу та продажів до фінансів та управління персоналом - кожен з яких відіграє ключову роль у досягненні загальних бізнес-цілей.

Високий пріоритет «Sentosa» віддає інтеграції передових технологій у всі процеси компанії. Використання сучасних комп'ютерних систем та інноваційних рішень спрямоване на підвищення рівня задоволення клієнтів, оптимізацію внутрішніх процесів та забезпечення надійного управління. Цей стратегічний підхід дозволяє «Sentosa» займати лідируючі позиції на ринку, пропонуючи своїм клієнтам виняткові відпочинкові переживання[1].

1.3 Принципи, технічні способи та математичні методи інформаційного забезпечення підприємства

Інформаційне забезпечення для туристичного агентства ТОВ «Sentosa» є критично важливим аспектом їхньої діяльності, оскільки воно визначає не лише ефективність внутрішніх процесів, але й якість обслуговування та задоволеність клієнтів. Ось принципи та технічні способи інформаційного забезпечення для ТОВ «Sentosa»:

Централізована система управління: Розробка та впровадження централізованої системи управління, яка об'єднує всі аспекти діяльності компанії, включаючи бронювання, облік клієнтів, фінансовий облік та інші. Це дозволить забезпечити цілісність та зручний доступ до всієї інформації для співробітників.

Система управління відносинами з клієнтами (CRM): Впровадження CRM-системи для збору, зберігання та аналізу даних про клієнтів, що дозволить ефективно

взаємодіяти з ними та розробляти персоналізовані пропозиції, враховуючи їхні попередні вподобання та історію замовлень.

Аналітичні системи: Використання аналітичних систем для аналізу даних про клієнтів, ринкових тенденцій та ефективності маркетингових кампаній з метою прийняття обґрунтованих управлінських рішень та вдосконалення стратегій розвитку.

Захист даних та кібербезпека: Забезпечення високого рівня захисту даних та кібербезпеки для запобігання несанкціонованому доступу до конфіденційної інформації про клієнтів та внутрішніх даних компанії.

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

ТОВ "Sentosa", як активний учасник туристичної індустрії, прагне інтегрувати передові IT-рішення для оптимізації своїх внутрішніх процесів. Аналіз існуючих методик і технологій обробки та передачі інформації дозволяє виявити найефективніші підходи для впровадження у структуру компанії.

Обробка інформації: Сучасні підходи до обробки даних включають використання розподілених обчислень, хмарних технологій та великих даних. Зокрема, хмарні рішення забезпечують гнучкість та масштабованість IT-інфраструктури, дозволяючи компаніям адаптуватися до змінних обсягів даних.

Передача інформації: Захищені канали зв'язку, такі як VPN, SSL/TLS шифрування, забезпечують безпечну передачу інформації між відділами компанії та її партнерами. Крім того, застосування протоколів електронного цифрового підпису та блокчейн технологій може забезпечити додатковий рівень безпеки та невід'ємність інформації.

Принципи побудови системи: Створення міцної інформаційної системи починається з ретельного планування архітектури системи, яка повинна включати ефективну інтеграцію внутрішніх та зовнішніх ресурсів, забезпечення високого рівня безпеки та надійності. Модульність та гнучкість системи дозволяють легко масштабувати її функціональність відповідно до потреб бізнесу.

Відомі рішення у галузі: Досвід інших компаній у туристичній індустрії показує значний успіх в інтеграції CRM-систем для управління взаєминами з клієнтами, систем управління ресурсами підприємства (ERP) для оптимізації внутрішніх процесів, а також інтелектуальних аналітичних систем для прогнозування попиту та оптимізації послуг.

З огляду на вищевикладене, ТОВ "Sentosa" має можливість вибрати найефективніші технологічні рішення та методики для підвищення ефективності своєї діяльності, забезпечуючи при цьому високий рівень безпеки обробки та передачі інформації[1].

1.5 Розробка схеми організаційної структури підприємства

ТОВ «Sentosa» поділяється на такі відділи:

Відділ продажів та маркетингу: Цей відділ відповідає за просування продуктів та послуг компанії, залучення нових клієнтів та підтримку вже існуючих відносин.

Відділ обслуговування клієнтів: Відділ, який забезпечує підтримку клієнтів, відповідає на їх запитання, розв'язує проблеми та забезпечує задоволеність клієнтів від обслуговування.

Фінансовий відділ: Відділ, що відповідає за фінансове планування, облік та аналіз фінансової діяльності компанії.

Операційний відділ: Відділ, який відповідає за повсякденну діяльність компанії, зокрема за виробництво, постачання та послуги.

Відділ розвитку та інновацій: Відділ, що займається стратегічним плануванням, пошуком нових можливостей для розвитку бізнесу та впровадженням інноваційних рішень.

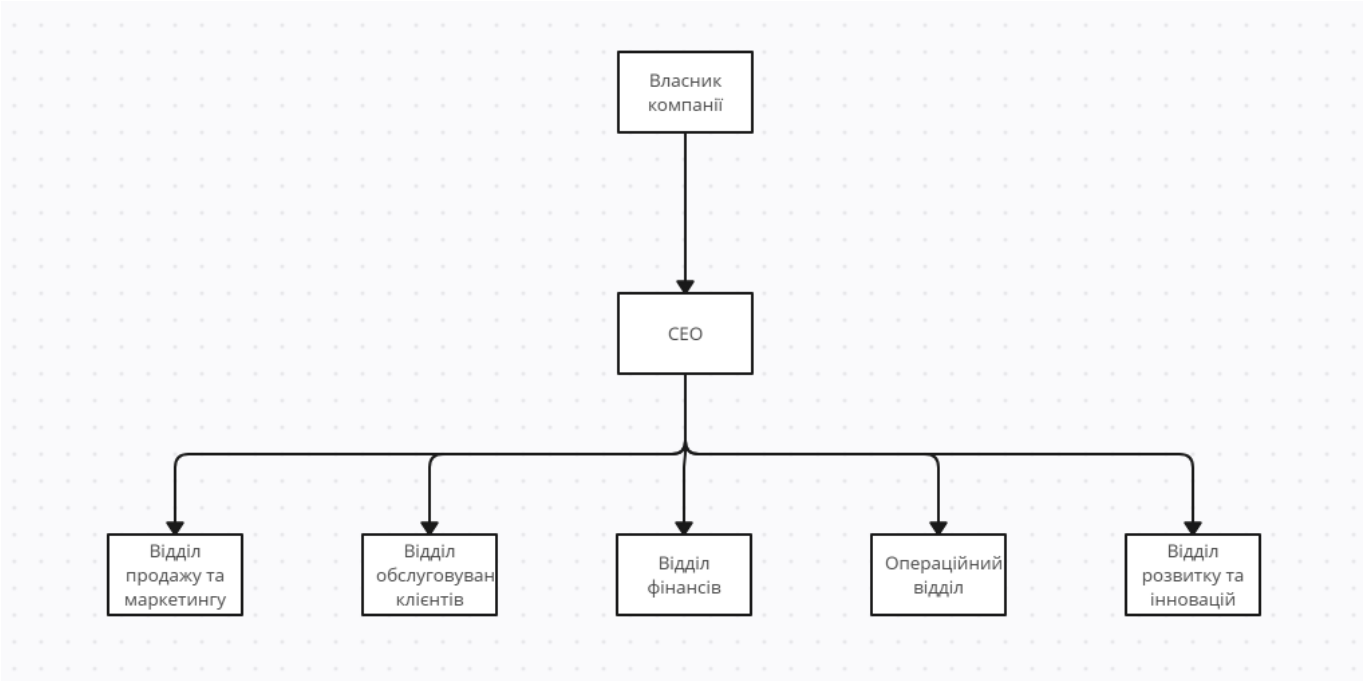

Рисунок 1.1 – Схема організаційної структури ТОВ «Sentosa»

Структурна схема розміщення підрозділів у будівлі в якій знаходиться: Відділ продажів та маркетингу, відділ обслуговування клієнтів, фінансовий відділ, операційний відділ та відділ розвитку та інновацій (рис. 1.2) [3].

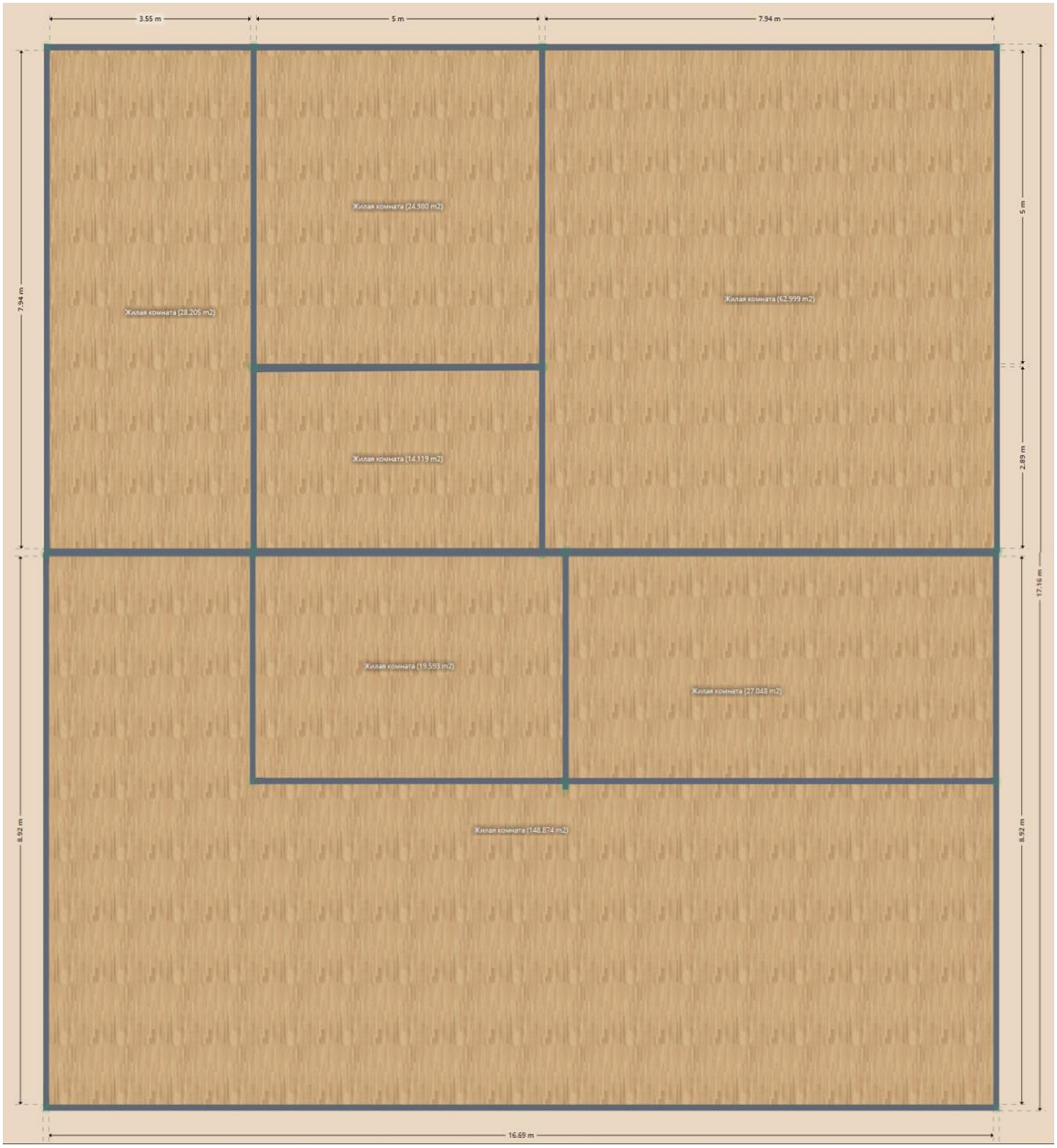

Рисунок 1.2 – Структурна схема розміщення підрозділів у будівлі

1.6 Завдання і мета роботи

Метою роботи є розробка комп'ютерної системи для ТОВ «Sentosa» з детальним опрацюванням побудови та налаштування корпоративної мережі, що охоплює глибоке дослідження, планування та впровадження корпоративної мережі. Це включає розробку здатної адаптуватися, високоефективної мережевої інфраструктури, заснованої на передових технологічних рішеннях, для забезпечення надійності, безпеки та високої доступності туристичних сервісів. Виконання цього комплексного завдання вимагає реалізації наступних етапів:

Глибокий аналіз існуючої інформаційної системи та потреб ТОВ «Sentosa» у автоматизації. Це передбачає детальний огляд нинішніх технологічних процесів, оцінку поточної продуктивності мережі та ідентифікацію ключових вимог до нової системи;

Визначення оптимальної мережевої архітектури та відбір обладнання. На цьому етапі важливо обґрунтувати вибір мережевих рішень, що підтримують високий рівень доступності, гарантують безпеку даних та можливість масштабування системи відповідно до зростаючих потреб бізнесу;

Розробка специфікацій для апаратного забезпечення. Уточнення технічних параметрів необхідного обладнання для створення ефективної мережевої інфраструктури;

Аналіз мережевого трафіку. Цей крок передбачає дослідження та оцінку обсягів даних, які циркулюють у мережі, для забезпечення її оптимальної продуктивності та ефективності;

Тестування функціональності мережі. Включає комплексне випробування мережевої системи та її компонентів для забезпечення високого рівня працездатності, надійності та сумісності різних елементів інфраструктури.

Очікуваним результатом роботи є створення надійної та безпечної корпоративної мережі, що забезпечить безперебійний обмін даними між всіма підрозділами ТОВ «Sentosa» та їх клієнтами. Така система має стати основою для ефективної взаємодії всередині компанії, покращення якості обслуговування клієнтів та підвищення загальної продуктивності діяльності ТОВ «Sentosa» у сфері туристичних послуг[2].

1.7 Визначення можливих напрямків рішення поставлених завдань

Серед можливих напрямків можуть бути:

– Інтеграція хмарних технологій для забезпечення гнучкості та масштабованості.

– Впровадження рішень для віртуалізації мережі (наприклад, SDN та NFV), що дозволить легше управляти ресурсами мережі та її конфігурацією.

– Застосування передових систем безпеки, включаючи шифрування даних, брандмауери нового покоління та інтрузивні системи виявлення і запобігання.

– Розгортання високопродуктивної та надійної апаратної інфраструктури, здатної підтримувати великі обсяги даних та високу швидкість передачі даних.

1.8 Обґрунтування вибраного напрямку інженерного рішення

– Використання обладнання та рішень Cisco

Cisco є світовим лідером у галузі мережевих технологій, що забезпечує високу якість та надійність обладнання. Використання рішень Cisco для корпоративної мережі ТОВ «Sentosa» дає наступні переваги:

Надійність та стабільність: Обладнання Cisco відоме своєю надійністю та здатністю працювати в критичних умовах, забезпечуючи безперебійну роботу мережі.

Інтегровані безпекові функції: Cisco пропонує розширені можливості забезпечення безпеки, включаючи вогнестінки, інтрузивні системи виявлення та запобігання, що критично важливо для захисту даних клієнтів.

– Розгортання VPN

Використання віртуальних приватних мереж (VPN) дозволить забезпечити безпечне підключення між різними локаціями ТОВ «Sentosa» та дистанційними користувачами, зокрема:

Захист даних: Всі дані, які передаються через VPN, шифруються, що мінімізує ризик їх перехоплення.

Гнучкість доступу: Співробітники можуть безпечно доступатися до корпоративних ресурсів з будь-якої точки світу.

– Налаштування DNS і TFTP

DNS (Domain Name System): Ефективне налаштування DNS сприятиме швидкому розв'язанню імен у IP-адреси, поліпшуючи час відгуку системи і загальну продуктивність мережі.

TFTP (Trivial File Transfer Protocol): Використання TFTP дозволить безпечно та ефективно розгортати конфігурації та оновлення програмного забезпечення на мережеві пристрої.

– Захист AAA (Authentication, Authorization, and Accounting)

Аутентифікація: Забезпечує перевірку ідентичності користувачів, перш ніж надавати доступ до мережі.

Авторизація: Визначає рівень доступу користувачів до ресурсів після їх успішної аутентифікації.

Ці рішення сприятимуть створенню ефективної, безпечної та надійної мережевої інфраструктури, здатної підтримувати вимоги ТОВ «Sentosa» до високої доступності та безпеки туристичних сервісів. Вибір цих технологій та методик відповідає найкращим галузевим практикам і забезпечує компанії перевагу у використанні новітніх технологічних рішень для досягнення бізнес-цілей.

2 РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ КОМП'ЮТЕРНОЇ АБО КІБЕРФІЗИЧНОЇ СИСТЕМИ

2.1 Технічні вимоги до комп'ютерної системи ….

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

Проектування комп'ютерної системи для ТОВ "Sentosa" спрямоване на створення ефективного механізму обміну інформацією між відділами компанії, а також на забезпечення надійного зберігання даних на FTP-сервері. Для забезпечення постійного доступу співробітників до корпоративних ресурсів, система має бути розроблена таким чином, щоб забезпечити її доступність протягом усіх робочих годин.

1. Мережа поділяється на 5-ть локальних мереж щоб задовольнити потреби переваг, а саме:

2. Продуктивність – швидкість передачі даних по локальним мережам набагато більша адже шлях пролягає не через усю мережу;

3. Масштабованість – легка заміна та додавання пристроїв локальної мережі;

4. Безпека – переважна реалізація більш точної системи безпеки такі як брандмауери або VPN та інше.

Необхідно здійснити поділ IP-адреси 172.24.128.0/21 на п'ять підмереж з урахуванням вимог до кількості вузлів в кожній з них:

– LAN1 має включати 18 вузлів;

– LAN2 розрахована на 67 вузлів;

– LAN3 повинна обслуговувати 121 вузол;

– LAN4 задіятиме 107 вузлів;

– LAN5 розрахована на 71 вузол.

Додатково, важливим аспектом є впровадження заходів забезпечення безпеки мережі, включаючи використання шифрування даних, фільтрацію трафіку та

застосування політик безпеки для захисту від несанкціонованого доступу та інших кіберзагроз. Також система має передбачати механізми резервного копіювання та відновлення даних для забезпечення надійності зберігання інформації та її доступності в критичних ситуаціях[2].

2.1.1.1.2 Вимоги до способів і засобів зв’язку між компонентами комп’ютерної системи

Пропускна здатність та швидкість передачі даних: Мережеві компоненти повинні підтримувати достатню пропускну здатність для обробки очікуваного обсягу даних без затримок, забезпечуючи ефективне обслуговування запитів користувачів та системних процесів.

Надійність зв’язку: Засоби зв'язку між компонентами повинні забезпечувати високий рівень надійності, мінімізуючи ризик відмов у критичні моменти.

Масштабованість: Система має бути готова до збільшення обсягу даних та кількості користувачів, з можливістю легкої додавання нових компонентів без зниження загальної продуктивності.

Безпека: Комунікаційні канали та протоколи повинні використовувати сучасні методи шифрування та аутентифікації для захисту даних від несанкціонованого доступу.

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

Сумісність інтерфейсів: Всі системи мають використовувати сумісні або стандартизовані інтерфейси для забезпечення безперешкодної інтеграції.

Обмін даними: Системи мають забезпечувати обмін даними у реальному часі або відповідно до заданих інтервалів, залежно від бізнес-вимог.

Єдність протоколів: Використання єдиних протоколів комунікацій дозволяє уникнути проблем зі сумісністю та підвищує ефективність системних інтеграцій.

Контроль доступу: Належні механізми управління доступом і правилами, що дозволяють регулювати, хто та як може взаємодіяти з системою, забезпечуючи безпеку та контроль.

Ці вимоги забезпечать, що мережа ТОВ «Sentosa» буде здатна ефективно інтегруватися з існуючими та майбутніми системами, що підтримає сталість бізнес-процесів та забезпечить високий рівень сервісу.

2.1.1.1.4 Вимоги до режимів функціонування системи

– Режим нормальної роботи: Система повинна функціонувати в нормальному режимі протягом робочих годин без перерв та забезпечувати доступність всіх необхідних функцій для користувачів.

– Режим безперервної підтримки та оновлення: Система повинна мати підтримку з боку IT-спеціалістів для оперативного вирішення проблем та оновлення програмного забезпечення з метою забезпечення безперебійної роботи та захисту від потенційних загроз.

2.1.1.1.5 Вимоги до діагностування системи

Інтегровані засоби моніторингу: Система має включати вбудовані інструменти для моніторингу стану апаратного та програмного забезпечення.

Протоколювання подій: Автоматичне протоколювання всіх системних подій та зберігання логів для аналізу та відстеження змін і помилок.

Інтерфейси для дистанційного доступу: Можливість дистанційного доступу до системи для виконання діагностичних процедур і виправлення помилок.

Система оповіщення: Автоматичне оповіщення технічної служби про критичні помилки або збої у системі.

2.1.1.1.6 Перспективи розвитку, модернізації системи

Масштабованість: Конструкція системи повинна дозволяти легко додавати нові компоненти та збільшувати її продуктивність без потреби в повному перепроектуванні.

Технологічні оновлення: Система має підтримувати інтеграцію з новітніми технологіями та стандартами, щоб залишатися актуальною на ринку.

Заміна застарілих компонентів: Програма заміни обладнання та програмного забезпечення, що вийшли з ужитку.

2.1.1.2 Вимоги до показників призначення

Продуктивність: Параметри, які визначають, наскільки ефективно система обробляє запити та виконує свої функції.

Надійність: Вимірювання частоти виникнення помилок та часу між відмовами.

Скальпованість: Здатність системи адаптуватися до збільшення обсягу даних або кількості користувачів.

2.1.1.3 Вимоги до патентної чистоти

Обладнання та програмне забезпечення, яке використовується в комп'ютерній системі, повинно дотримуватися патентних вимог.

Для цього необхідно використовувати ліцензійне програмне забезпечення.

2.1.1.4 Додаткові вимоги

Умови експлуатації: Забезпечення стабільної роботи системи у відповідності до кліматичних умов регіону.

Обладнання: Визначення технічних характеристик активного обладнання, таких як потужність, кількість портів, опції монтажу.

Кабель-канали та розетки: Специфікації для типів і розміщення кабель-каналів та розеток.

Комунікаційне обладнання: Вимоги до розташування і типів шаф, кабельних трас.

Резервування: Розробка системи з високим рівнем резервування для забезпечення безперервності бізнес-процесів.

2.1.2 Вимоги функцій, виконуваним системою

Перелік функцій: Визначення ключових задач, які система повинна виконувати, включаючи обробку даних, забезпечення безпеки, взаємодію з іншими системами.

Часовий регламент: Встановлення максимально допустимих часів на виконання кожної функції.

Якість та точність: Вимоги до якості обробки даних і точності інформації, яку система генерує.

2.1.3 Вимоги до видів забезпечення комп'ютерної системи

2.1.3.1 Вимоги до математичного забезпечення

– Склад математичних методів і моделей:

Статистичний аналіз: Використання методів статистичного аналізу для обробки даних та прогнозування.

Оптимізація: Застосування алгоритмів лінійної та нелінійної оптимізації для підвищення ефективності ресурсного планування.

Штучний інтелект та машинне навчання: Розробка та впровадження моделей машинного навчання для автоматизації процесів та покращення прийняття рішень.

– Область застосування та обмеження:

Прогнозування попиту: Використання прогностичних моделей для точного визначення майбутнього попиту на туристичні послуги.

Розподіл ресурсів: Моделі оптимізації для раціонального розподілу ресурсів між різними відділами та сервісами.

Аналіз задоволеності клієнтів: Використання аналітичних інструментів для аналізу відгуків клієнтів та покращення якості обслуговування.

– Способи використання:

Інтеграція з IT-системами: Математичні моделі та алгоритми мають бути інтегровані з існуючими IT-системами для забезпечення їх ефективної роботи.

Користувацькі інтерфейси: Розробка зрозумілих та легких у використанні користувацьких інтерфейсів для візуалізації результатів математичних розрахунків.

Динамічне оновлення: Моделі та алгоритми мають підтримувати можливість легкого оновлення у відповідь на зміни у даних або в операційному середовищі.

– Алгоритми, що підлягають розробці:

Покращення алгоритмів прогнозування: Розробка новітніх методів для підвищення точності прогнозів.

Автоматизація процесів: Створення спеціалізованих алгоритмів для автоматизації рутинних задач та процесів.

Захист даних: Розробка алгоритмів для забезпечення безпеки даних від несанкціонованого доступу або витоку.

2.1.3.2 Вимоги до інформаційного забезпечення

– Конфіденційність: Система інформаційного забезпечення має використовувати надійні методи захисту конфіденційності даних.

– Масштабованість: Система має бути гнучкою та готовою до розширення в разі зростання потреб.

– Доступність: Забезпечення безперебійної роботи системи цілодобово.

– Резервне копіювання: Гарантування наявності резервних копій інформації у випадку відмови сервера.

– Аналітика даних і звітність: Наявність інструментів аналізу даних і можливостей звітності для надання інформації та підтримки процесів управління та прийняття рішень.

2.1.3.3 Вимоги до лінгвистичного забезпечення

Все лінгвістичне забезпечення системи для організації взаємодії з користувачем повинно використовувати в переважно українську та англійську мови.

2.1.3.4 Вимоги до технічного забезпечення

– Види технічних засобів:

Комп'ютерне обладнання: Включає сервери, робочі станції, мобільні пристрої, мережеве обладнання (маршрутизатори, комутатори).

Програмно-технічні комплекси: ПО та апаратні платформи, інтегровані для виконання специфічних завдань (наприклад, системи управління базами даних, CRM системи).

Комплектуючі вироби: Джерела безперебійного живлення, системи охолодження, модулі розширення.

– Функціональні та конструктивні характеристики:

Продуктивність: Здатність обладнання витримувати навантаження, передбачене в рамках операційної діяльності компанії.

Надійність: Висока доступність та мінімальний ризик відмов у критичні моменти.

Масштабованість: Можливість збільшення обсягу технічних ресурсів без значних затрат часу та коштів.

Безпека: Захист від несанкціонованого доступу та втручання в роботу системи.

2.1.3.5 Вимоги до організаційного забезпечення

– Процедури взаємодії: Чіткі процедури для взаємодії між підрозділами, що забезпечують ефективну комунікацію та вирішення задач.

– Автоматизація процесів: Впровадження автоматизованих систем для спрощення рутинних завдань та покращення взаємодії.

2.1.3.6 Вимоги до методичного забезпечення

Склад нормативно-технічної документації:

Стандарти: Застосування міжнародних та національних стандартів в області IT (ISO/IEC, IEEE).

Нормативи: Відповідність вимогам з охорони праці, пожежної безпеки та екологічним нормам.

Методики: Розробка і застосування методик для аналізу, тестування та експлуатації системи.

2.2 Розробка апаратної частини комп’ютерної системи

2.2.1 Розробка загальної архітектури мережі підприємства

Підключення між маршрутизаторами виконується за допомогою кабелів Serial DTE або крос-кабелів. Маршрутизатори з комутаторами з'єднуються між собою за допомогою прямих кабелів, так само, як і комп'ютери до комутаторів. Для підключення комутаторів використовується крос-кабель.

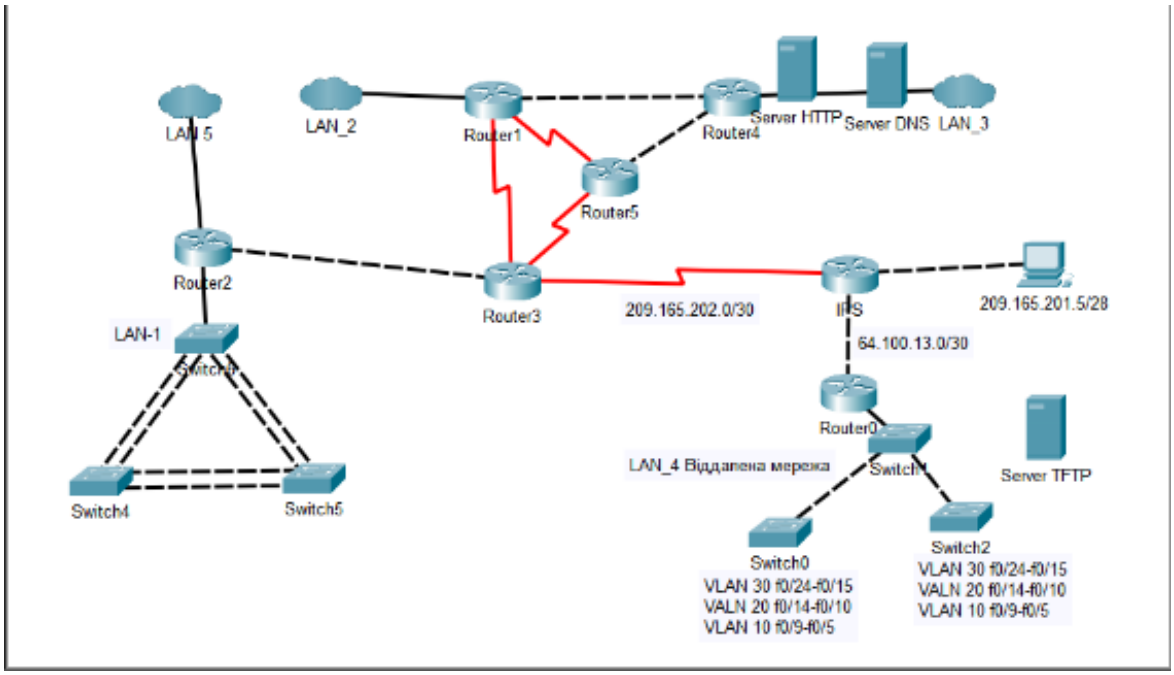

Рисунок 2.3 – Структурна схема комплексу технічних засобів комп’ютерної системи

2.2.2 Вибір і обґрунтування структурної схеми комплексу технічних засобів комп’ютерної системи

Ця схема включає:

Використання маршрутизаторів і комутаторів: Розміщення маршрутизаторів і комутаторів дозволяє ефективно керувати мережним трафіком, забезпечує високу доступність і розподіл навантаження між різними вузлами мережі.

Сегментація мережі через VLAN: Використання VLAN допомагає в ізоляції трафіку в межах мережі, підвищує безпеку і спрощує управління мережею.

Основні принципи вибору даної структурної схеми базуються на наступних міркуваннях:

Масштабованість: Схема забезпечує легке масштабування мережі з мінімальними змінами у вже існуючій конфігурації. Додавання нових сегментів мережі або підключення нового обладнання може бути виконано без значних витрат часу та ресурсів.

Надійність: Структура мережі включає резервні з'єднання між ключовими компонентами (як видно з червоних ліній на діаграмі), що забезпечує високий рівень надійності та доступності послуг в умовах відмови одного або декількох вузлів.

Безпека: Використання різних рівнів мережевих адрес і сегментування через VLAN дозволяє впроваджувати диференційовані політики безпеки, обмежуючи доступ до ресурсів компанії і забезпечуючи захист від зовнішніх і внутрішніх загроз.

Оптимізація витрат: Структура схеми оптимізована таким чином, щоб зменшити витрати на технічне обладнання та експлуатаційні витрати, використовуючи ефективне підключення і взаємодію компонентів системи.

2.2.3 Розробка специфікації апаратних засобів комп’ютерної системи

Таблиця 2.1 – Специфікація обладнання

Позиція	Найменування і технічна характеристика	Тип, марка, позначення документа	Одиниці виміру	Кількість
1	**2**	**3**	**4**	**5**
1	Маршрутизатор: 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 2911	Од.	5
2	Комутатор: 24 x Ethernet 10/100/1000 Мбіт/сек, RIP v1, RIP v2, OSPF, USB-порт, LAN Base, 4 SFP слоти	Cisco Catalyst 2960-24TT	Од.	24
4	Сервер: 2 шт x Intel Xeon E5-2650L v2 (1.70-2.10 GHz),	Cisco UCS C220 M3 LFF	Од.	3

2.2.4 Розрахунок інтенсивності трафіку вихідного трафіку найбільшої локальної мережі підприємства

Пропускна здатність лінії вихідного каналу дорівнює 1000Мбіт/с.

Швидкість надходження пакетів повинна бути менше, ніж швидкість відправлення для того, щоб не перевантажувати канал.

Середня інтенсивність трафіку μ=176 кадрів/с, а середня довжина повідомлення складає 650 байт.

Припустимо, що всі користувачі одночасно використовують послуги. Розрахуємо пропускну здатність LAN_3, яка складається з 121 вузлів. Пропускна здатність мережі на рівні доступу буде дорівнювати:

$$P_{р.р} = \mu * L_{пов} * N * 8 = 176 * 650 * 121 * 8 = 110{,}739 \text{ Мбіт/с}, \quad (2.1)$$

де N – кількість вузлів в мережі

$L_{пов}$ – середня довжина повідомлення

Отримані результати не перевищують заданих параметрів мережі по вихідному каналу, тому перевантажень не буде.

Комутатор рівня доступу передає трафік до маршрутизатора через вихідний порт зі швидкістю передачі даних 1000Мбіт/с.

Загальне навантаження на комутатор не повинно перевищувати:

$$\mu_{вих} = 1000\,000\,000/(650*8) = 192308 \text{ пакетів/с} \quad (2.2)$$

Оскільки кожне джерело в середньому виробляє в середньому 176 пакетів/с, то кількість приєднань, якими обмежен комутатор рівня доступу, складає максимум:

$$N = \mu_{вих}/\mu = 192308/178 = 1080 \text{ джерел} \quad (2.3)$$

Це задовольняє найбільшу мережу з 121 ПК.

Кожен з 121 ПК посилає потік заявок з інтенсивністю 176 кадрів/с. Інтенсивність вихідного трафіку:

$$\lambda = N * \mu = 121 * 98 = 11\,858 \text{ пакетів/с} \quad (2.4)$$

Коефіцієнт затримки:

$$\rho = \lambda/\mu_{вих} = 11858/192308 = 0{,}06 \quad (2.5)$$

Коефіцієнт зайнятості комутатора рівня доступу:

$$\rho=\rho/(1-\rho)=0,06/0,94=0,063 \quad (2.6)$$

Середня затримка кадру, пов’язана з чергою M/M/1, дорівнює:

$$T=1/(\mu_{вих}-\lambda)=1/(192308-11858)=5,54 \text{ мкс} \quad (2.7)$$

Середня довжина черги:

$$L_{чер}= \rho^2 /(1-\rho)=0,06^2 /0,94=0,0038 \quad (2.8)$$

Середній час перебування пакета у черзі:

$$T_{оч}= L_{чер}/ \lambda=0,0038/11858=0,320 \text{ мкс} \quad (2.9)$$

Це значення менше 6 мс, що задовольняє вимогам.

3 РОЗРОБКА КОРПОРАТИВНОЇ МЕРЕЖІ

3.1 Проектування логічної топології

На рисунку 3.1 представлено структуру корпоративної мережі. Вона містить центральну та дистанційну частини, а також частину, що належить постачальнику інтернет-послуг.

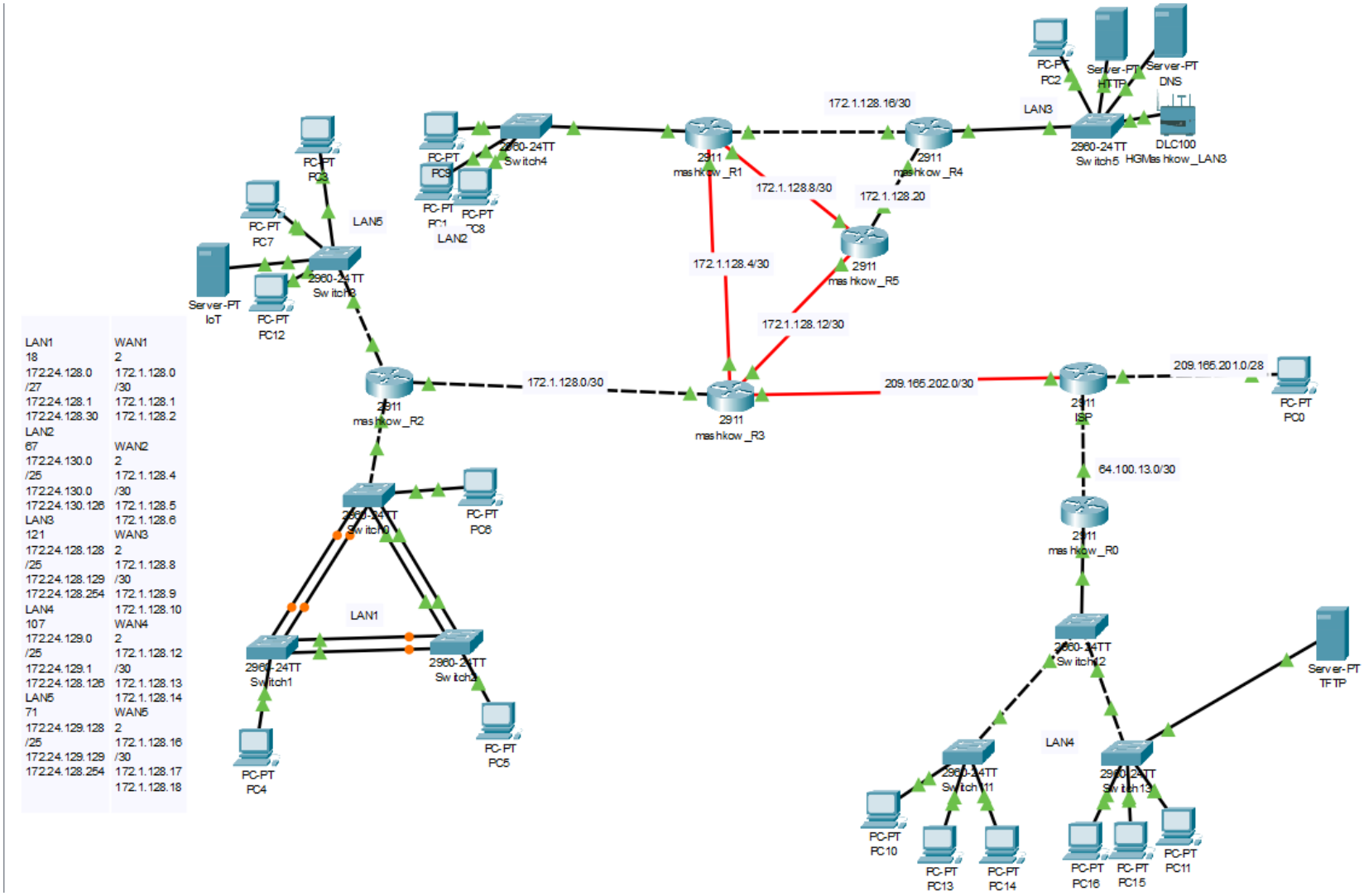

Рисунок 3.4 – Схема логічної топології

3.2 Вибір та опис мережного обладнання

У рамках проектування мережі компанії необхідно вибрати обладнання, що забезпечить надійність, високу пропускну здатність та можливість масштабування мережі. Нижче описано основне мережеве обладнання, яке було вибрано для імплементації мережевої інфраструктури.

– Маршрутизатор: Cisco 2911

Технічна характеристика:

Інтегровані інтерфейси: 4 вбудованих GE порти, 3 портів 1000Base-X (SFP).

Маршрутизація та обробка: Інтегровані Routing Processor (RP), SPA Interface Processor (SIP) та Embedded Services Processor (ESP).

Пропускна здатність: до 3 Гбіт/с.

Модульність: 1 слот для Network Interface Modules (NIM) та 1 слот для Shared Port Adapters (SPA).

Захист: Система підтримує криптографічні механізми, Dual Power Supply (P/S) для збільшення надійності.

Пам'ять: 8 ГБ оперативної пам'яті.

Живлення: 2 x AC.

– Комутатор: Cisco Catalyst 2960-24TT

Технічна характеристика:

Порти: 24 x Ethernet 10/100/1000 Мбіт/сек.

Маршрутизація: Підтримка RIP v1, RIP v2 та OSPF.

Керування: Вбудоване програмне забезпечення LAN Base забезпечує базові можливості керування мережею.

– Сервер: Cisco UCS C220 M3 LFF

Технічна характеристика:

Процесори: 2 шт x Intel Xeon E5-2650L v2 (1.70-2.10 GHz).

Оперативна пам'ять: 8 GB DDR3.

Мережеві інтерфейси: 2x порти 1 Gb Ethernet для забезпечення мережевих з'єднань та управління.

Розширення: Сервер має можливість для додавання жорстких дисків та додаткових мережевих карт, що дозволяє збільшити об'єм зберігання та пропускну здатність.

3.3 Розрахунок схеми адресації корпоративної мережі

Розділення мережі 172.24.128.0/21 на підмережі передбачає створення окремих сегментів IP-адресного простору для кожної з підмереж. Метод VLSM дозволяє ефективно управляти цим процесом, забезпечуючи точне відповідність кількості адрес кожної підмережі до її реальних потреб.

Таблиця 3.1 – Блок адрес мережі та кількість вузлів в кожній підмережі

№	Блок адрес	LAN1	LAN2	LAN3	LAN4	LAN5
11	172.24.128.0/21	18	67	121	107	71

Тобто, необхідно створити 5 підмереж для 384 користувачів.

Для розділення блоку адрес 172.24.128.0/21 на п’ять підмереж використовується метод VLSM, що дозволяє ефективно розподілити адресний простір в залежності від потреб кожної підмережі у вузлах.

Для LAN1 з 18 вузлами: використовуємо маску /27, що забезпечує 32 адреси, досить для 18 вузлів з урахуванням адреси мережі та широкомовної адреси.

Для LAN2 з 67 вузлами: обираємо маску /25, надаючи 128 адрес, що достатньо для 67 вузлів.

Для LAN3 з 121 вузлом: також використовуємо маску /25 для 128 адрес.

Для LAN4 з 107 вузлами: застосовуємо маску /25, що забезпечує 128 адрес.

Для LAN5 з 71 вузлом: обираємо маску /25, що забезпечує 128 адрес.

Підмережа LAN1 (18 вузлів)

Визначення маски: Для підтримки 18 вузлів з врахуванням мережевої та широкомовної адрес, використовуємо маску /27, яка надає 32 адрес.

Двійковий розрахунок: LAN1 - 172.24.128.0, що у двійковому форматі: 10101100.00011000.10000000.00000000. Широкомовна адреса для цієї підмережі буде 172.24.128.31, що в двійковому форматі виглядає як 10101100.00011000.10000000.00011111.

Діапазон IP-адрес: 172.24.128.1 - 172.24.128.30.

Підмережа LAN2 (67 вузлів)

Визначення маски: Для підтримки 67 вузлів з врахуванням мережевої та широкомовної адрес, використовуємо маску /25, яка надає 128 адрес.

Двійковий розрахунок: Виходимо з наступної адреси після LAN1 - 172.24.128.32, що у двійковому форматі: 10101100.00011000.10000000.00100000. Широкомовна адреса для цієї підмережі буде 172.24.128.127, що в двійковому форматі виглядає як 10101100.00011000.10000000.01111111.

Діапазон IP-адрес: 172.24.128.33 - 172.24.128.126.

Підмережа LAN3 (121 вузлів)

Визначення маски: Аналогічно, для підтримки 121 вузла використовуємо маску /25, надаючи 128 адрес.

Двійковий розрахунок: Стартуємо з адреси 172.24.128.128 (10101100.00011000.10000000.10000000). Широкомовна адреса буде 172.24.128.255 (10101100.00011000.10000000.11111111).

Діапазон IP-адрес: 172.24.128.129 - 172.24.128.254.

Підмережа LAN4 (107 вузлів)

Визначення маски: Через велику кількість вузлів в LAN4 також використовуємо маску /25.

Двійковий розрахунок: Починаючи з нового сегмента адрес 172.24.129.0 (10101100.00011000.10000001.00000000). Широкомовна адреса для LAN4 буде 172.24.129.127 (10101100.00011000.10000001.01111111).

Діапазон IP-адрес: 172.24.129.1 - 172.24.129.126.

Підмережа LAN5 (71 вузлів)

Визначення маски: Для підтримки 71 вузла, використовуємо маску /25, що надає 128 адрес.

Двійковий розрахунок: З наступною доступною адресою 172.24.129.128 (10101100.00011000.10000001.10000000). Широкомовна адреса буде 172.24.129.255 (10101100.00011000.10000001.11111111).

Діапазон IP-адрес: 172.24.129.129 - 172.24.129.254.

Таблиця 3.2 – Схема адресації мережі

Назва мережі	Кількість вузлів	Номер мережі	Маска мережі	Початкове значення діапазону можливих адрес вузлів у підмережі	Кінцеве значення діапазону можливих адрес вузлів у підмережі
LAN1	18	172.24.128.0	/27	172.24.128.1	172.24.128.30
LAN2	67	172.24.130.0	/25	172.24.130.33	172.24.130.126
LAN3	121	172.24.128.128	/25	172.24.128.129	172.24.128.254
LAN4	107	172.24.129.0	/25	172.24.129.1	172.24.128.126
LAN5	71	172.24.129.128	/25	172.24.129.129	172.24.128.254

Для каналів між маршрутизаторами буде застосовуватися блок адрес 172.1.128.0/21. Так само за допомогою методу VLSM розділимо мережу на п’ять підмереж з двома вузлами в кожній. В таблиці 3.3 представлено схему адресації каналів між маршрутизаторами.

Таблиця 3.3 – Схема адресації каналів між маршрутизаторами

Назва мережі	Кількість вузлів	Номер мережі	Маска мережі	Початкове значення діапазону можливих адрес вузлів у підмережі	Кінцеве значення діапазону можливих адрес вузлів у підмережі
WAN1	2	172.1.128.0	/30	172.1.128.1	172.1.128.2
WAN2	2	172.1.128.4	/30	172.1.128.5	172.1.128.6
WAN3	2	172.1.128.8	/30	172.1.128.9	172.1.128.10
WAN4	2	172.1.128.12	/30	172.1.128.13	172.1.128.14
WAN5	2	172.1.128.16	/30	172.1.128.17	172.1.128.18

Таблиця 3.4 – Схема адресації маршрутизаторів

Пристрій	Інтерфейс	IP-адреса	Маска
mashkow_R0	Gig0/0	64.100.13.2	255.255.255.252
	Gig0/1	Vlan	
mashkow_R1	Gig0/0	172.24.130.1	255.255.255.128
	Gig0/1	172.1.128.5	255.255.255.252
	Se0/0/0	172.1.128.17	255.255.255.252
	Se0/0/1	172.1.128.9	255.255.255.252
mashkow_R2	G0/1	172.1.128.1	255.255.255.252
	Gig0/2	172.24.128.1	255.255.255.224
	Gig0/3	172.24.129.129	255.255.255.128

Продовження таблиці 3.4

mashkow_R3	Gig0/1	172.1.128.2	255.255.255.252
	Se0/0/1	172.1.128.6	255.255.255.252
	Se0/0/2	172.1.128.13	255.255.255.252
	Se0/0/3	209.165.202.1	255.255.255.252
mashkow_R4	Gig0/1	172.1.128.18	255.255.255.252
	Gig0/2	172.1.128.21	255.255.255.252
	Gig0/3	172.24.128.129	255.255.255.128
mashkow_R5	Se0/1/1	172.1.128.14	255.255.255.252
	Se0/0/0	172.1.128.210	255.255.255.252
	Gig0/1	172.1.128.22	255.255.255.252
ISP	Se0/0/0	209.165.202.2	255.255.255.252
	Gig0/1	64.100.13.1	255.255.255.252
	Gig0/2	209.165.201.1	255.255.255.224

3.4 Вибір та налаштування способу маршрутизації

3.4.1 Базове налаштування конфігурації пристроїв

Базове налаштування конфігурації пристроїв на прикладі mashkow_R3:

```
hostname mashkow_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 # mashkow_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 12321_ mashkow_R3 password admincisco // призначення імені користувача та паролю
ip domain-name mashkow_R3// налаштування імені домена
crypto key generate rsa // створення ключа шфируваня
1024 // вибір довжини ключа шифрування
int se0/0/0 // вибір DCE-інтерефейсу
clock rate 128000 // встановлення значення тактової частоти
int se0/0/1
clock rate 128000
```

В LAN_1 використовується технологія Etherchannel, яка дозволяє об’днати декілька фізичних інтерфейсів мережевого пристрою в один логічний канал. Це дозволяє збільшити пропускну здатність та підвищити надійність каналів в мережі. Налаштування Etherchannel на прикладі комутатора з цієї 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 проходженя 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
```

3.4.2 Налаштування маршрутизаторів корпоративної мережі

Для призначення адрес комп’ютерам в мережі буде використовуватись DHCP – мережевий протокол, який дозволяє автоматично призначати IP-адреси вузлам в підмережах. Це спрощує адміністрування мережі та налаштування пристроїв.

Налаштування DHCP на прикладі маршрутизатора mashkow_R1:

```
ip dhcp excluded-address 172.24.130.3 172.24.130.5
ip dhcp excluded-address 172.24.130.127
ip dhcp excluded-address 172.24.130.128
ip dhcp pool LAN-2
network 172.24.130.0 255.255.255.128
default-router 172.24.130.1
dns-server 172.24.128.250
```

Щоб забезпечити взаємодію між користувачами з різних підмереж, необхідно організувати маршрутизацію між цими мережами. Існують два основних методи організації маршрутів: статичний та динамічний. У рамках статичної маршрутизації, маршрути задаються вручну, тоді як динамічна маршрутизація дозволяє автоматично адаптуватися до змін у мережі, забезпечуючи більшу гнучкість і автоматизацію. У даній роботі використовується протокол динамічної маршрутизації OSPF, який є одним з найбільш вживаних у сучасних мережевих рішеннях. OSPF використовує алгоритм SPF для пошуку найкоротших шляхів, що підвищує швидкість роботи мережі. Основні переваги OSPF включають його масштабованість, безпеку, підтримку VLSM та сумісність з технікою різних виробників. Конфігурація протоколу OSPF буде продемонстрована на прикладі маршрутизатора mashkow_R1.

```
router ospf 1
 log-adjacency-changes
 passive-interface default
 no passive-interface GigabitEthernet0/0
 no passive-interface GigabitEthernet0/1
 no passive-interface GigabitEthernet0/2
 no passive-interface Serial0/3/0
 no passive-interface Serial0/3/1
 auto-cost reference-bandwidth 1000
 network 172.24.130.0 0.0.0.127 area 0
```

```
network 172.1.128.16 0.0.0.3 area 0
network 172.1.128.4 0.0.0.3 area 0
network 172.1.128.8 0.0.0.3 area 0
```

На граничному маршрутизаторі mashkow_R3 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 209.165.201.0 255.255.255.240 209.165.202.1
```

3.4.3 Налаштування роботи Інтернет

Щоб забезпечити доступ системи до Інтернету, необхідно впровадити NAT, технологію, яка дозволяє трансформувати одну або декілька приватних IP-адрес в одну або декілька зовнішніх IP-адрес та навпаки, включаючи перетворення номерів портів.

```
ip access-list extended NAT11
deny ip 172.24.128.0 0.0.0.31 172.24.129.0 0.0.0.127
deny ip 172.24.128.0 0.0.0.127 172.24.129.0 0.0.0.127
deny ip 172.24.128.128 0.0.0.127 172.24.129.0 0.0.0.127
deny ip 172.24.129.128 0.0.0.127 172.24.129.0 0.0.0.127
deny ip 172.1.128.0 0.0.0.255 172.24.129.0 0.0.0.127
permit ip 172.24.128.0 0.0.0.31 any
permit ip 172.24.128.0 0.0.0.127 any
permit ip 172.24.128.128 0.0.0.127 any
permit ip 172.24.129.128 0.0.0.127 any
ip nat inside source list NAT12 pool Internet
ip nat inside source static 172.24.128.200 209.165.200.4
ip nat inside source static 172.24.128.60 209.165.200.3
```

```
interface Serial0/3/0
ip nat inside
interface GigabitEthernet0/0
ip nat inside
interface GigabitEthernet0/1
ip nat inside
interface GigabitEthernet0/2
ip nat inside
interface Serial0/3/1
ip nat outside
```

3.5 Налаштування мереж VLAN, маршрутизації між VLAN

Технологія VLAN застосовується для поділу однієї фізичної мережі на кілька віртуальних підмереж. Завдяки VLAN можна скоротити потребу в фізичному розміщенні пристроїв та кабелях, покращити безпеку та ефективніше управляти мережевим трафіком. Підмережу LAN_3 розділено на три віртуальні підмережі. Підмережа LAN_4 була розділена на три підмережі VLAN. Номери VLAN мереж представлені в таблиці 3.4 [5].

Таблиця 3.5 – Адресація мереж VLAN

Назва	Адреса мережі	Хост	Маска	Використовувані адеси
VLAN10	172.24.129.0	30	/27	172.24.129.1 - 172.24.129.30
VLAN20	172.24.129.32	30	/27	172.24.129.33 - 172.24.129.62
VLAN30	172.24.129.64	30	/27	172.24.129.65 - 172.24.129.94
VLAN99	72.24.129.96	14	/28	172.24.129.97 - 172.24.129.110
VLAN100	172.24.129.112	14	/28	172.24.129.113 - 172.24.129.126

Технологія VLAN застосовується для поділу однієї фізичної мережі на кілька віртуальних сегментів. Це сприяє зниженню необхідності у фізичному розміщенні обладнання та кабельної інфраструктури, покращує безпеку системи та підвищує ефективність управління мережевим трафіком. Підмережа LAN_3 була поділена на три окремі VLAN.

Налаштування VLAN на прикладі комутатора з мережі:

int range fa0/6-10 // вибір портів
switchport mode access // налаштування портів
switchport access vlan 10 // присвоювання портам влану
int range fa0/11-15
switchport mode access
switchport access vlan 20
int range fa0/16-24
switchport mode access
switchport access vlan 30
int range fa0/1-5
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 дозволених VLAN на транковому порті
Налаштування портів на комутаторах, привласнивши їм адреси з мережі Management VLAN, на прикладі комутатора:
int vlan 99 // вибір VLAN
ip address 172.24.129.98 255.255.255.240 // призначення IP-адреси
ip default-gateway 172.24.129.97 // вказання IP-адреси шлюзу за замовчуванням

Налаштовуємо підінтерфейси на маршрутизаторі, 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 172.24.129.0 255.255.255.224 // вказання IP-адреси підінтерфейсу
int g0/1.20
encapsulation dot1Q 20
ip address 172.24.129.32 255.255.255.224
int g0/1.30
encapsulation dot1Q 30
ip address 172.24.129.64 255.255.255.224
int g0/1.99

```
encapsulation dot1Q 99
ip address 172.24.129.96 255.255.255.240
```

Протокол DHCP застосовуватиметься для автоматичного розподілу IP-адрес мережевим вузлам у різних VLAN. Конфігурація DHCP на маршрутизаторі, який функціонуватиме як DHCP-сервер, включатиме наступні кроки:

```
ip dhcp excluded-address 172.24.129.1 172.24.129.5
ip dhcp excluded-address 172.24.129.126
ip dhcp excluded-address 172.24.129.127
ip dhcp excluded-address 172.24.129.1 172.24.129.10
ip dhcp excluded-address 172.24.129.5
ip dhcp pool LAN4-VLAN10
network 172.24.129.0 255.255.255.224
default-router 172.24.129.1
dns-server 172.24.128.250
ip dhcp pool LAN4-VLAN20
network 172.24.129.32 255.255.255.224
default-router 172.24.129.33
dns-server 172.24.128.250
ip dhcp pool LAN4-VLAN30
network 172.24.129.64 255.255.255.224
default-router 172.24.129.65
dns-server 172.24.128.250
```

3.5.2 Конфігурація віртуальної приватної мережі (VPN)

VPN — це технологія, яка застосовується для створення безпечних з'єднань через відкриті, небезпечні мережі, такі як інтернет. У даному випадку, VPN використовуватиметься для забезпечення доступу з віддаленої локації до головної мережі.

Налаштування VPN :

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

ip access-list extended VPN11 // створення ACL-списку VPN12, щоб визначити трафік з основної мережі до віддаленої

permit ip 172.24.129.0 0.0.0.127 172.24.128.0 0.0.0.31 // надання доступу на проходження пакетів з основної на віддалену мережу

permit ip 172.24.129.0 0.0.0.127 172.24.128.32 0.0.0.63

permit ip 172.24.129.0 0.0.0.127 172.24.128.128 0.0.0.127

permit ip 172.24.129.0 0.0.0.127 172.24.129.128 0.0.0.127

permit ip 172.24.129.0 0.0.0.127 172.1.128.0 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 209.165.202.2 // 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 209.165.202.2 // створення піра

set transform-set TS // вибір набору перетворень

match address VPN11 // прив'язка до списку VPN12

int GigabitEthernet0/1 // вибір інтерфейсу

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

3.6 Захист інформації в комп'ютерній системі від несанкціонованого доступу

3.6.1 Налаштування маршрутизаторів на підтримку служби AAA

AAA представляє собою систему управління та контролю доступу до мережевих ресурсів, виконуючи ролі ідентифікації та авторизації користувачів. Одним із ключових елементів AAA є сервер RADIUS, який забезпечує централізовані послуги аутентифікації та авторизації для користувачів, що звертаються за доступом до мережі через маршрутизатори та комутатори.

Налаштовуємо всі маршрутизаторів на підтримку служби AAA на прикладі одного з роутерів

aaa new-model // увімкнення служби AAA

radius-server host 172.24.128.251 auth-port 1645 key radius123 // вказанн 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 mashkow_R3 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 методуаутентифікації для доступу через VTY-порти

3.7 Перевірка комп'ютерної Системи підприємства

Перевіряємо базові налаштування обладнання на прикладі маршрутизатора mashkow_R2. Використовуючи команду do show running-config, ми аналізуємо назву пристрою, налаштування паролів для доступу до консолі, ліній vty та їхню конфігурацію для використання протоколу ssh, пароль для доступу до привілейованого режиму, налаштування банера MOTD а також ім'я домену.

```
!
hostname mashkow_R2
!
```

Рисунок 3.5 – Ідентифікація маршрутизатору

```
!
line con 0
 password 7 0822455D0A16
 login authentication console
!
```

Рисунок 3.6 – Доступ до консольного інтерфейсу через пароль

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

Рисунок 3.7 – Аутентифікація для термінальних ліній з використанням ssh

```
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
```

Рисунок 3.8 – Ключ доступу до розширеного режиму

```
!
banner motd ^Cmashkow_R2^C
!
```

Рисунок 3.9 – Зображення стартового повідомлення системи

```
!
ip domain-name mashkow_R2
!
```

Рисунок 3.10 – Визначення доменного імені

```
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 – Застосування технології EtherChannel

```
mashkow_R3#show ip protocol

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 209.165.202.1
  It is an autonomous system boundary router
  Redistributing External Routes from,
    static
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.1.128.0 0.0.0.3 area 0
    172.1.128.12 0.0.0.3 area 0
    172.1.128.4 0.0.0.3 area 0
    209.165.202.0 0.0.0.3 area 0
  Passive Interface(s):
    Vlan1
    GigabitEthernet0/1
    GigabitEthernet0/2
    Serial0/2/1
  Routing Information Sources:
    Gateway         Distance      Last Update
    172.1.128.22         110      00:24:11
    172.24.128.33        110      00:24:11
    172.24.128.129       110      00:24:12
    172.24.129.97        110      00:24:06
    172.24.129.129       110      00:24:07
    209.165.202.1        110      00:24:04
    209.165.202.2        110      00:24:05
  Distance: (default is 110)
```

Рисунок 3.12 – Конфігурація протоколу OSPF

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC3	PC10	ICMP		0.000	N	0	(edit)	

Рисунок 3.13 – Взаємозв'язок між мережами LAN_4 та LAN_5

```
mashkow_R3#show interfaces serial0/3/0
Serial0/3/0 is up, line protocol is up (connected)
  Hardware is HD64570
  Internet address is 172.1.128.14/30
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0 (size/max/drops); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/0/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 1158 kilobits/sec
  5 minute input rate 54 bits/sec, 0 packets/sec
  5 minute output rate 54 bits/sec, 0 packets/sec
     1520 packets input, 106008 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     1483 packets output, 103840 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

Рисунок 3.14 – Передача даних через послідовні інтерфейси

```
     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 3.15 – Початкова конфігурація маршрутизатора mashkow_R3

```
mashkow_R2

User Access Verification

Username: mashkow12321ck1
Password:
mashkow_R2>en
Password:
mashkow_R2#
```

Рисунок 3.16 – Активація служби аутентифікації та обліку на маршрутизаторі

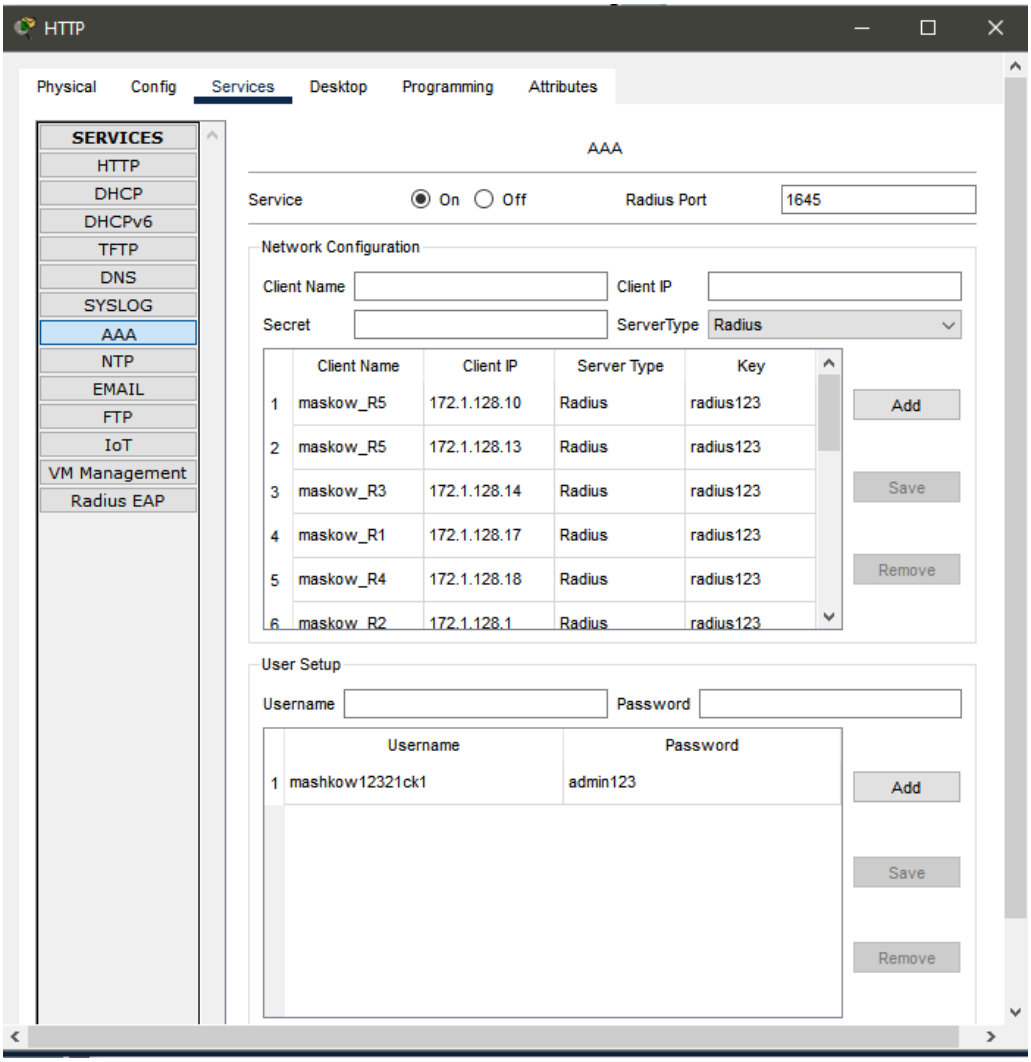

Рисунок 3.17 – Налаштування сервера для RADIUS

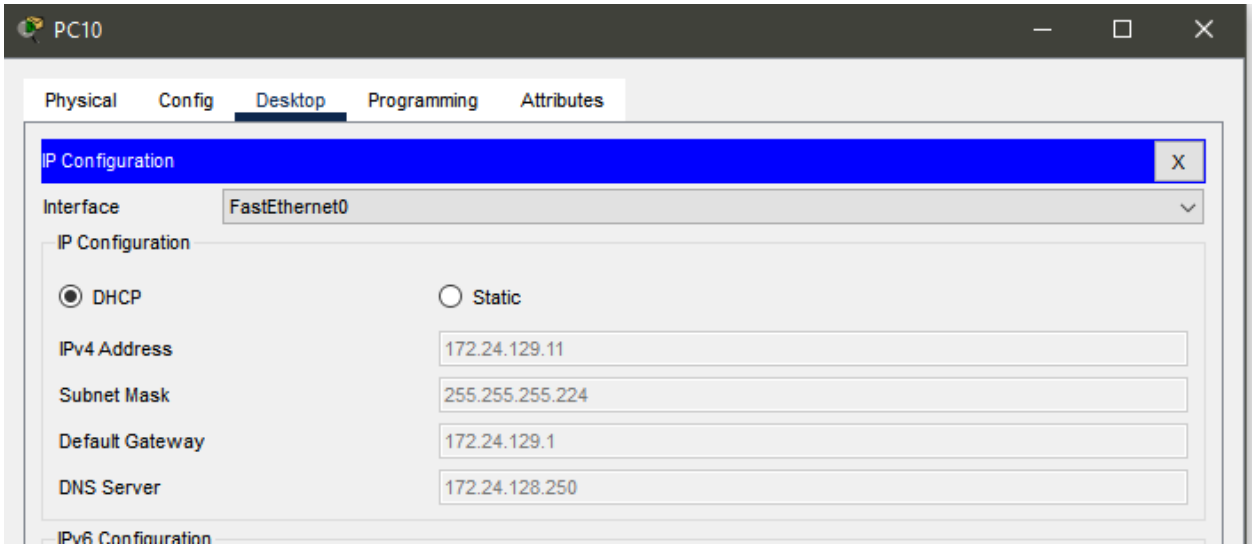

Рисунок 3.18 – Адреса комп'ютера PC10

```
mashkow_R3#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     172.1.128.2     YES manual up                    up
GigabitEthernet0/1     unassigned      YES unset  up                    down
GigabitEthernet0/2     unassigned      YES unset  up                    down
Serial0/2/0            209.165.202.1   YES manual up                    up
Serial0/2/1            unassigned      YES unset  down                  down
Serial0/3/0            172.1.128.14    YES manual up                    up
Serial0/3/1            172.1.128.5     YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
mashkow_R3#
```

Рисунок 3.19 – Адресація 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
------------------------------------------------------------------------------
```

Рисунок 3.20 – Вказівка портів та імен VLAN

```
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 3.21 – Конфігурація транк-портів

Як бачимо з рис. 3.23, зв’язок між PC10 та PC13, які знаходять в VLAN10 та VLAN20 відповідно, є успішним.

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC10	PC13	ICMP		0.000	N	0	(edit)	(delete)
	Successful	PC13	PC10	ICMP		0.000	N	1	(edit)	(delete)

Рисунок 3.22 – Взаємодія між VLAN10 та VLAN20

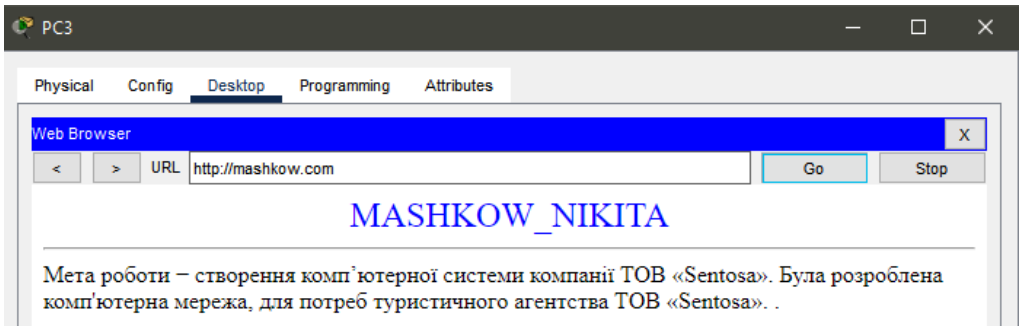

Рисунок 3.23 – Веб-сайт з інформацією про наукове завдання

4 РОЗРОБКА КОМПОНЕНТА СИСТЕМИ

4.1 Інженерне рішення по розробці компонента Системи

Інтернет речей представляє собою мережу фізичних об'єктів, що з'єднані з Інтернетом та мають можливість взаємодії. Ця система зазвичай включає в себе датчики, які моніторять умови навколишнього середовища, та пристрої, що активуються або деактивуються залежно від даних датчиків і налаштувань користувача. Це дозволяє автоматизувати багато процесів, таких як керування освітленням, температурою, вологістю тощо.

Під час створення корпоративної мережі особливу увагу приділяється розробці IoT компонентів, які контролюють доступ до приміщень за допомогою IRID міток і карт, а також системам клімат-контролю. Важливі елементи такої системи включають температурні датчики, кондиціонери, автоматичні вікна, пожежні датчики, вентилятори, картрідери, RFID мітки та сирени. Система також включає механізми для аварійного реагування, зокрема пожежогасіння.

Окрему систему термом-регулювання реалізувати у LAN3.

Ця IoT система інтегрована в мережу компанії та використовує сучасні протоколи для передачі даних, забезпечуючи надійність та ефективність роботи. Завдяки застосуванню технологій IoT створюється розумна система, здатна автоматично адаптуватися до змін в умовах навколишнього середовища і забезпечувати комфортні умови для користувачів без їхнього втручання [7].

4.2 Налаштування обладнання та сервісів системи IoT

Для розгортання IoT-системи в офісі спершу встановлюємо IoT-пристрої та датчики, підключаючи їх до Home Gateway. На цих Home Gateway в мережі налаштовуємо бездротову точку доступу, використовуючи як приклад мережу LAN2 з SSID "Mashkow_LAN2_12321ck1" та паролем "Mashkow__12321ck1", вдаючись до протоколу безпеки WPA2-PSK та методу шифрування AES.

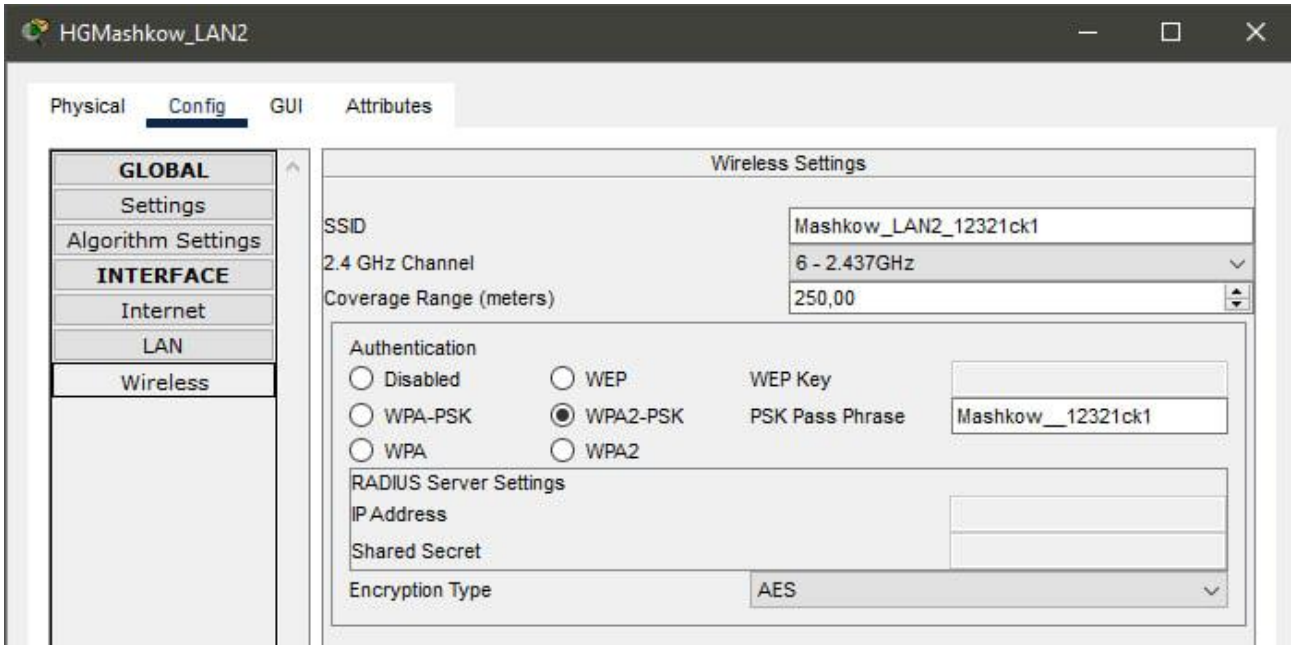

Рисунок 4.1 – Налаштування бездротової мережі

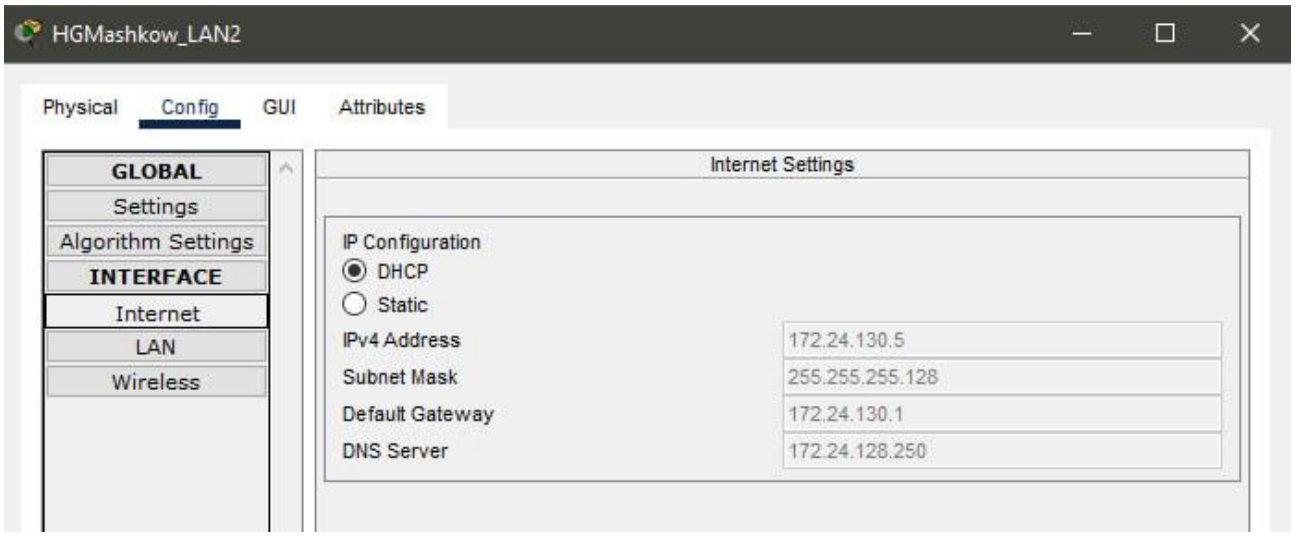

Рисунок 4.2 – Налаштування підключення до LAN2

Кожен IoT-пристрій налаштовуємо для підключення до Home Gateway, вводячи відповідні SSID та пароль. В якості IoT-сервера використовується IoT сервер в LAN5 з адресою "172.24.129.150". Топологічна схема корпоративної мережі з розміщенням IoT-пристроїв зображена на рис. 4.4

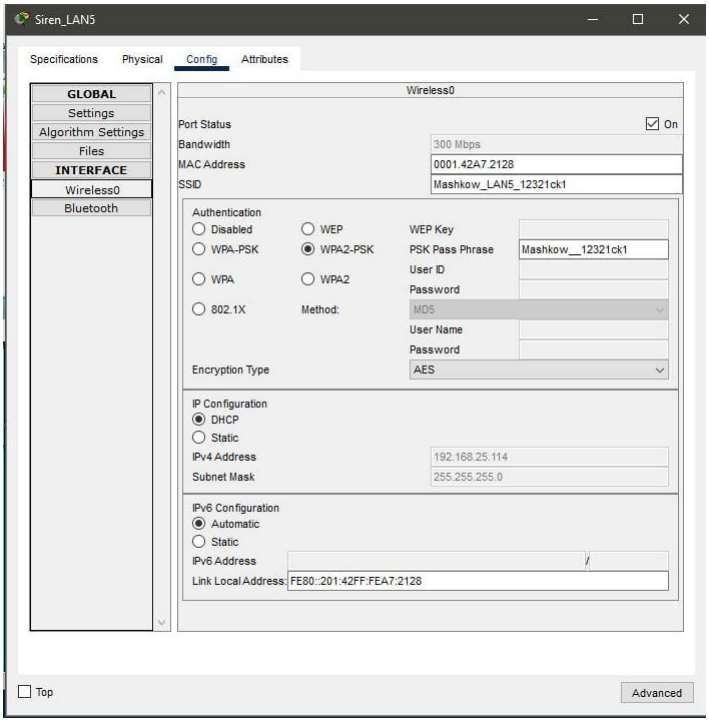

Рисунок 4.3 – Налаштування бездротової мережі на пристроях

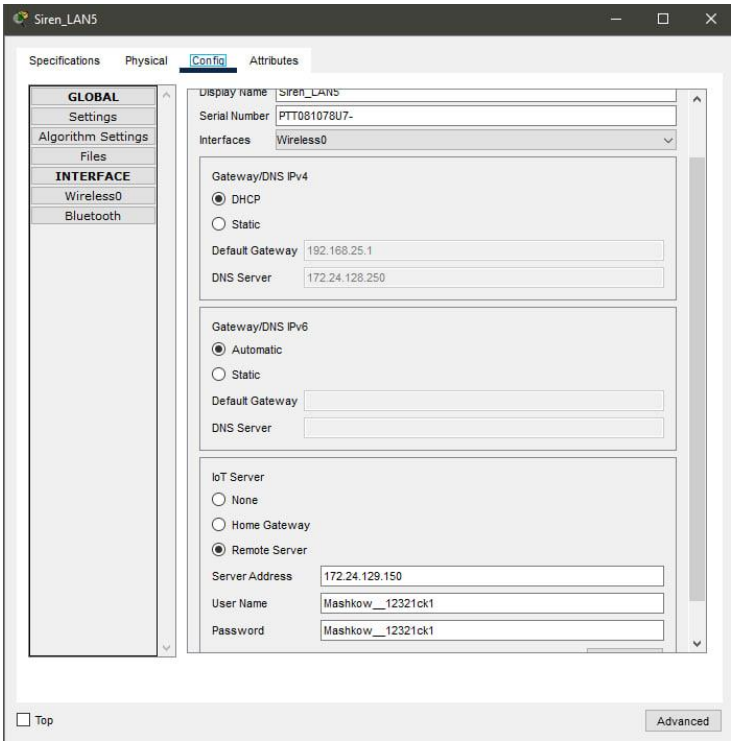

Рисунок 4.4 – Налаштування підключення до віддаленого серверу

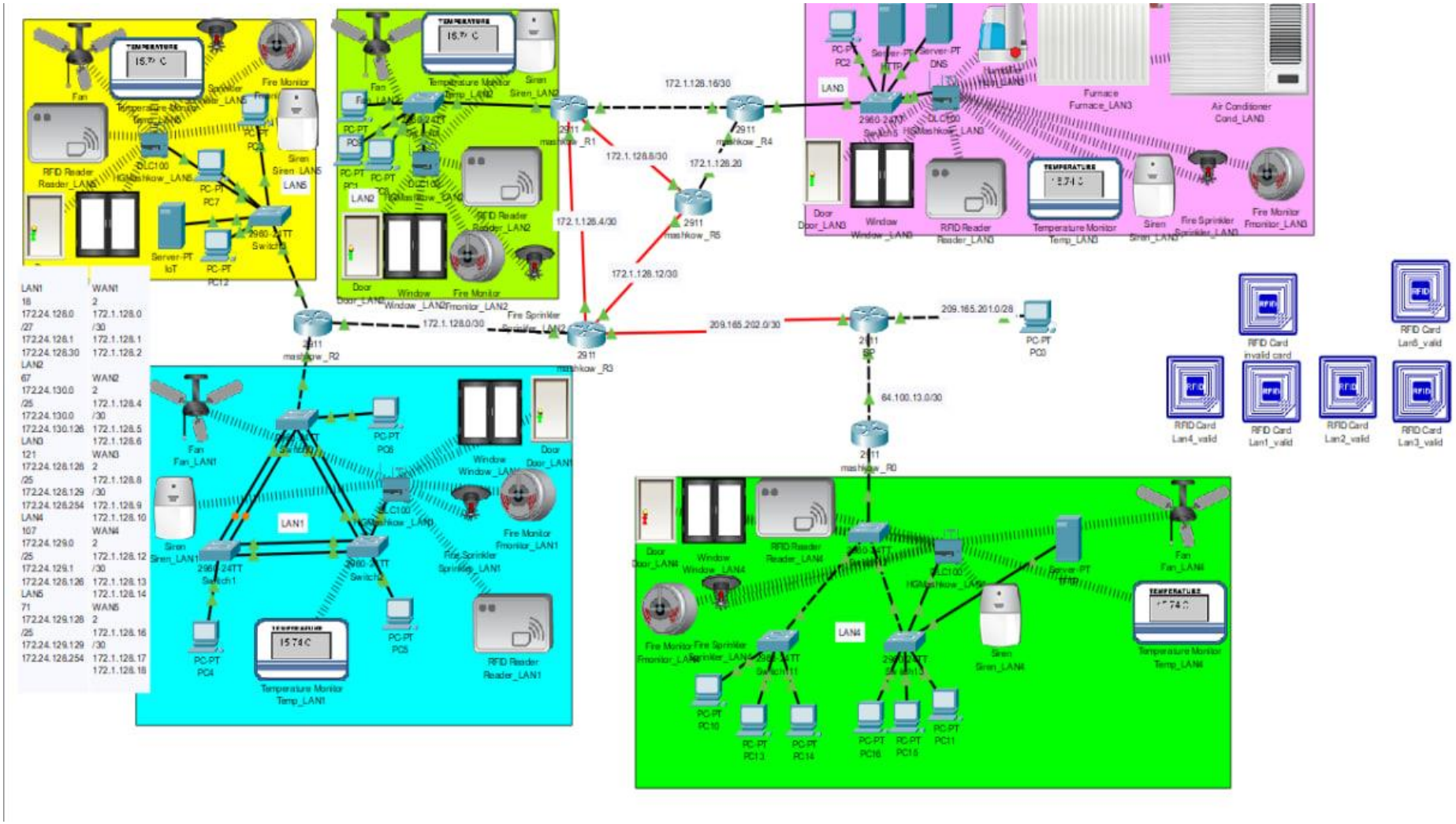

Рисунок 4.5 – Топологічна схема корпоративної мережі компанії з розміщенням IoT пристроїв

Для того, щоб налаштувати параметри роботи IoT-системи на будь-якому комп'ютері всередині мережі, необхідно спочатку запустити програму IoT Monitor. Цей інструмент дозволяє централізовано керувати всіма пристроями, підключеними до системи. В інтерфейсі програми вам потрібно ввести адресу шлюзу, який з'єднує всі IoT-пристрої з мережею, а також ваші облікові дані, тобто логін і пароль. Після авторизації ви отримаєте доступ до головної сторінки інтерфейсу управління.

На цій сторінці ви побачите список всіх підключених до системи IoT-пристроїв. Цей список часто візуалізується у вигляді таблиці або сітки, де кожен пристрій представлений окремою карткою або рядком. Для кожного пристрою вказані основні характеристики, такі як статус з'єднання, поточний стан і можливо навіть короткий опис. Також можна переглядати історію взаємодій і статистику роботи пристроїв.

На рисунку 4.6, на який посилається опис, зазвичай зображується приклад веб-інтерфейсу з відображенням всіх підключених пристроїв. Це може бути знімок екрану, який демонструє як виглядає список пристроїв на практиці, допомагаючи користувачам зорієнтуватися в можливостях та функціоналі IoT Monitor.

Заходимо на вкладку «Conditions» та натискаємо «Add» для додавання умов спрацювання пристроїв.

Для роботи з доступом, створено по 3 сценарії на підмережу, у першому сценарії відчиняться двері при валідном стані рідера, у другому двері зачиняються при спокійному стані рідера та у третьому сценарії рідер стає валідний при зчитані картки с пулом номерів.

При роботи з вікнами передбачено їх використання у багатьох сценаріях але їх основний сценарій це відкривання при температурі від 20 до 23 градусів для провітрювання приміщення, далі для всіх підмереж розроблено сценарій роботи з стельовим вентилятором, при температурі від 23 градусів він вмикається та зачиняються двері.

Окремо для LAN3 розроблено систему клімат контролю, при температурі нижчої за 19 градусів вмикається зволожувач повітря та батареї на нагрів, при температурі 23 та більше викається кондиційованння.

При виявлені будь де у мережі вогню, вмикається сповіщальна сирена во всій будівлі, та вмикається локальне тушіння де датчик вловив вогонь.

Для віддаленої мережі налаштовано теж саме як і в основній мережі тільки всі сценарії відокремлені шо б при впливі на будь яку с мереж сценарії не пересікались.

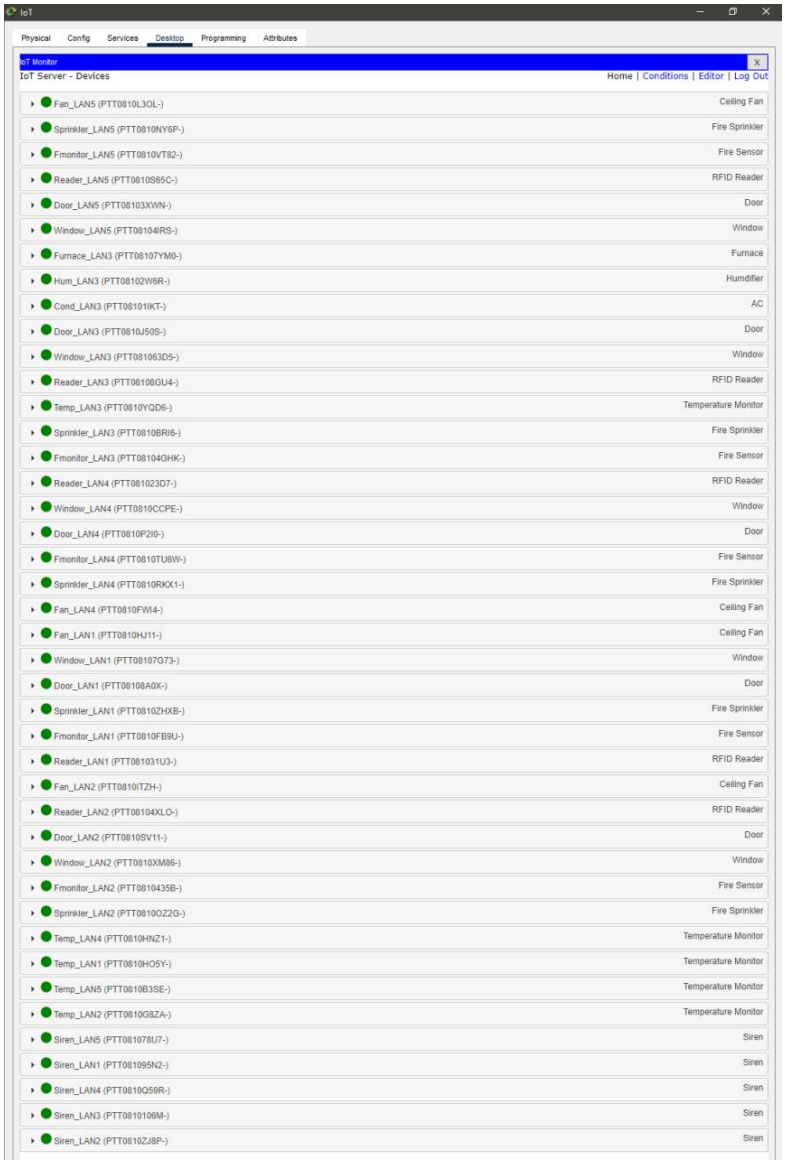

Рисунок 4.6 – Під’єднані IoT-пристрої основної мережі

Actions	Enabled	Name	Condition	Actions
Edit Remove	Yes	Door_close_LAN4	Reader_LAN4 Status is Waiting	Set Door_LAN4 Lock to Lock
Edit Remove	Yes	Door_Open_LAN4	Reader_LAN4 Status is Valid	Set Door_LAN4 Lock to Unlock
Edit Remove	Yes	Reader_Valid_LAN4	Reader_LAN4 Card ID = 401	Set Reader_LAN4 Status to Valid
Edit Remove	Yes	Door_close_LAN1	Reader_LAN1 Status is Waiting	Set Door_LAN1 Lock to Lock
Edit Remove	Yes	Door_Open_LAN1	Reader_LAN1 Status is Valid	Set Door_LAN1 Lock to Unlock
Edit Remove	Yes	Reader_Valid_LAN1	Reader_LAN1 Card ID = 101	Set Reader_LAN1 Status to Valid
Edit Remove	Yes	Door_close_LAN2	Reader_LAN2 Status is Waiting	Set Door_LAN2 Lock to Lock
Edit Remove	Yes	Door_Open_LAN2	Reader_LAN2 Status is Valid	Set Door_LAN2 Lock to Unlock
Edit Remove	Yes	Reader_Valid_LAN2	Reader_LAN2 Card ID = 201	Set Reader_LAN2 Status to Valid
Edit Remove	Yes	Door_close_LAN3	Reader_LAN3 Status is Waiting	Set Door_LAN3 Lock to Lock
Edit Remove	Yes	Door_Open_LAN3	Reader_LAN3 Status is Valid	Set Door_LAN3 Lock to Unlock
Edit Remove	Yes	Reader_Valid_LAN3	Reader_LAN3 Card ID = 301	Set Reader_LAN3 Status to Valid
Edit Remove	Yes	Door_close_LAN5	Reader_LAN5 Status is Waiting	Set Door_LAN5 Lock to Lock
Edit Remove	Yes	Door_Open_LAN5	Reader_LAN5 Status is Valid	Set Door_LAN5 Lock to Unlock
Edit Remove	Yes	Reader_Valid_LAN5	Reader_LAN5 Card ID = 501	Set Reader_LAN5 Status to Valid
Edit Remove	Yes	Fire_invalid_LAN1_2_3_5	Match all: • Fmonitor_LAN5 Fire Detected is false • Fmonitor_LAN3 Fire Detected is false • Fmonitor_LAN2 Fire Detected is false • Fmonitor_LAN1 Fire Detected is false	Set Sprinkler_LAN5 Status to false Set Sprinkler_LAN3 Status to false Set Sprinkler_LAN2 Status to false Set Sprinkler_LAN1 Status to false
Edit Remove	Yes	Fire_valid_LAN1	Fmonitor_LAN1 Fire Detected is true	Set Sprinkler_LAN1 Status to true Set Window_LAN1 On to false
Edit Remove	Yes	Fire_valid_LAN2	Fmonitor_LAN2 Fire Detected is true	Set Sprinkler_LAN2 Status to true Set Window_LAN2 On to false
Edit Remove	Yes	Fire_valid_LAN3	Fmonitor_LAN3 Fire Detected is true	Set Sprinkler_LAN3 Status to true Set Window_LAN3 On to false
Edit Remove	Yes	Fire_valid_LAN4	Fmonitor_LAN4 Fire Detected is true	Set Sprinkler_LAN4 Status to true Set Window_LAN4 On to false
Edit Remove	Yes	Fire_invalid_LAN4	Fmonitor_LAN4 Fire Detected is false	Set Sprinkler_LAN4 Status to false
Edit Remove	Yes	Fire_valid_LAN5	Fmonitor_LAN5 Fire Detected is true	Set Sprinkler_LAN5 Status to true Set Window_LAN5 On to false
Edit Remove	Yes	FAN_ON_LAN1	Match all: • Temp_LAN1 Temperature > 23.0 °C • Fmonitor_LAN1 Fire Detected is false	Set Fan_LAN1 Status to High Set Window_LAN1 On to false
Edit Remove	Yes	FAN_OFF_LAN1	Temp_LAN1 Temperature < 23.0 °C	Set Fan_LAN1 Status to Off
Edit Remove	Yes	FAN_ON_LAN2	Match all: • Temp_LAN2 Temperature > 23.0 °C • Fmonitor_LAN2 Fire Detected is false	Set Fan_LAN2 Status to High Set Window_LAN2 On to false
Edit Remove	Yes	FAN_OFF_LAN2	Temp_LAN2 Temperature < 23.0 °C	Set Fan_LAN2 Status to Off
Edit Remove	Yes	FAN_ON_LAN4	Match all: • Temp_LAN4 Temperature > 23.0 °C • Fmonitor_LAN4 Fire Detected is false	Set Fan_LAN4 Status to High Set Window_LAN4 On to false
Edit Remove	Yes	FAN_OFF_LAN4	Temp_LAN4 Temperature < 23.0 °C	Set Fan_LAN4 Status to Off
Edit Remove	Yes	FAN_ON_LAN5	Match all: • Fmonitor_LAN5 Fire Detected is false • Temp_LAN5 Temperature > 23.0 °C	Set Fan_LAN5 Status to High
Edit Remove	Yes	FAN_OFF_LAN5	Temp_LAN5 Temperature < 23.0 °C	Set Fan_LAN5 Status to Off
Edit Remove	Yes	TEMP_HIGH_ON_LAN3	Match all: • Temp_LAN3 Temperature > 25.0 °C • Fmonitor_LAN3 Fire Detected is false	Set Window_LAN3 On to false Set Cond_LAN3 On to true
Edit Remove	Yes	TEMP_HIGH_OFF_LAN3	Match all: • Fmonitor_LAN3 Fire Detected is false • Temp_LAN3 Temperature < 25.0 °C	Set Cond_LAN3 On to false
Edit Remove	Yes	TEMP_LOW_ON_LAN3	Match all: • Temp_LAN3 Temperature < 20.0 °C • Fmonitor_LAN3 Fire Detected is false	Set Hum_LAN3 Status to true Set Furnace_LAN3 On to true Set Window_LAN3 On to false
Edit Remove	Yes	TEMP_LOW_OFF_LAN3	Temp_LAN3 Temperature > 20.0 °C	Set Hum_LAN3 Status to false Set Furnace_LAN3 On to false
Edit Remove	Yes	Siren_ON_LAN1-2-3-5	Match any: • Fmonitor_LAN5 Fire Detected is true • Fmonitor_LAN3 Fire Detected is true • Fmonitor_LAN1 Fire Detected is true • Fmonitor_LAN2 Fire Detected is true	Set Siren_LAN5 On to true Set Siren_LAN1 On to true Set Siren_LAN3 On to true Set Siren_LAN2 On to true
Edit Remove	Yes	Siren_OFF_LAN1-2-3-5	Match all: • Fmonitor_LAN5 Fire Detected is false • Fmonitor_LAN3 Fire Detected is false • Fmonitor_LAN2 Fire Detected is false • Fmonitor_LAN1 Fire Detected is false	Set Siren_LAN5 On to false Set Siren_LAN1 On to false Set Siren_LAN3 On to false Set Siren_LAN2 On to false
Edit Remove	Yes	Siren_ON_LAN4	Fmonitor_LAN4 Fire Detected is true	Set Siren_LAN4 On to true
Edit Remove	Yes	Siren_OFF_LAN4	Fmonitor_LAN4 Fire Detected is true	Set Siren_LAN4 On to false
Edit Remove	Yes	Window_open_LAN1	Match all: • Temp_LAN1 Temperature is between 20.0 °C and 23.0 °C • Fmonitor_LAN1 Fire Detected is false	Set Window_LAN1 On to true
Edit Remove	Yes	Window_open_LAN2	Match all: • Temp_LAN2 Temperature is between 20.0 °C and 23.0 °C • Fmonitor_LAN2 Fire Detected is false	Set Window_LAN2 On to true
Edit Remove	Yes	Window_open_LAN3	Match all: • Temp_LAN3 Temperature is between 20.0 °C and 23.0 °C • Fmonitor_LAN3 Fire Detected is false	Set Window_LAN3 On to true
Edit Remove	Yes	Window_open_LAN4	Match all: • Temp_LAN4 Temperature is between 20.0 °C and 23.0 °C • Fmonitor_LAN4 Fire Detected is false	Set Window_LAN4 On to true
Edit Remove	Yes	Window_open_LAN5	Match all: • Temp_LAN5 Temperature is between 20.0 °C and 23.0 °C • Fmonitor_LAN5 Fire Detected is false	Set Window_LAN5 On to true
Edit Remove	Yes	Window_close_LAN1	Temp_LAN1 Temperature < 20.0 °C	Set Window_LAN1 On to false
Edit Remove	Yes	Window_close_LAN2	Temp_LAN2 Temperature < 20.0 °C	Set Window_LAN2 On to false
Edit Remove	Yes	Window_close_LAN3	Temp_LAN3 Temperature < 20.0 °C	Set Window_LAN3 On to false
Edit Remove	Yes	Window_close_LAN4	Temp_LAN4 Temperature < 20.0 °C	Set Window_LAN4 On to false
Edit Remove	Yes	Window_close_LAN5	Temp_LAN5 Temperature < 20.0 °C	Set Window_LAN5 On to false

Add

Рисунок 4.7 – Сценарії мережі

4.3 Перевірка роботи компонента Системи

Для перевірки роботи налаштовано середовище Cisco Packet Tracer для періодичного змінення температури та додано елемент який симулює вогонь.

Перевірка системи при наявності валідної ключ картки на прикладі LAN4(рис. 4.8)

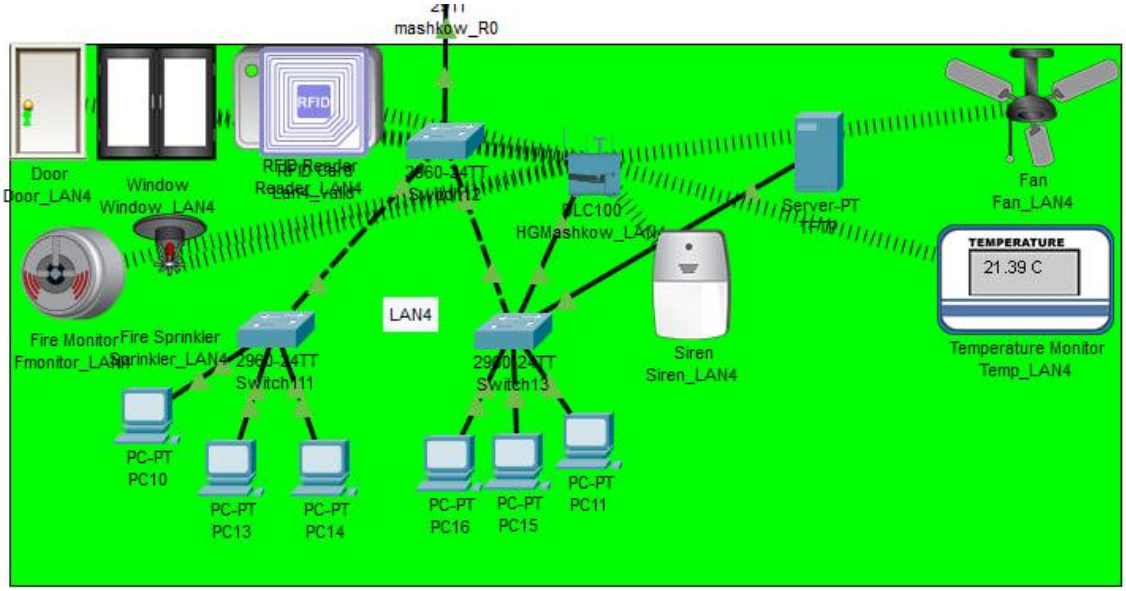

Рисунок 4.8 – Наявність валідної ключ карти

Рисунок 4.9 – Поведінка при невалідній картці

Перевірка системи при температурі від 20 до 23 градусів на прикладі системи з LAN4(рис. 4.10)

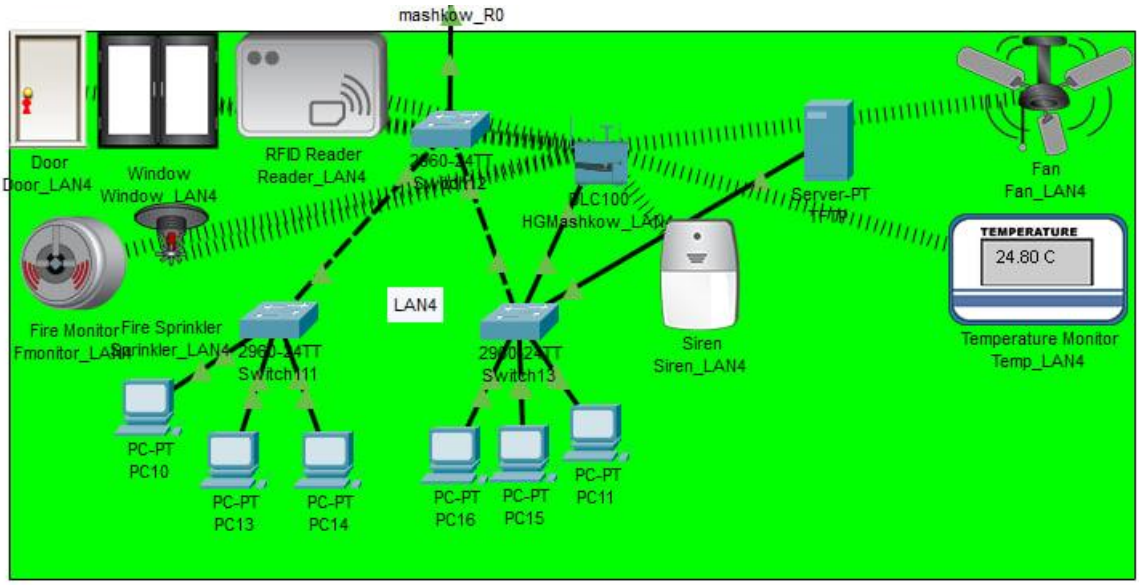

Рисунок 4.10 – Поведінка системи при температурі від 20 до 23 градусів

Перевірка системи при температурі від 23 градусів на прикладі системи з LAN4(рис. 4.11)

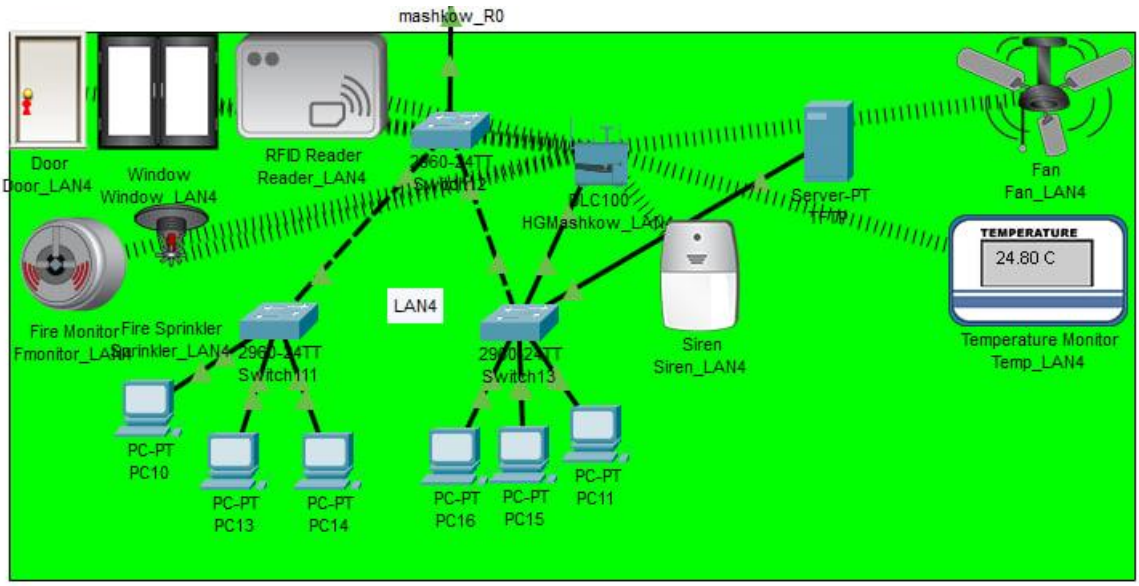

Рисунок 4.11 – системи при температурі від 23 градусів

Наступним етапом є тестування LAN3, це мережа з повним кліматичним контролем. Перевірка системи при температурі 21(рис. 4.12), температурі від 23(рис. 4.13) та температурі до 19 градусів (рис. 4.14).

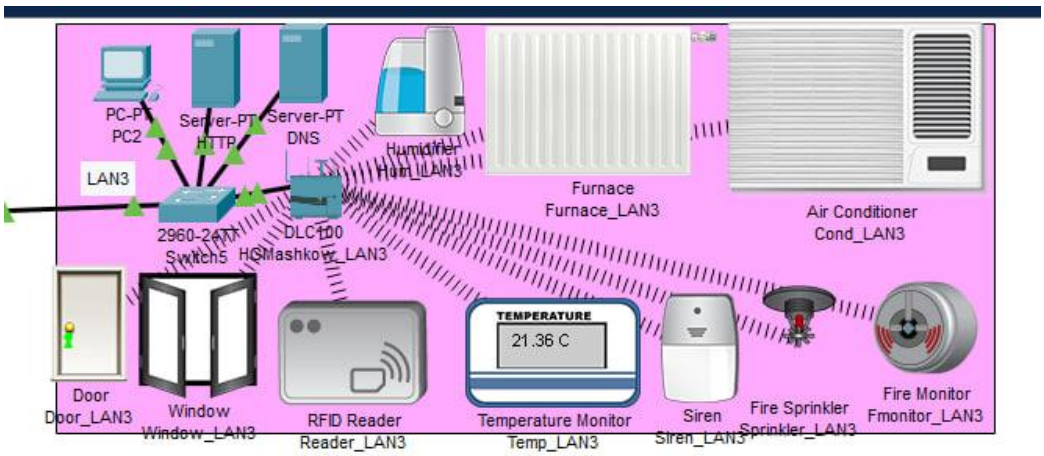

Рисунок 4.12 – Поведінка системи при при температурі 21

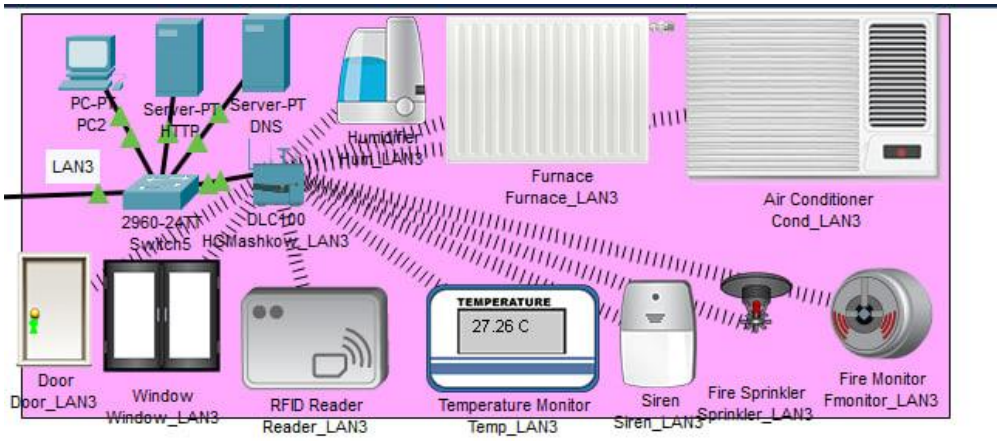

Рисунок 4.13 – Поведінка системи при температурі від 23

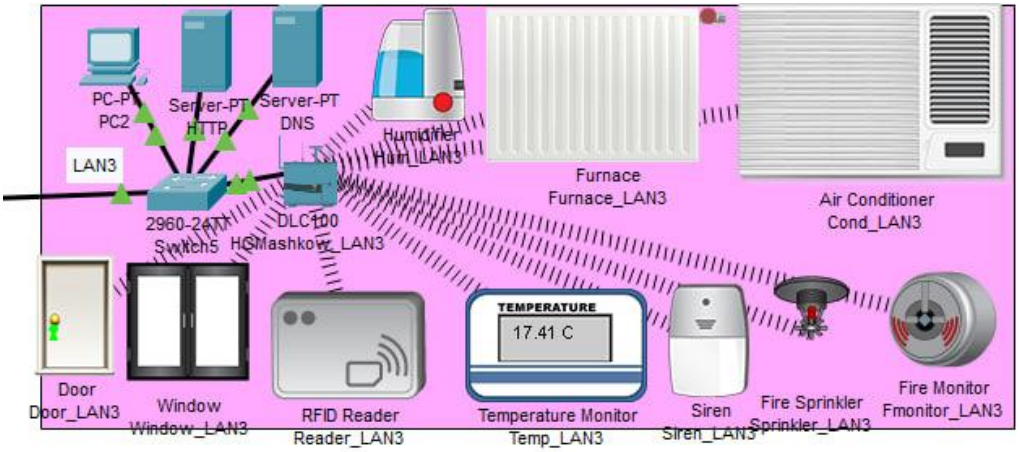

Рисунок 4.14 – Поведінка системи при та температурі до 19 градусів

Перевірка системи пожар-тушіння наведена на рисунках 4.15-18.

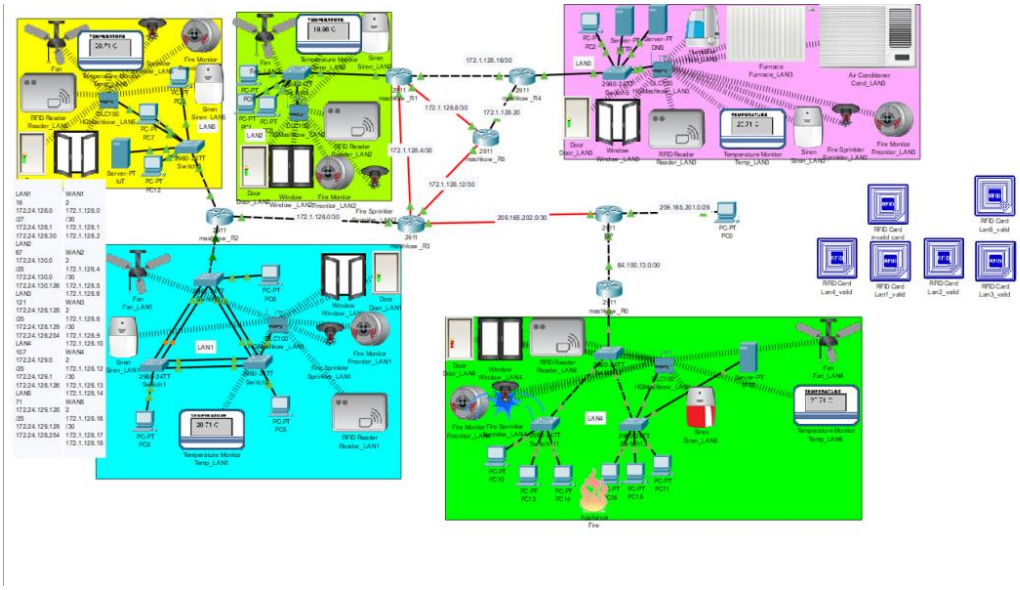

Рисунок 4.15 – Наявність місця займання у віддаленій мережі

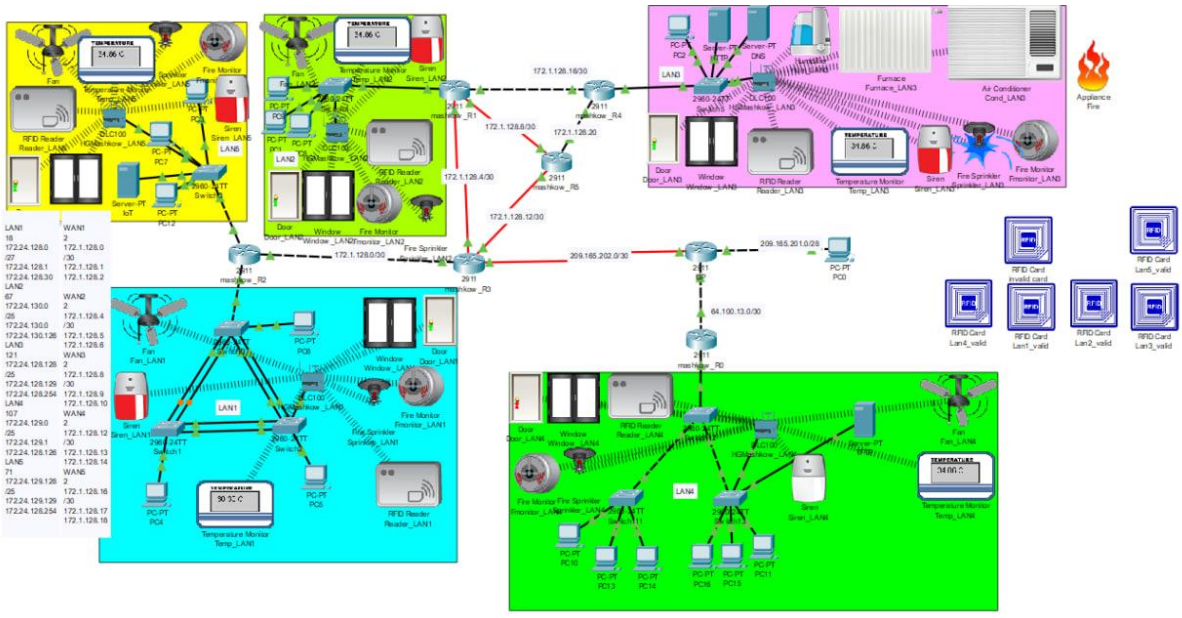

Рисунок 4.16 – Наявність місця займання у підмережі LAN3

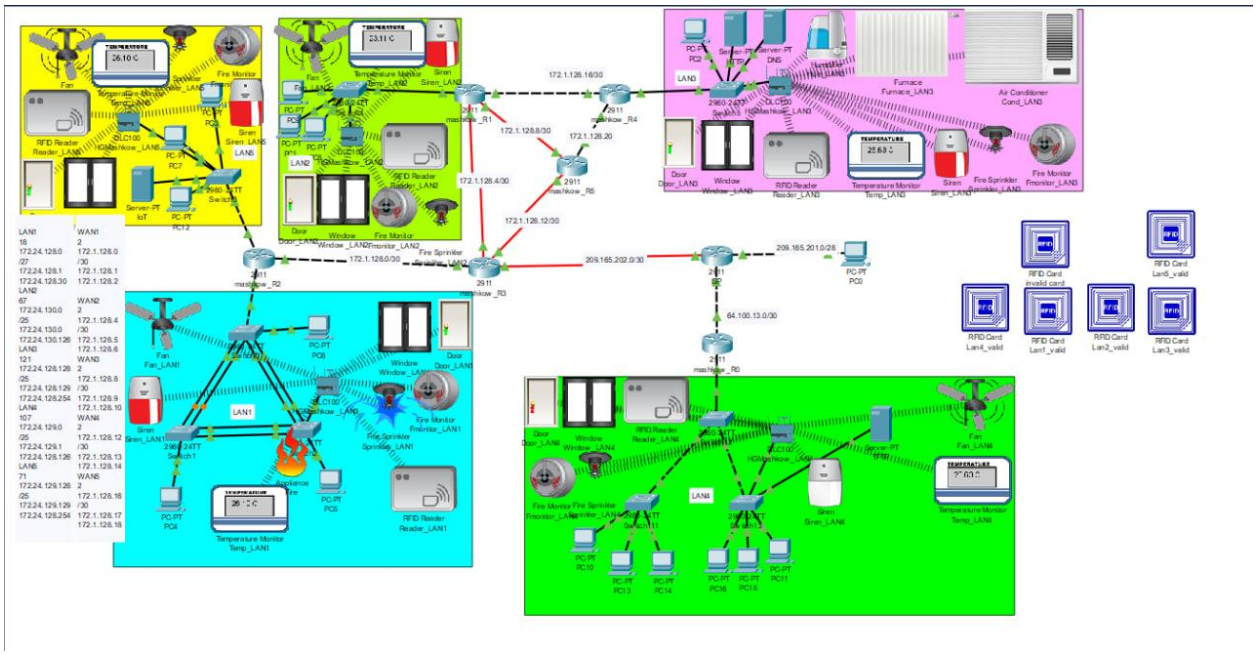

Рисунок 4.17 – Наявність місця займання у підмережі LAN1

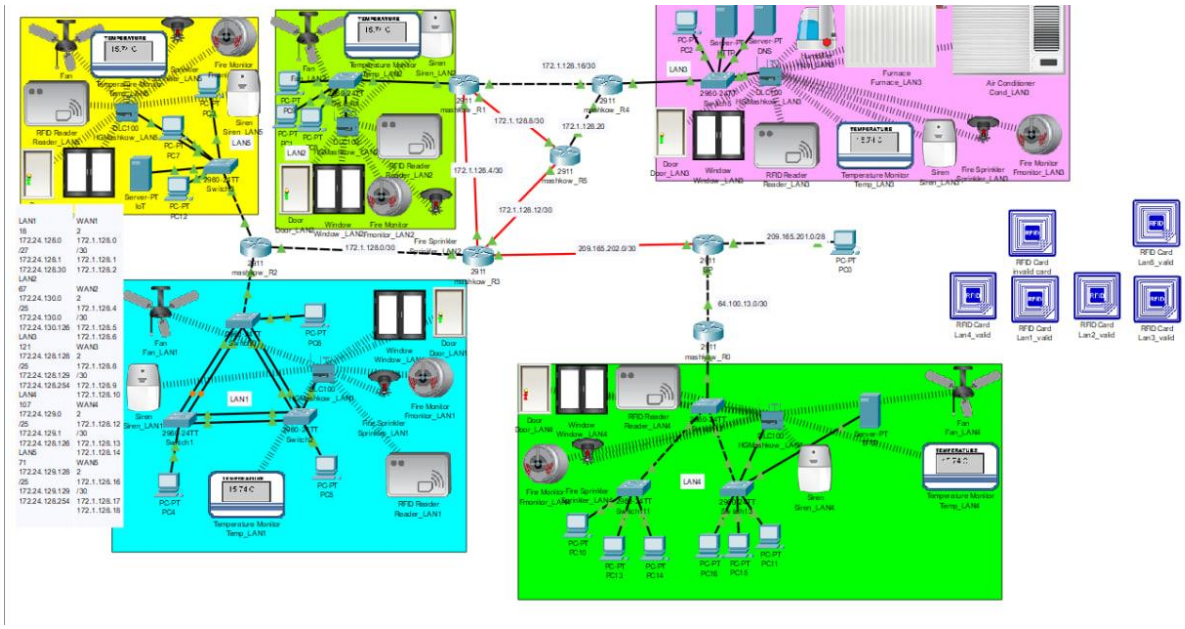

Рисунок 4.18 – Система у стані спокою

ВИСНОВКИ

У рамках кваліфікаційної роботи, присвяченої побудові та налаштуванню корпоративної мережі для ТОВ «Sentosa», було досягнуто низки значущих результатів, що відповідають сучасному рівню наукових і технічних знань у галузі інформаційних технологій та комп'ютерної інженерії. Розроблена мережева архітектура забезпечує високу надійність, безпеку та ефективність обміну даними внутрішньої корпоративної інфраструктури.

Основні галузі використання результатів роботи охоплюють не лише внутрішнє використання компанією «Sentosa», але й можуть бути адаптовані для впровадження в інших організаціях, що потребують оптимізації мережевих ресурсів та забезпечення цифрової безпеки.

У мережі реалізовано детально продумані сценарії для автоматизації функцій безпеки та комфорту. Для кожної підмережі створено три основних сценарії керування доступом до приміщень, засновані на статусі рідера, які забезпечують автоматичне відчинення та зачинення дверей відповідно до валідності доступу. Сценарії для вікон і стельових вентиляторів використовуються для регулювання температури і провітрювання приміщень, залежно від змін температурних умов. Додатково, для підмережі LAN3 розроблено спеціалізовану систему клімат-контролю, що реагує на більш широкий спектр температурних змін, включаючи активацію зволожувача повітря та систем кондиціонування. У випадку виявлення вогню, активується сирена і місцеве пожежогасіння, що гарантує швидку реакцію на пожежні інциденти. Сценарії для віддаленої мережі розроблені таким чином, щоб вони були ізольовані від основної мережі, забезпечуючи незалежність і безпеку керування для кожної зони без перехресного впливу.

Наукова та науково-технічна значущість даної роботи полягає у розробці та впровадженні передових підходів до адміністрування корпоративних мереж, використанні новітніх технологій для моніторингу та управління мережевими

потоками, що сприяє підвищенню загальної ефективності інформаційної системи.

Враховуючи динамічний розвиток інформаційних технологій, доцільно продовжувати дослідження в даній області, особливо в контексті розвитку методів штучного інтелекту та машинного навчання для автоматизації процесів моніторингу та управління мережевою інфраструктурою. Також перспективним є подальше вдосконалення механізмів кібербезпеки із застосуванням сучасних криптографічних методів захисту даних.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. «Sentosa» сайт компанії [Електронний ресурс] – Режим доступу до ресурсу: http://sentosa.com (дата звернення 10.05.2024р.)

2. 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.

3. Структура управління організацією. Лекція з навчальної дисципліни «Менеджмент організацій» Для студентів спеціальності 073 «Менеджмент» / Павленчик А. О. – Львівський державний університет фізичної культури імені Івана Боберського, 2020. – 16 с.

4. Цифрова трансформація: від стратегії до реалізації / Юрій Груша. – Львів: ЛНУ ім. Івана Франка, 2022. – 210 с.

5. Введення в інтернет речей / Сергій Кіріченко. – Харків: ХНУРЕ, 2021. – 165 с.

6. Data Communications and Networking / Behrouz A. Forouzan. – New York: McGraw-Hill Education, 2022. – 912 с.

7. Computer Networks: A Systems Approach / Larry L. Peterson, Bruce S. Davie. – Cambridge, MA: Morgan Kaufmann, 2021. – 960 с.

8. Modern Operating Systems / Andrew S. Tanenbaum, Herbert Bos. – Upper Saddle River, NJ: Pearson, 2021. – 1136 с.

9. Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare / Thomas A. Johnson. – Boca Raton, FL: CRC Press, 2021. – 340 с.

10. Principles of Computer Security: CompTIA Security+ and Beyond / Wm. Arthur Conklin, Greg White, Dwayne Williams, Roger L. Davis, Chuck Cothren. – New York: McGraw-Hill Education, 2022. – 768 с.

Додаток А

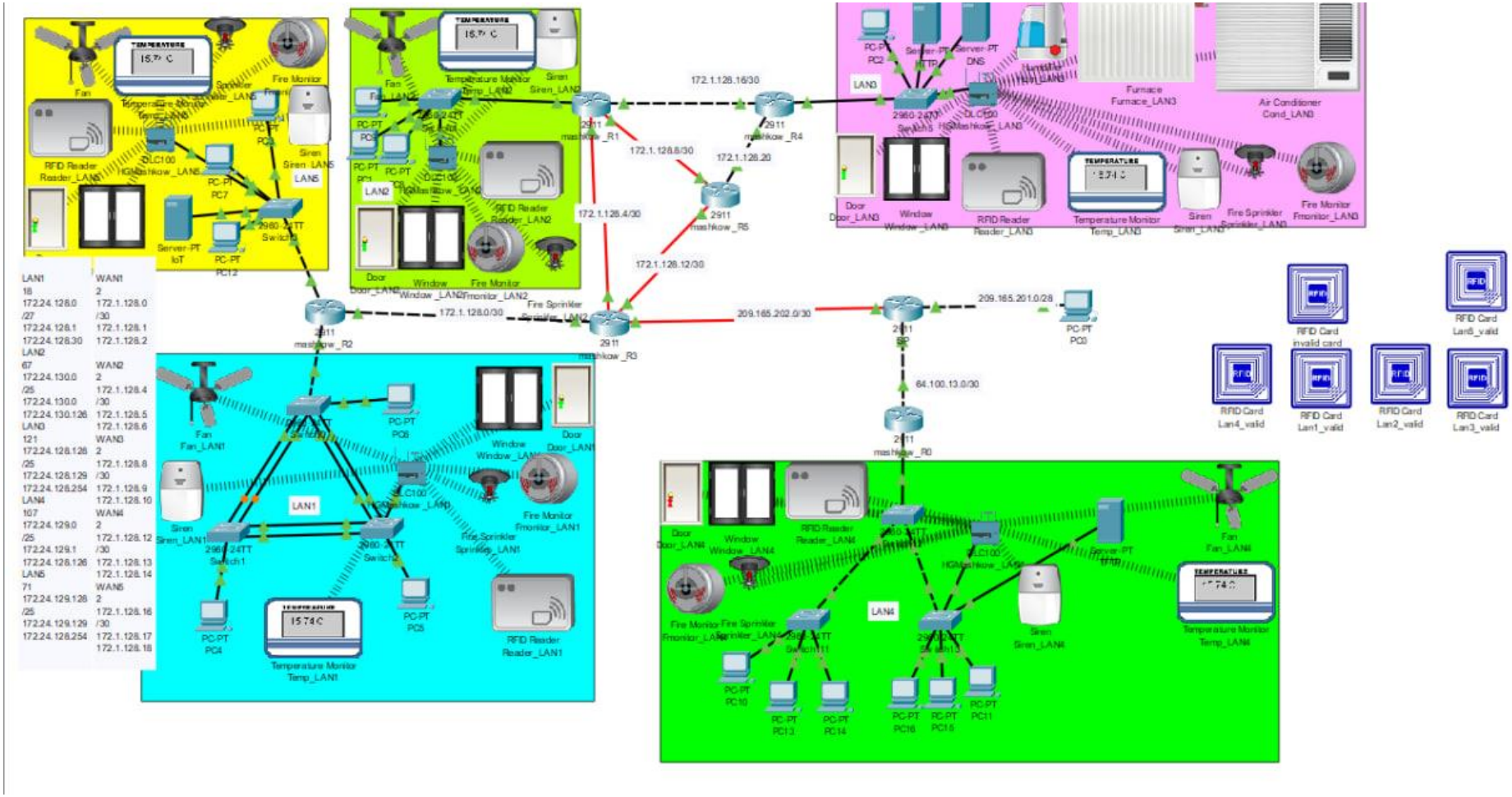

Рисунок ДА.1 – Загальна архітектура мережі

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

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ НАЛАШТУВАННЯ МЕРЕЖІ КОМП’ЮТЕРНОЇ СИСТЕМИ

Текст програми

804.02070743.24004-01 12 01

Листів 16

2024

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.

ЗМІСТ

1. mashkow_R1

```
mashkow_R1#show run
Current configuration : 2251 bytes
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
hostname mashkow_R1
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
ip dhcp excluded-address 172.24.128.33 172.24.128.35
ip dhcp excluded-address 172.24.128.127
ip dhcp excluded-address 172.24.128.128
ip dhcp pool LAN-2
network 172.24.128.0 255.255.255.128
default-router 172.24.128.33
dns-server 172.24.128.250
aaa new-model
aaa authentication login console group radius local
aaa authentication login default local
no ip cef
no ipv6 cef
username 123191_mashkow_R1 password 7 082048430017061E010803
username mashkow12321ck1 password 7 082048430017544541
license udi pid CISCO2911/K9 sn FTX1524W772-
ip domain-name mashkow_R1
spanning-tree mode pvst
interface GigabitEthernet0/0
ip address 172.24.128.33 255.255.255.128
duplex auto
speed auto
```

```
interface GigabitEthernet0/1
ip address 172.1.128.17 255.255.255.252
duplex auto
speed auto
!
interface GigabitEthernet0/2
no ip address
duplex auto
speed auto
!
interface Serial0/3/0
ip address 172.1.128.6 255.255.255.252
!
interface Serial0/3/1
ip address 172.1.128.9 255.255.255.252
!
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 GigabitEthernet0/2
no passive-interface Serial0/3/0
no passive-interface Serial0/3/1
auto-cost reference-bandwidth 1000
network 172.24.128.0 0.0.0.127 area 0
```

```
network 172.1.128.16 0.0.0.3 area 0
network 172.1.128.4 0.0.0.3 area 0
network 172.1.128.8 0.0.0.3 area 0
!
ip classless
!
ip flow-export version 9
banner motd ^Cmashkow_R1^C
radius server host
address ipv4 172.24.128.251 auth-port 1645
key radius123
radius server 172.24.128.251
address ipv4 172.24.128.251 auth-port 1645
key radius123
line con 0
password 7 0822455D0A16
login authentication console
!
line aux 0
!
line vty 0 4
password 7 0822455D0A16
login authentication default
transport input ssh
line vty 5 15
password 7 0822455D0A16
login authentication default
transport input ssh
end
```

2. mashkow_R3

```
mashkow_R3#show run
Current configuration : 2937 bytes
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname mashkow_R3
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
aaa new-model
aaa authentication login console group radius local
aaa authentication login default local
no ip cef
no ipv6 cef
username 123191_mashkow_R3 password 7 082048430017061E010803
username mashkow12321ck1 password 7 082048430017544541
license udi pid CISCO2911/K9 sn FTX152413GN-
ip domain-name mashkow_R3
spanning-tree mode pvst
interface GigabitEthernet0/0
ip address 172.1.128.2 255.255.255.252
ip nat inside
duplex auto
speed auto
!
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
```

```
!
interface GigabitEthernet0/2
no ip address
duplex auto
speed auto
!
interface Serial0/2/0
ip address 209.165.202.1 255.255.255.252
ip nat outside
!
interface Serial0/2/1
no ip address
clock rate 128000
!
interface Serial0/3/0
ip address 172.1.128.14 255.255.255.252
ip nat inside
!
interface Serial0/3/1
ip address 172.1.128.5 255.255.255.252
ip nat inside
clock rate 128000
!
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 Serial0/2/0
no passive-interface Serial0/3/0
no passive-interface Serial0/3/1
auto-cost reference-bandwidth 1000
network 172.1.128.0 0.0.0.3 area 0
network 172.1.128.12 0.0.0.3 area 0
network 172.1.128.4 0.0.0.3 area 0
network 209.165.202.0 0.0.0.3 area 0
!
ip nat pool Internet 209.165.200.5 209.165.200.30 netmask 255.255.255.224
ip nat inside source list NAT11 pool Internet
ip nat inside source static 172.24.128.251 209.165.200.4
ip nat inside source static 172.24.128.250 209.165.200.3
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 NAT11
deny ip 172.24.128.0 0.0.0.31 172.24.129.0 0.0.0.127
deny ip 172.24.128.0 0.0.0.127 172.24.129.0 0.0.0.127
deny ip 172.24.128.128 0.0.0.127 172.24.129.0 0.0.0.127
deny ip 172.24.129.128 0.0.0.127 172.24.129.0 0.0.0.127
deny ip 172.1.128.0 0.0.0.255 172.24.129.0 0.0.0.127
permit ip 172.24.128.0 0.0.0.31 any
permit ip 172.24.128.0 0.0.0.127 any
permit ip 172.24.128.128 0.0.0.127 any
```

```
permit ip 172.24.129.128 0.0.0.127 any
permit ip 172.1.128.0 0.0.0.255 any
!
banner motd ^Cmashkow_R3^C
!
radius server host
address ipv4 172.24.128.251 auth-port 1645
key radius123
radius server 172.24.128.251
address ipv4 172.24.128.251 auth-port 1645
key radius123
line con 0
password 7 0822455D0A16
login authentication console
!
line aux 0
!
line vty 0 4
password 7 0822455D0A16
login authentication default
transport input ssh
line vty 5 15
password 7 0822455D0A16
login authentication default
transport input ssh
end
```

3. mashkow_R0

```
Current configuration : 3192 bytes
!
```

```
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname mashkow_R0
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
ip dhcp excluded-address 172.24.129.1 172.24.129.5
ip dhcp excluded-address 172.24.129.126
ip dhcp excluded-address 172.24.129.127
ip dhcp excluded-address 172.24.129.1 172.24.129.10
ip dhcp excluded-address 172.24.129.5
!
ip dhcp pool LAN4-VLAN10
network 172.24.129.0 255.255.255.224
default-router 172.24.129.1
dns-server 172.24.128.250
ip dhcp pool LAN4-VLAN20
network 172.24.129.32 255.255.255.224
default-router 172.24.129.33
dns-server 172.24.128.250
ip dhcp pool LAN4-VLAN30
network 172.24.129.64 255.255.255.224
default-router 172.24.129.65
dns-server 172.24.128.250
!
!
aaa new-model
!
aaa authentication login console group radius local
```

```
aaa authentication login default local
ip cef
no ipv6 cef
!
!
!
username 123191_mashkow_R0 password 7 082048430017061E010803
username mashkow12321ck1 password 7 082048430017544541
!
!
license udi pid CISCO2911/K9 sn FTX1524MF8K-
license boot module c2900 technology-package securityk9
ip domain-name mashkow_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
no ip address
duplex auto
speed auto
!
interface GigabitEthernet0/1.10
encapsulation dot1Q 10
ip address 172.24.129.1 255.255.255.224
!
interface GigabitEthernet0/1.20
encapsulation dot1Q 20
```

```
ip address 172.24.129.33 255.255.255.224
!
interface GigabitEthernet0/1.30
encapsulation dot1Q 30
ip address 172.24.129.65 255.255.255.224
!
interface GigabitEthernet0/1.99
encapsulation dot1Q 99
ip address 172.24.129.97 255.255.255.240
!
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
no passive-interface GigabitEthernet0/1.10
no passive-interface GigabitEthernet0/1.20
no passive-interface GigabitEthernet0/1.30
no passive-interface GigabitEthernet0/1.99
auto-cost reference-bandwidth 1000
network 172.24.129.0 0.0.0.127 area 0
```

```
network 64.100.13.0 0.0.0.3 area 0
!
ip classless
!
ip flow-export version 9
!
!
ip access-list extended VPN1
permit ip 172.24.129.0 0.0.0.127 172.24.128.0 0.0.0.127
permit ip 172.24.129.0 0.0.0.127 172.24.128.0 0.0.0.31
permit ip 172.24.129.0 0.0.0.127 172.24.128.128 0.0.0.127
permit ip 172.24.129.0 0.0.0.127 172.24.129.128 0.0.0.127
permit ip 172.24.129.0 0.0.0.127 172.1.128.0 0.0.0.255
!
banner motd ^Cmashkow_R0^C
!
radius server host
address ipv4 172.24.128.251 auth-port 1645
key radius123
radius server 172.24.128.251
address ipv4 172.24.128.251 auth-port 1645
key radius123
line con 0
password 7 0822455D0A16
login authentication console
!
line aux 0
!
line vty 0 4
password 7 0822455D0A16
```

login authentication default
transport input ssh
line vty 5 15
password 7 0822455D0A16
login authentication default
transport input ssh
end

4.switch12

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.switch0

```
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
```