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 Сидоренка Дмитра Ігоровича
(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 ТОВ ВФ «ЛІБЕРТА» з детальним опрацюван--ням, налаштування та безпеки корпоративної мережі»
(назва за наказом ректора)

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	проф. Цвіркун Л.І.			
спеціальної частини	проф. Цвіркун Л.І.			
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 Сидоренка Д.І. **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 ТОВ ВФ «ЛІБЕРТА» з детальним опрацюван--ням, налаштування 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 кваліфікаційної роботи	05.05.2024
Розробка апаратної частини	Розробити вимоги до функцій, виконуваними системою корпоративної мережі	12.05.2024
Розробка корпоративної мереж	Побудувати в Packet Tracer модель корпоративної мережі компанії, виконати налаштування та перевірку роботи системи	26.05.2024
Розробка компонента системи	Розробити автоматизації клімату, систему доступу та систему оповіщення при пожежі	09.06.2024

Завдання видано проф. Гнатушенко В.В
(підпис керівника) (прізвище, ініціали)

Дата видачі 06.02.2024

Дата подання до екзаменаційної комісії 18.06.2024

Прийнято до виконання

(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 86 с., 45 рис., 6 табл., 1 додатки, 11 джерел.

Ключові слова: автоматизація, безпека мережі, інтернет речей, кліматконтроль, корпоративна мережа, маршрутизація, налаштування мережі, впровадження, статистичні маршрути, комутація.

Об’єкт розробки: комп'ютерна система корпоративної мережі “LIBERTA”.

Мета роботи: розробка, конфігурація та забезпечення безпеки корпоративної мережі з інтеграцією IoT-системи для контролю клімату та автоматизації пожежогасіння.

Здійснено: розробка і налаштування компонентів IoT-системи для контролю клімату та автоматизованого пожежогасіння, конфігурація маршрутизаторів і комутаторів, налаштування основних мережевих протоколів та забезпечення безпеки мережі.

Об’єктом розробки є комп'ютерна система корпоративної мережі TOV VF “LIBERTA”. Ця мережа включає IoT-систему для контролю клімату та автоматизації процесів пожежогасіння в підмережах з серверним обладнанням.

Метою роботи є створення надійної і безпечної корпоративної мережі з інтеграцією сучасних IoT-технологій для автоматичного контролю клімату та забезпечення пожежної безпеки.

Для досягнення мети були використані такі методи дослідження: аналіз вимог до мережі, моделювання мережевих топологій у Cisco Packet Tracer, тестування налаштувань у лабораторних умовах. Використана апаратура включає маршрутизатори та комутатори Cisco, а також різноманітні датчики IoT для контролю клімату і задимленості.

Результатом роботи стало створення ефективної корпоративної мережі, яка включає IoT-систему для автоматизації клімат-контролю і пожежогасіння. Новизна полягає у інтеграції IoT-рішень в існуючу мережеву інфраструктуру з використанням сучасних протоколів безпеки та передачі даних.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

AAA – Authentication, Authorization, and Accounting (Аутентифікація, авторизація та облік)

AES – Advanced Encryption Standard (Стандарт шифрування)

DHCP – Dynamic Host Configuration Protocol (Протокол динамічної конфігурації хостів)

EtherChannel – Технологія об'єднання декількох фізичних каналів зв'язку в один логічний

IP – Internet Protocol (Інтернет-протокол)

IoT – Internet of Things (Інтернет речей)

NAT – Network Address Translation (Трансляція мережевих адрес)

OSPF – Open Shortest Path First (Протокол маршрутизації)

SSID – Service Set Identifier (Ідентифікатор набору послуг)

VLAN – Virtual Local Area Network (Віртуальна локальна мережа)

VPN – Virtual Private Network (Віртуальна приватна мережа)

WPA2-PSK – Wi-Fi Protected Access 2 - Pre-Shared Key (Захищений доступ до Wi-Fi 2 з попередньо спільним ключем)

ВСТУП

У сучасному світі інформаційних технологій комп'ютерні системи та мережеві інфраструктури відіграють вирішальну роль у функціонуванні та розвитку підприємств. Компанія ТОВ ВФ "ЛІБЕРТА", яка активно розвивається на ринку, визначає новітні технології як основу своєї конкурентоспроможності та ефективності. З огляду на це, критично важливим є створення та підтримка високонадійної та безпечної корпоративної мережі, яка б забезпечувала стабільність роботи усіх відділів компанії.

Робота присвячена детальному аналізу та розробці комп'ютерної системи ТОВ ВФ "ЛІБЕРТА". Основна увага приділяється трьом ключовим аспектам: конструкції мережі, її конфігурації та аспектам мережевої безпеки. Ціль роботи полягає у створенні вичерпного проєкту, який би охоплював всі необхідні компоненти для забезпечення ефективності та безпеки інформаційних потоків у корпоративному середовищі.

Для досягнення цієї мети будуть використані наступні методи: визначення вимог до мережі, проектування мережевої архітектури, вибір обладнання, розробка політик безпеки та їх імплементація. Такий підхід дозволить не тільки оптимізувати внутрішні процеси компанії, але й мінімізувати потенційні ризики, пов'язані з кіберзагрозами та збоями в системі.

1 СТАН ПИТАННЯ І ПОСТАНОВКА ЗАВДАННЯ

1.1 Стисла характеристика галузі та умов застосування виробу

Компанія ТОВ ВФ "ЛІБЕРТА" активно функціонує в галузі виробництва та оброблення інших скляних виробів, у тому числі технічних, де використання передових технологій і комп'ютерних систем є ключовим фактором успіху. Основні вимоги до ІТ-інфраструктури у цій галузі включають високу надійність, оперативність обробки даних та захист інформації від несанкціонованого доступу. З огляду на це, комп’ютерна система, що проектується, повинна відповідати наступним умовам:

– Висока доступність: Система повинна забезпечувати стале та надійне з’єднання для усіх відділів компанії, мінімізуючи час простою та збої в роботі.

– Безпека: З огляду на значну кількість конфіденційних даних, які обробляються в рамках діяльності компанії у виробництві та обробці скла, система має включати сучасні засоби шифрування, аутентифікації та захисту від вірусів та інших кіберзагроз.

– Масштабованість: У випадку розширення діяльності компанії, система повинна бути готова до легкого додавання нових робочих станцій та відділів без зниження загальної продуктивності мережі.

– Інтегрованість: Комп’ютерна система має ефективно інтегруватися з існуючими програмними та апаратними рішеннями, які вже використовуються у компанії для контролю якості, обробки та логістики скляних виробів.

– Відповідність законодавчим вимогам: Система повинна відповідати всім національним та міжнародним законодавчим стандартам щодо обробки та зберігання даних.

Для задоволення цих умов, проектування комп’ютерної системи вимагає детального аналізу поточних потреб компанії, а також антиципації майбутніх розширень та технологічних оновлень.

1.2 Характеристика підприємства та умов застосування КС

Об’єкт впровадження – ТОВ ВФ "ЛІБЕРТА"

ТОВ ВФ "ЛІБЕРТА" є ключовим гравцем у галузі виробництва та оброблення скляних виробів, зокрема технічних скловиробів. Компанія відома своєю відданістю інноваціям, високим стандартам якості та відповідальності перед клієнтами. З метою не тільки задовольнити, а й перевершити очікування клієнтів, "ЛІБЕРТА" неперервно впроваджує передові технології в процеси виробництва та контролю якості.

Заснована з ідеєю постійного розвитку та удосконалення, "ЛІБЕРТА" слідує філософії, що у всіх аспектах діяльності, від проектування продукції до процесів обслуговування клієнтів, має бути присутня відданість якості та інноваціям. Такий підхід втілюється завдяки керівництву компанії, де кожен член команди є професіоналом, зосередженим на підвищенні ефективності послуг та розширенні бізнес-горизонтів "ЛІБЕРТА".

1.3 Принципи, технічні способи та математичні методи інформаційного забезпечення підприємства

ТОВ ВФ "ЛІБЕРТА" розташовано в центральному зоні міста Дніпро, 25 ул. Святослава Храброго.

Розташування у промисловому районі забезпечує легкий доступ до транспортних.

Комплекс складається з головного адміністративного будинку та складського приміщення у будівлі.

Топографічна схема розміщення структурних підрозділів показана на рис. 1.2

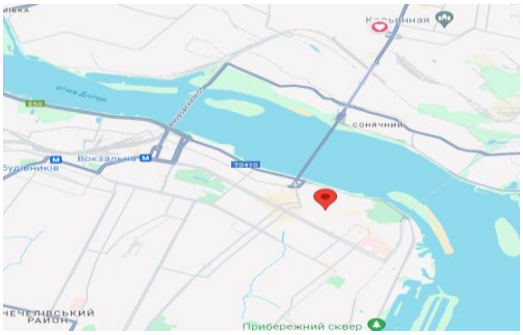

Рисунок 1.1 – Топографічна схема розміщення структурних підрозділів ТОВ «Sentosa»

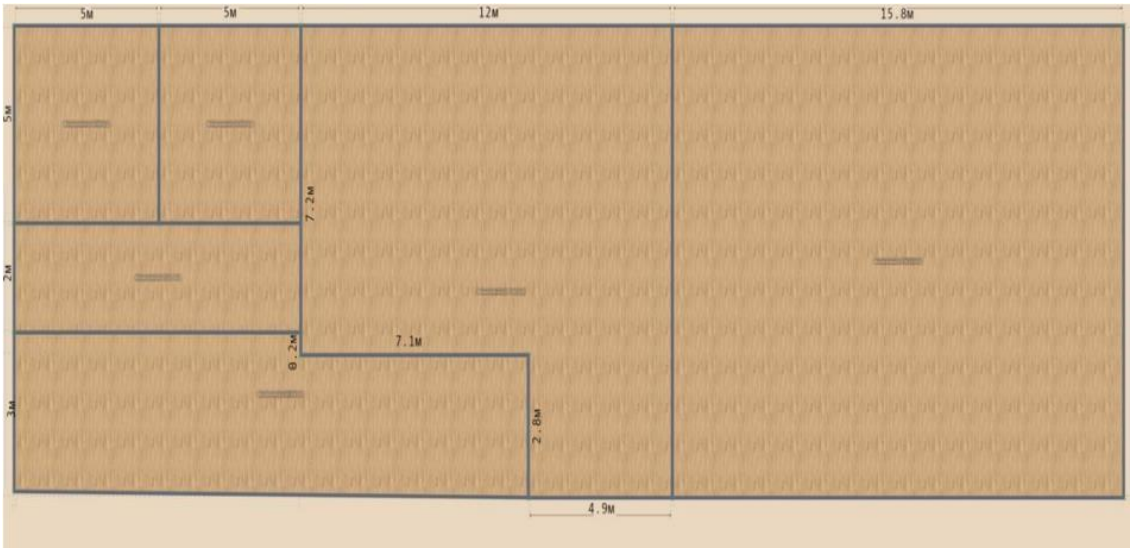

Рисунок 1.2 – Структурна схема розміщення підрозділів у будівлі

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

Огляд існуючих інженерних рішень у галузі комп'ютерних систем може допомогти визначити напрямки розв'язання поставлених завдань. У сучасних умовах швидкого розвитку технологій інформаційних систем, існують різноманітні підходи та рішення, що можуть бути застосовані.

Хмарні технології можуть забезпечити гнучкість та доступність у роботі мережі, використовуючи хмарні сервіси для зберігання даних та виконання обчислень. Це дозволяє зосередитися на бізнес-процесах, позбавляючи від необхідності обслуговування великої кількості обладнання.

Інтернет речей (IoT) дозволяє підключати до мережі різноманітні пристрої, що може бути корисним для збору даних та автоматизації процесів у підприємстві. Однак, це також створює нові виклики з точки зору безпеки мережі та обробки великого обсягу даних.

Ще одним напрямком розв'язання завдань є використання віртуалізації та контейнеризації. Ці технології дозволяють ефективно використовувати ресурси серверів, розгортати та масштабувати програмне забезпечення швидко та

ефективно. Вони також сприяють підвищенню надійності системи та забезпеченню швидкого відновлення у разі виникнення проблем.

Іншим важливим аспектом є застосування технологій шифрування та ідентифікації для забезпечення безпеки мережі. Використання сучасних методів шифрування даних та двофакторної аутентифікації може запобігти несанкціонованому доступу до інформації та захистити її від витоку.

Також варто розглянути впровадження систем моніторингу та аналізу мережі. Ці системи дозволяють вчасно виявляти та реагувати на загрози безпеки, а також оптимізувати роботу мережі для підвищення її ефективності.

Ці напрямки можуть бути використані для розробки та впровадження високонадійних та безпечних комп'ютерних систем у компанії.

1.5 Розробка схеми організаційної структури підприємства

Керівництво "ЛІБЕРТА" встановлює стратегічні цілі, що відображають прагнення до лідерства у галузі та зміцнення конкурентних позицій на ринку. Організаційна структура компанії розроблена таким чином, що забезпечує ефективну взаємодію між відділами:

– Відділ продажів та маркетингу: Займається просуванням продукції та послуг компанії, залученням нових клієнтів та підтримкою існуючих відносин.

– Відділ обслуговування клієнтів: Забезпечує підтримку клієнтів, відповідає на запити, розв'язує проблеми та забезпечує задоволеність клієнтів.

– Фінансовий відділ: Відповідає за фінансове планування, облік та аналіз фінансової діяльності компанії.

– Операційний відділ: Керує повсякденною діяльністю компанії, зокрема виробництвом, постачанням та логістикою.

– Відділ розвитку та інновацій: Займається стратегічним плануванням, розробкою нових продуктів та впровадженням інновацій.

Високий пріоритет в "ЛІБЕРТА" віддається 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 "ЛІБЕРТА" займати лідируючі позиції на ринку та пропонувати своїм клієнтам виняткові вироби зі скла.

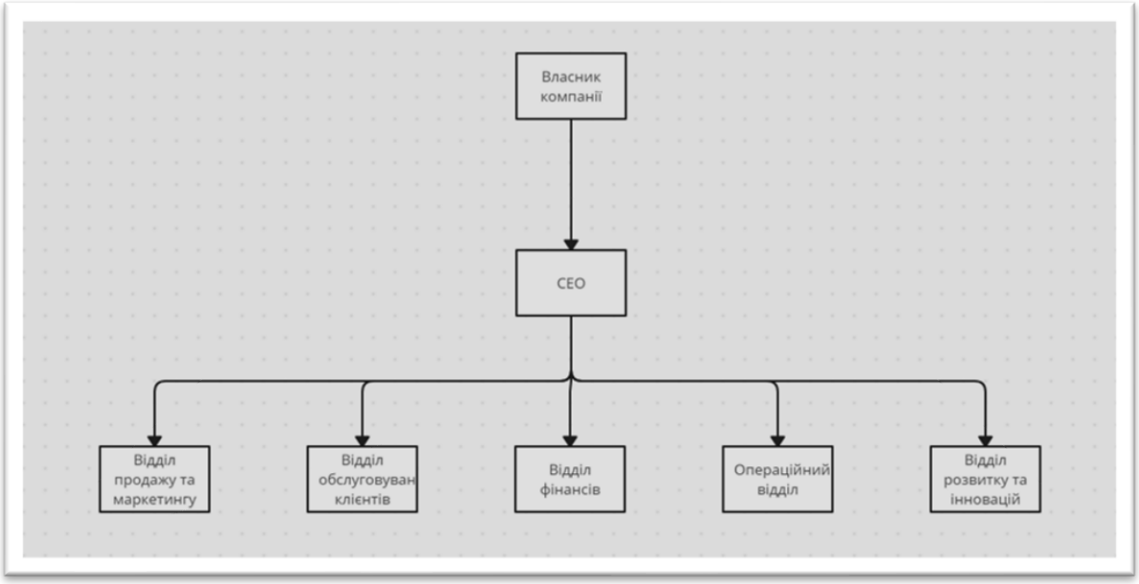

Рисунок 1.3 – Схема організаційної структури

1.6 Завдання і мета роботи

Метою роботи є розробка і впровадження комплексної комп'ютерної системи для ТОВ ВФ "ЛІБЕРТА", яка б забезпечила ефективне управління виробничими, логістичними та адміністративними процесами з урахуванням специфіки галузі виробництва і оброблення скляних виробів. Система повинна включати в себе передові технології обробки та передачі інформації, високий рівень безпеки даних, та можливість гнучкої інтеграції з іншими інформаційними системами і технологіями.

Завдання роботи:

1) Аналіз існуючої системи:

– Вивчення поточного стану інформаційних систем та мережевої інфраструктури в компанії.

– Оцінка потреб компанії у зв'язку з виробничими, адміністративними та логістичними процесами.

2) Проектування системи:

– Розробка технічного завдання для нової комп'ютерної системи.

– Проектування мережевої архітектури та вибір обладнання.

Завдяки впровадженню сучасної комп'ютерної системи очікується значне покращення ефективності виробничих та управлінських процесів в ТОВ ВФ "ЛІБЕРТА", збільшення продуктивності, зниження витрат та підвищення рівня задоволення клієнтів.

1.7 Визначення можливих напрямків рішення поставлених завдань

Для вирішення поставлених завдань можна розглянути наступні напрямки:

Розробка масштабованої мережі. Впровадження принципів та структур після який мережа може бути з легкістю масштабована.

Використання IoT. Впровадження системи IoT для моніторингу виробничих процесів та управління обладнанням дозволить забезпечити більш точний контроль за виробництвом та підтримувати обладнання в ефективному стані.

Використання аналітики даних. Впровадження системи аналізу даних дозволить вчасно виявляти та аналізувати тенденції, що сприятиме прийняттю кращих управлінських рішень.

Забезпечення кібербезпеки. Важливим напрямком є забезпечення безпеки інформації та мережі, що може включати в себе впровадження систем антивірусного захисту, захисту мережі та інших заходів.

Ці напрямки можуть бути використані для реалізації поставлених завдань з розробки та впровадження комп'ютерної системи у ТОВ ВФ "ЛІБЕРТА".

1.8 Обґрунтування вибраного напрямку інженерного рішення

Вибір конкретного напрямку інженерного рішення для розробки та впровадження комплексної комп'ютерної системи у ТОВ ВФ "ЛІБЕРТА" може бути обґрунтований наступними аргументами:

Забезпечення надійності та безпеки даних. Впровадження сучасних технологій обробки та збереження інформації, а також заходів з кібербезпеки дозволить забезпечити високий рівень захисту конфіденційної інформації компанії.

Підвищення ефективності роботи персоналу. Розробка мобільних додатків для співробітників та клієнтів компанії може значно полегшити доступ до необхідної інформації та підвищити продуктивність працівників.

Моніторинг та аналіз даних. Використання систем аналітики даних дозволить компанії вчасно виявляти та аналізувати тенденції, що сприятиме прийняттю кращих управлінських рішень та підвищить конкурентоспроможність.

Гнучкість та масштабованість системи. Важливим аспектом є можливість гнучкої інтеграції з іншими інформаційними системами та технологіями, що забезпечить зручність та ефективність використання комп'ютерної системи у майбутньому.

Ці аргументи обгрунтовують вибір напрямку інженерного рішення для розробки та впровадження комплексної комп'ютерної системи у ТОВ ВФ "ЛІБЕРТА", яка забезпечить покращення управління та ефективність у всіх сферах діяльності компанії.

2 РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ КОМП’ЮТЕРНОЇ

2.1 Технічні вимоги до комп’ютерної системи компанії

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 ВФ "ЛІБЕРТА" спрямоване на створення ефективного механізму обміну інформацією між відділами компанії, з особливою увагою до забезпечення надійного зберігання даних та їхнього захисту. Система має бути розроблена таким чином, аби забезпечити постійний доступ співробітників до корпоративних ресурсів протягом усіх робочих годин.

У рамках цього проекту планується створення п'яти локальних мереж (LAN), кожна з яких має свої специфічні вимоги до IP-адресації для ефективного налаштування підмереж. Для цього необхідно здійснити поділ IP-адреси 172.24.168.0/21 на п'ять підмереж з урахуванням кількості вузлів, що обслуговуються кожною з них:

LAN1 має включати 16 вузлів;

LAN2 розрахована на 84 вузлів;

LAN3 повинна обслуговувати 98 вузол;

LAN4 задіятиме 18 вузлів;

LAN5 розрахована на 117 вузол.

Крім того, важливим аспектом є впровадження заходів забезпечення безпеки мережі. Це включає застосування шифрування даних, фільтрацію трафіку, а також використання політик безпеки для захисту від несанкціонованого доступу та інших кіберзагроз. Система також має передбачати механізми резервного копіювання та відновлення даних для забезпечення надійності зберігання інформації та її доступності в критичних ситуаціях.

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

Зв'язок між компонентами комп'ютерної системи повинен забезпечувати високу швидкість передачі даних для підтримки ефективної роботи системи. Для цього необхідно використовувати високошвидкісні мережеві протоколи та технології, такі як Gigabit Ethernet або 10 Gigabit Ethernet для підключення серверів, комутаторів і основних мережевих вузлів.

Зв'язок повинен бути надійним і стійким до відмов. Для цього слід використовувати резервування мережевих шляхів та компонентів. Наприклад, дублювання ліній зв'язку і застосування технологій, таких як Spanning Tree Protocol (STP) для запобігання петлям у мережі, а також використання кластеризації серверів для забезпечення високої доступності.

Захист інформації під час передачі даних є критично важливим. Для цього необхідно використовувати шифрування даних, як-от протоколи SSL/TLS для захисту мережевого трафіку, а також IPsec для забезпечення конфіденційності, цілісності та автентичності даних на рівні мережі. Крім того, слід застосовувати VPN (віртуальні приватні мережі) для захищеного доступу до ресурсів мережі з віддалених місць.

Система повинна бути легко масштабованою, щоб підтримувати зростання мережі та збільшення кількості користувачів і пристроїв. Це включає можливість додавання нових комутаторів, маршрутизаторів та інших мережевих пристроїв без значних змін у існуючій інфраструктурі. Використання модульних комутаторів і маршрутизаторів, а також архітектур, які підтримують масштабованість (наприклад, Spine-Leaf), може значно полегшити цей процес.

Забезпечення сумісності між різними компонентами системи є важливим для стабільної роботи. Це включає підтримку загальноприйнятих протоколів і стандартів, таких як Ethernet, TCP/IP, SNMP для моніторингу та управління мережею. Крім того, слід враховувати сумісність обладнання від різних виробників для уникнення проблем з інтеграцією.

Для забезпечення надійного та ефективного зв’язку між компонентами системи необхідно використовувати якісне мережеве обладнання, таке як маршрутизатори, комутатори, точки доступу та мережеві адаптери. Комутатори повинні підтримувати необхідні рівні VLAN для сегментації трафіку, а маршрутизатори — протоколи маршрутизації, такі як OSPF або BGP, для оптимальної передачі даних.

Для зв’язку між стаціонарними компонентами системи слід використовувати сучасні кабельні системи, такі як мідні кабелі категорії 6а або оптичні кабелі, які забезпечують високу пропускну здатність та надійність. Важливо також забезпечити правильне прокладання кабелів з дотриманням стандартів та рекомендацій для мінімізації впливу електромагнітних завад і фізичних ушкоджень.

Для мобільних пристроїв та місць, де прокладання кабелів недоцільне, необхідно використовувати бездротові засоби зв’язку, такі як Wi-Fi 6 (802.11ax) або Wi-Fi 7 (802.11be). Ці технології забезпечують високу швидкість передачі даних, знижену затримку та підвищену ефективність використання спектру.

Для управління та моніторингу мережевих з'єднань слід використовувати програмні засоби, такі як системи управління мережею (NMS) і програмне забезпечення для моніторингу мережевого трафіку (наприклад, Wireshark, PRTG). Ці інструменти дозволяють адміністратору контролювати стан мережі, виявляти та усувати проблеми, а також оптимізувати продуктивність мережі.

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

Для забезпечення безперебійної взаємодії з суміжними системами необхідно використовувати загальноприйняті мережеві протоколи та стандарти. Це включає підтримку протоколів TCP/IP, Ethernet, IPv4 та IPv6, а також протоколів маршрутизації, таких як OSPF, BGP та EIGRP. Дотримання стандартів, визначених організаціями, такими як IEEE та IETF, забезпечить сумісність із зовнішніми мережами та пристроями.

Для захисту взаємодії з суміжними системами слід використовувати міжмережеві екрани (фаєрволи) та контролери доступу. Вони повинні підтримувати сучасні методи автентифікації та шифрування для забезпечення безпечного обміну даними. Це включає використання VPN для захищеного доступу до зовнішніх мереж та TLS/SSL для захисту мережевого трафіку.

Взаємодія з суміжними системами вимагає інтеграції систем управління та моніторингу. Слід використовувати протоколи SNMP, Syslog та інші стандарти для збору та аналізу даних про стан мережі. Це дозволить ефективно моніторити взаємодію між системами та виявляти потенційні проблеми.

Для забезпечення гнучкої взаємодії з суміжними системами слід використовувати API. Вони дозволять обмінюватися даними та керувати функціями між різними системами. Використання RESTful API, SOAP або інших сучасних технологій дозволить забезпечити ефективну інтеграцію.

Взаємодія з суміжними системами повинна забезпечувати високу пропускну здатність та мінімальну затримку. Це особливо важливо для критичних застосунків та сервісів, які вимагають швидкого обміну даними. Використання високошвидкісних мережевих технологій та оптимізація маршрутизації допоможе досягти необхідних показників продуктивності.

Система повинна бути відмовостійкою та мати можливості резервування для забезпечення безперервної роботи у випадку збоїв. Це включає використання резервних ліній зв'язку, дублювання важливих компонентів та автоматичне переключення на резервні ресурси у разі виникнення проблем. Важливо також передбачити механізми швидкого відновлення після аварій.

Для забезпечення безпеки взаємодії з суміжними системами необхідно впровадити надійні методи автентифікації та авторизації. Це може включати використання двофакторної автентифікації (2FA), централізованих систем управління ідентифікацією (IDM) та роле-орієнтованого контролю доступу (RBAC).

Система повинна бути захищена від зовнішніх атак та зловмисного програмного забезпечення. Це передбачає використання антивірусних засобів,

систем виявлення та запобігання вторгнень (IDS/IPS), а також регулярне оновлення програмного забезпечення для усунення вразливостей.

Необхідно вести детальну документацію всіх взаємозв'язків із суміжними системами. Це включає опис мережевої топології, використовуваних протоколів, налаштувань безпеки та процедур взаємодії. Така документація допоможе у підтримці та масштабуванні системи.

Для ефективного управління взаємодією з суміжними системами слід використовувати системи управління конфігураціями (наприклад, Ansible, Puppet, Chef). Це дозволить автоматизувати процеси налаштування та забезпечити єдність конфігурацій на всіх рівнях системи.

Загалом, дотримання цих вимог забезпечить надійну, безпечну та ефективну взаємодію створюваної системи із суміжними системами, що є критично важливим для успішної реалізації проекту.

2.1.1.1.4 Вимоги до режимів функціонування системи

Система повинна функціонувати у кількох основних режимах: нормальному, режимі високого навантаження, аварійному та режимі технічного обслуговування. У нормальному режимі система працює за стандартними параметрами, обробляє та передає дані, зберігає інформацію та забезпечує постійний моніторинг і управління. У режимі високого навантаження система повинна автоматично або вручну масштабувати ресурси для підтримки стабільної роботи, використовувати балансування навантаження та оптимізацію продуктивності. Аварійний режим активується при виникненні критичних помилок або збоїв і вимагає швидкого виявлення проблем, автоматичного переключення на резервні компоненти та швидкого відновлення нормальної роботи. Під час технічного обслуговування повинно бути забезпечене планування робіт, резервне копіювання даних і обмеження доступу для мінімізації ризиків.

Для забезпечення безперервності роботи система повинна мати високу доступність (99.9% і вище) завдяки кластеризації та резервуванню критичних компонентів і даних. Безпека повинна бути на високому рівні у всіх режимах

функціонування, що включає шифрування даних, багаторівневу автентифікацію та авторизацію, а також постійний моніторинг безпеки.

2.1.1.1.5 Вимоги до діагностування системи

Для виявлення потенційних проблем необхідно регулярно проводити автоматичні та ручні діагностичні тести. Це можуть бути тести на продуктивність, перевірка цілісності даних, аналіз логів, а також перевірка безпеки. Результати тестів повинні зберігатися для подальшого аналізу та звітності.

2.1.1.1.6 Перспективи розвитку, модернізації системи

Розвиток системи повинен передбачати постійне впровадження новітніх технологій. Це може включати перехід на більш швидкі та ефективні мережеві протоколи, такі як 10 Gigabit Ethernet або 40/100 Gigabit Ethernet, а також впровадження технологій наступного покоління, як-от Wi-Fi 6 (802.11ax) та Wi-Fi 7 (802.11be) для підвищення пропускної здатності бездротових мереж.

Модернізація системи повинна включати інтеграцію з хмарними сервісами для підвищення гнучкості та масштабованості. Використання хмарних платформ, таких як AWS, Azure або Google Cloud, дозволить зменшити витрати на власне обладнання та забезпечить можливість швидкого масштабування ресурсів відповідно до потреб бізнесу.

Впровадження рішень на основі штучного інтелекту (AI) та машинного навчання (ML) може значно покращити ефективність роботи системи. Це включає автоматизацію процесів моніторингу та діагностики, прогнозування можливих збоїв, а також оптимізацію використання ресурсів на основі аналізу великих обсягів даних.

З огляду на постійне зростання кіберзагроз, модернізація системи повинна включати впровадження передових засобів захисту. Це може включати використання нових методів автентифікації, таких як біометричні дані або багатофакторна автентифікація (MFA), вдосконалення систем виявлення та

запобігання вторгнень (IDS/IPS), а також впровадження систем безпеки на основі поведінкових моделей.

Періодична модернізація апаратного забезпечення є необхідною для підтримання високої продуктивності та надійності системи. Це може включати оновлення серверів, мережевих комутаторів, маршрутизаторів та інших критичних компонентів, щоб відповідати сучасним стандартам та забезпечити максимальну ефективність.

Система повинна бути готова до інтеграції з новими додатками та сервісами, що можуть виникнути в майбутньому. Це включає використання стандартних API, підтримку нових форматів даних та забезпечення сумісності з різноманітними платформами та пристроями.

Покращення користувацького досвіду є важливим аспектом розвитку системи. Це може включати вдосконалення інтерфейсів користувача, забезпечення більшої зручності та функціональності, а також впровадження нових сервісів та можливостей для користувачів.

Модернізація системи повинна враховувати екологічні аспекти, такі як зменшення енергоспоживання, використання енергоефективного обладнання та впровадження екологічно чистих технологій. Це допоможе не тільки знизити витрати на енергоспоживання, але й покращити екологічний імідж компанії.

2.1.1.2 Вимоги до патентної чистоти

Перед початком проектування та впровадження нових технологій і рішень у систему, необхідно провести ретельний аналіз патентного ландшафту. Це включає дослідження існуючих патентів у відповідних технологічних галузях, виявлення потенційних патентних ризиків і оцінку можливості використання певних технологій без порушення прав третіх осіб. Аналіз патентного ландшафту повинен проводитися як внутрішніми експертами компанії, так і за участю зовнішніх патентних консультантів.

Для кожного компонента та технології, які планується використовувати у системі, необхідно провести перевірку на патентну чистоту. Це включає аналіз патентних баз даних для виявлення патентів, що можуть бути порушені, а також оцінку можливості отримання ліцензій на використання певних запатентованих рішень. Особливу увагу слід приділити програмному забезпеченню, апаратним компонентам і методам обробки даних.

У разі виявлення необхідності використання запатентованих технологій, слід вжити заходів для отримання відповідних ліцензій та дозволів. Це може включати укладення ліцензійних угод з власниками патентів, придбання прав на використання технологій або укладення угод про співпрацю. Важливо забезпечити, щоб всі ліцензії були юридично оформлені та відповідали вимогам патентного законодавства.

Патентне середовище постійно змінюється, тому необхідно регулярно моніторити нові патентні заявки та видачі патентів, що можуть вплинути на діяльність компанії. Це дозволить своєчасно виявляти потенційні загрози та вживати заходів для мінімізації патентних ризиків. Моніторинг може здійснюватися за допомогою спеціалізованих програмних засобів та аналітичних інструментів.

Компанія повинна впровадити внутрішню політику патентної чистоти, яка включає процедури перевірки та документування патентної чистоти для всіх нових проектів та розробок. Це включає навчання співробітників з питань патентного законодавства, регулярні перевірки проектів на відповідність вимогам патентної чистоти, а також документування всіх дій, пов'язаних з патентною перевіркою та ліцензуванням.

Для забезпечення високого рівня патентної чистоти компанія повинна співпрацювати з досвідченими патентними консультантами та адвокатами. Це дозволить отримувати професійні консультації з питань патентного права, своєчасно виявляти потенційні ризики та вживати необхідних заходів для їх усунення. Взаємодія з патентними консультантами також допоможе у вирішенні патентних спорів та захисті інтересів компанії.

2.1.2 Вимоги до видів забезпечення комп’ютерної системи

2.1.2.1 Вимоги до математичного забезпечення

Не надаються.

2.1.2.2 Вимоги до інформаційного забезпечення

Інформаційне забезпечення системи TOV VF "LIBERTA" має бути структуроване таким чином, щоб забезпечити ефективну обробку, зберігання та передачу даних. Основні вимоги до інформаційного забезпечення включають:

Дані повинні бути структурованими відповідно до встановлених стандартів і форматів для забезпечення сумісності між різними підсистемами. Використання форматів XML, JSON, SQL дозволить забезпечити інтеграцію та взаємодію з іншими системами. Всі дані повинні бути чітко задокументовані, з описом їх структури, типів і обмежень.

Система повинна забезпечувати цілісність і консистентність даних на всіх етапах їх обробки та зберігання. Це включає механізми контролю версій даних, використання транзакційних систем з функцією відкату змін, а також регулярне проведення перевірок цілісності даних. Важливо також впровадити системи автоматичного виявлення та виправлення помилок у даних.

Захист даних

Всі дані повинні бути захищені від несанкціонованого доступу, модифікації та втрати. Для цього необхідно використовувати сучасні методи шифрування як при зберіганні даних (AES-256), так і при їх передачі (TLS/SSL). Доступ до даних повинен контролюватися за допомогою багаторівневих систем автентифікації та авторизації, з використанням ролей та прав доступу.

Система повинна забезпечувати високий рівень доступності даних для користувачів та додатків. Це включає використання реплікації даних, резервного копіювання та відновлення, а також впровадження високодоступних кластерів баз даних. Важливо забезпечити безперебійну роботу системи навіть у випадку збоїв або аварійних ситуацій.

2.1.2.3 Вимоги до лінгвистичного забезпечення

Система повинна підтримувати кілька мов, включаючи українську, англійську необхідні для користувачів. Це включає інтерфейс користувача, документацію, повідомлення про помилки та будь-які інші текстові елементи. Потрібно забезпечити можливість легко переключатися між мовами без втрати даних чи функціональності.

2.1.2.4 Вимоги до технічного забезпечення

Для забезпечення ефективної роботи системи необхідно використовувати сучасні сервери, які можуть обробляти великі обсяги даних та забезпечувати високу продуктивність. Сервери повинні мати багатоядерні процесори (не менше 8 ядер), значну кількість оперативної пам'яті (не менше 64 ГБ) та швидкі накопичувачі (SSD або NVMe) з можливістю розширення. Сервери повинні підтримувати віртуалізацію та мати резервні блоки живлення для підвищення надійності.

Мережеве обладнання повинно включати комутатори та маршрутизатори, які підтримують високошвидкісні протоколи передачі даних (Gigabit Ethernet, 10 Gigabit Ethernet) та забезпечують мінімальні затримки і втрати пакетів. Обладнання повинно підтримувати функції QoS, VLAN, STP та інші протоколи для ефективного управління трафіком та забезпечення надійності мережі.

Системи зберігання даних повинні забезпечувати високу швидкість доступу до даних та надійність зберігання. Це можуть бути мережеві системи зберігання (NAS, SAN) або кластерні рішення для розподіленого зберігання. Обов'язковою є підтримка RAID-масивів для захисту від втрати даних у випадку відмови дисків, а також можливість масштабування обсягу зберігання.

Робочі станції для користувачів повинні мати достатню продуктивність для виконання їхніх задач. Це включає сучасні процесори, не менше 8 ГБ оперативної пам'яті, SSD-накопичувачі для швидкого завантаження системи та додатків, а також високоякісні дисплеї. Важливо забезпечити сумісність з усім використовуваним програмним забезпеченням.

2.1.2.5 Вимоги до методичного забезпечення

Необхідно розробити та впровадити стандарти для всіх аспектів роботи з системою, включаючи управління даними, безпеку, резервне копіювання, управління користувачами та доступом. Ці стандарти повинні бути документовані і доступні для всіх користувачів системи.

Всі операції та процедури повинні виконуватися відповідно до встановлених протоколів. Це включає протоколи безпеки, протоколи резервного копіювання і відновлення, а також протоколи моніторингу та управління системою.

Розробка детальних керівництв користувача, які включають інструкції щодо використання системи, вирішення поширених проблем та відповіді на часті питання. Керівництва повинні бути написані зрозумілою мовою та містити ілюстрації та приклади.

Розробка спеціалізованих інструкцій для технічного персоналу, адміністраторів та інших працівників, які забезпечують підтримку і управління системою. Ці інструкції повинні охоплювати всі технічні аспекти, процедури обслуговування та оновлення системи.

Проведення регулярних тренінгів для користувачів та технічного персоналу для ознайомлення з новими функціями системи, оновленнями програмного забезпечення та новими методиками роботи.

2.2 Розробка апаратної частини комп’ютерної системи

2.2.1 Розробка загальної архітектури мережі підприємства

Маршрутизатори з'єднуються між собою за допомогою кабелів Serial DTE або крос-кабелів, що забезпечує надійний і швидкий обмін даними між різними сегментами мережі. Використання таких кабелів створює стабільні та ефективні з'єднання, необхідні для оптимального функціонування мережі. У цій мережевій архітектурі маршрутизатори відіграють важливу роль, забезпечуючи зв'язок між різними підмережами та дозволяючи їм обмінюватися інформацією.

Маршрутизатори з'єднуються з комутаторами за допомогою прямих кабелів, що гарантує високу пропускну здатність і надійність з'єднань. Таке підключення дозволяє комутаторам ефективно передавати дані між різними пристроями в мережі, включаючи персональні комп'ютери, сервери та інші мережеві пристрої. Прямі кабелі легко встановлюються та забезпечують стабільне з'єднання без втрат даних.

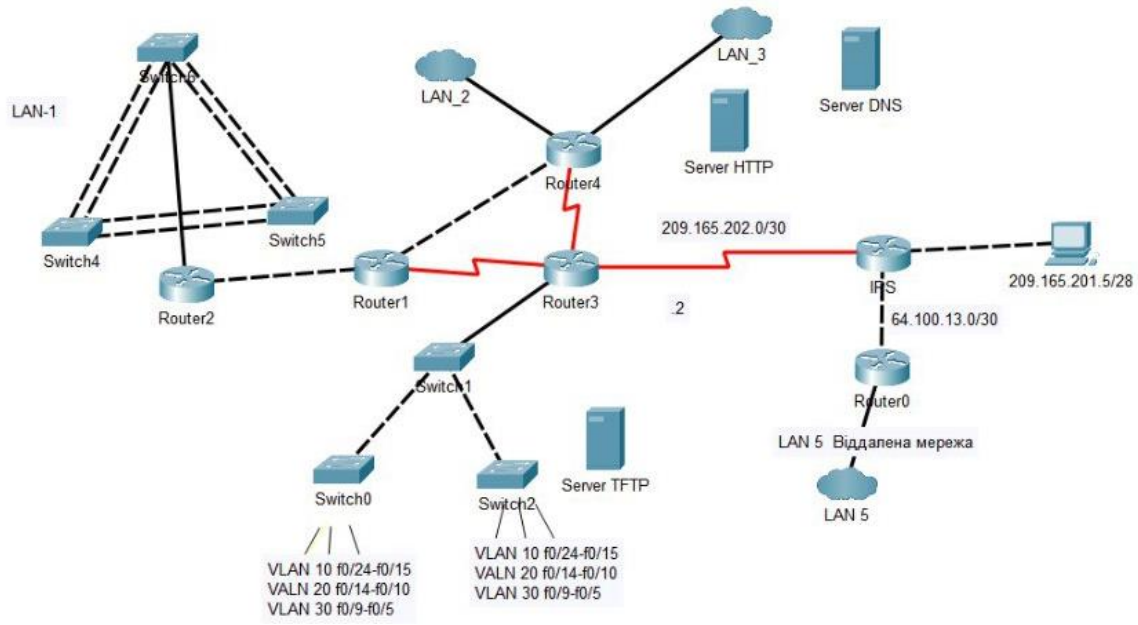

Рисунок 2.1 – Структурна схема комплексу технічних засобів комп’ютерної системи

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

Структурна схема передбачає використання резервування на рівні маршрутизаторів та комутаторів. Комутатори у LAN-1 з'єднані між собою та з Router1 і Router2, що забезпечує альтернативні маршрути передачі даних у випадку відмови одного з компонентів. Використання VLAN дозволяє ізолювати різні типи трафіку, що підвищує безпеку і стабільність мережі.

Схема дозволяє легко додавати нові підмережі та пристрої без суттєвих змін у поточній конфігурації. Використання VLAN спрощує управління мережею та

розширення її функціональних можливостей. Можливість підключення додаткових маршрутизаторів і комутаторів дозволяє масштабувати мережу відповідно до зростання потреб компанії.

Використання окремих VLAN для різних типів трафіку дозволяє підвищити безпеку мережі, зменшуючи можливість несанкціонованого доступу до критичних ресурсів. З'єднання з віддаленими мережами через захищені канали (IPS) забезпечує безпеку передачі даних між географічно розподіленими сегментами мережі.

Застосування сучасних маршрутизаторів та комутаторів з високою пропускною здатністю забезпечує ефективну передачу даних між підмережами і пристроями. Використання VLAN і сегментація мережі дозволяє оптимізувати використання мережевих ресурсів, знижуючи навантаження на окремі компоненти.

Структурна схема забезпечує зручне адміністрування і управління мережею. Використання централізованого управління VLAN та інтерфейсів маршрутизаторів спрощує процес налаштування та моніторингу мережевих ресурсів. Наявність документованих стандартів і протоколів забезпечує систематичний підхід до управління мережею.

2.2.3 Розробка специфікації апаратних засобів комп’ютерної системи

Для забезпечення надійної роботи комп'ютерної системи TOV VF "LIBERTA" необхідно детально розробити специфікацію апаратних засобів, які будуть використовуватися в мережі. У цьому випадку використовуються маршрутизатори Cisco 2911 та комутатори Cisco 2960-24TT. Нижче наведена детальна специфікація для кожного типу обладнання.

Маршрутизатори Cisco 2911 є частиною серії Cisco 2900 Integrated Services Routers (ISR), які забезпечують високий рівень продуктивності та надійності для малих і середніх підприємств.

1. Процесор**:** Multi-core CPU з апаратним прискоренням
2. Пам'ять: 512 MB DDR2 DRAM (можливе розширення до 2.5 GB)
3. Flash пам'ять**:** 256 MB (можливе розширення до 8 GB)

Інтерфейси**:**

1. вбудованих 10/100/1000 Ethernet порти

2. 1 вбудований ISM слот для внутрішнього службового модуля

3. 2 вбудовані розширювальні слоти Enhanced High-Speed WAN Interface Card (EHWIC)

4. 2 вбудовані слоти для цифрових сигналів (DSP)

5. 1 вбудований слот для службового модуля (SM)

6. Підтримка інтерфейсів WAN**:** серійні, Ethernet, E1/T1, xDSL, 3G/4G

Функціональні можливості**:**

1. Підтримка протоколів маршрутизації (RIP, OSPF, EIGRP, BGP)

2. Підтримка VPN (IPsec, SSL VPN)

3. Підтримка QoS для управління трафіком

4. Підтримка бездротових і мобільних підключень

Маршрутизатори Cisco 2911 використовуються для забезпечення зв'язку між різними підмережами та зовнішніми мережами, підтримують високошвидкісний обмін даними та забезпечують безпеку мережі.

Комутатори Cisco 2960-24TT є частиною серії Cisco Catalyst 2960, які призначені для забезпечення надійного з'єднання в мережах малого та середнього бізнесу.

Порти**:**

1. 24 порти 10/100 Ethernet для підключення кінцевих пристроїв

2. порти 10/100/1000 Ethernet uplink для підключення до основних мережевих компонентів

3. Пропускна здатність: 16 Gbps

4. Переключення**:** 35.7 Mpps (мільйонів пакетів в секунду)

5. Пам'ять**:** 64 MB DRAM, 32 MB Flash

Функціональні можливості:

1. Підтримка VLAN для сегментації мережі

2. Підтримка протоколів Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), Multiple Spanning Tree Protocol (MSTP)

3. Підтримка якості обслуговування (QoS) для управління трафіком

4. Підтримка IEEE 802.1x для контролю доступу до мережі

5. Підтримка технології EnergyWise для управління енергоспоживанням

Управління:

1. Веб-інтерфейс для налаштування та моніторингу

2. CLI (інтерфейс командного рядка) для детального управління

3. Підтримка протоколів управління мережею (SNMP, RMON)

Усе мережеве обладнання, за винятком бездротових маршрутизаторів, вибрано від компанії Cisco, тому проблем із сумісністю компонентів системи не очікується.

Таблиця 2.1 – Специфікація обладнання

Позиція	Найменування і технічна характеристика	Тип, марка, позначення документа	Одиниці виміру	Кількість
1	**2**	**3**	**4**	**5**
1	Cisco 2911 System, Crypto, 4 built-in GE, Dual P/S, 20Gbit, 6x1000Base-X (SFP), 2x10G SFP+ інтегровані RP, SIP та ESP, 1xNIM, 1xSPA, RAM 8Gb, 2xAC	Cisco 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.	17

Продовження таблиці 2.1

3	Сервер: 2 шт x Intel Xeon E5-2650L v2 (1.70-2.10 GHz), 8 GB DDR3, 2x порта 1 Gb Ethernet, Cisco Integrated Management Controller (CIMC)	Cisco UCS C220 M3 LFF	Од.	3

Розглянемо вибір структурованої кабельної мережі (СКМ) на прикладі LAN_3. Для цього спроектуємо схему поверху та розміщення кабелів, як показано на рис. 2.2. У СКМ зазначено кількість необхідних компонентів для системи відповідно до технічного завдання замовника, з урахуванням можливості масштабування, окрім кількості кабелів та кабель-каналів.

Специфікація структурованої кабельної мережі представлена в таблиці 2.2.

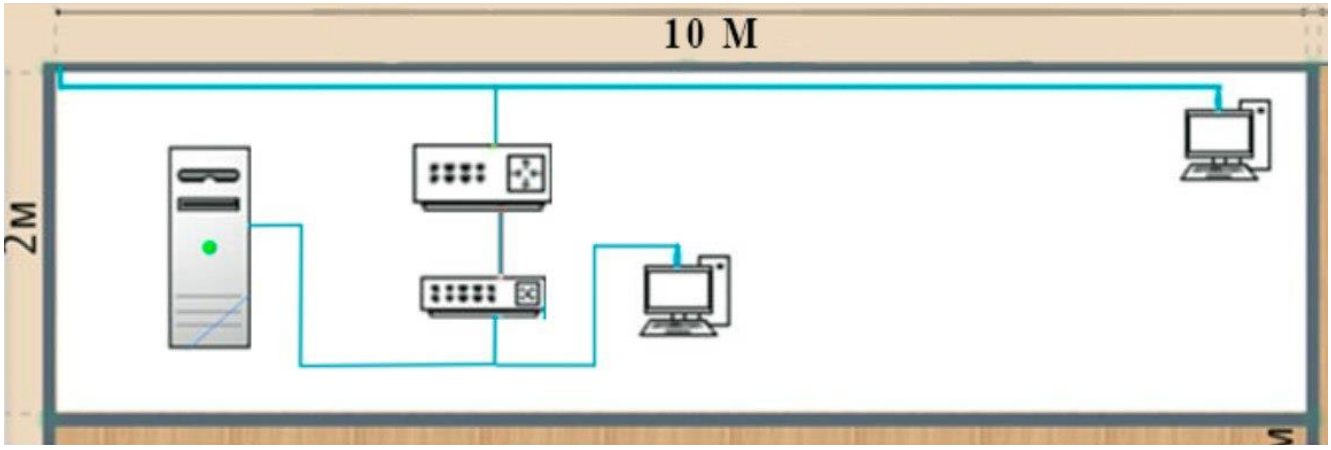

Рисунок 2.2 – Схема розміщення кабельних мереж для LAN_3

Таблиця 2.2 – Специфікація структурованої кабельної мережі

Позиція	Найменування	Одиниці	Кількість	Примітки
1.	**2.**	**4.**	**5.**	**6.**
1.	Кабельний канал 40×25 мм	м.	30	За проектом макету LAN_4

Продовження таблиці 2.2

2.	Розетка комп'ютерна RJ-45 UTP подвійна	од.	53	За проектом для LAN_4
3.	Lan кабель UTP КПВ-ВП cat.5E 4x2x0,51	м.	40	За проектом макету
4.	Розетка із заземленням подвійна	од.	65	За проектом для LAN_4
5.	Кабель живлення ПВС 3*2,5	м.	30	За проектом макету
6.	Кабельний канал 40×25 мм	м.	32	За проектом макету
7.	Комутаційна коробка	од.	1	За проектом для LAN_4

2.2.4 Розрахунок інтенсивності трафіку вихідного трафіку найбільшої локальної мережі підприємства

В підмережі встановлений комутатор Cisco2960, що об'єднує 117 ПК працівників. Вихідний трафік з комутатора надсилається до роутера в лінію з пропускною здатністю, що становить 1000 Мбіт/с.

Для того, щоб комутатор не був перенасичений, швидкість надходження пакетів не повинна перевищувати швидкості їх відправлення. Вважаємо, що послугами одночасно користуються 100% користувачів. Середня інтенсивність трафіку μ=196 (кадрів/с), а середня довжина повідомлення – 1150 байт.

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

$$P_{р.р.} = \mu * L_{пов} * N * 8 = 196 * 1150 * 117 * 8 = 15.8 \text{ Мбіт/с} \quad (2.1)$$

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

N – кількість вузлів в мережі.

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

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

$$\mu_{вих} = 10^9 / (1150 * 8) = 108\,696 \text{ пакетів/с} \quad (2.2)$$

Оскільки в середньому, кожне джерело виробляє 86 пакетів/с, то маршрутизатор обмежений кількістю приєднань, яку ми можемо дізнатись наступним чином:

$$N = \mu_{вих} / \mu = 108\ 696/\ 86 \approx 1264 \text{ джерела} \quad (2.3)$$

Ця кількість задовольняє кількості вузлів у найбільшій нашій локальній мережі, до якої входить 117 ПК.

Кожен з 117 ПК посилає потік заявок з інтенсивністю у 86 кадрів/с. Звідси, можем розрахувати інтенсивність вихідного трафіку:

$$\lambda = N * \mu = 117*196 = 1720 \text{ пакетів/с.} \quad (2.4)$$

Коефіцієнт затримки:

$$\rho = \frac{\lambda}{\mu вих} = \frac{1720}{108696} = 0{,}016 \quad (2.5)$$

Коефіцієнт зайнятості маршрутизатора:

$$\frac{\rho}{1-\rho} = \frac{0{,}016}{1-0{,}016} = 0{,}016 \quad (2.6)$$

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

$$T = \frac{1}{(\mu-\lambda)} = \frac{1}{(108696 - 1720)} = 9{,}35 \text{ мкс} \quad (2.7)$$

Середня довжина черги:

$$L_{чер} = \frac{\rho^2}{1-\rho} = \frac{0{,}016^2}{1-0.016} = 0.0026 \quad (2.8)$$

Середній час перебування пакета у черзі:

$$T_{оч} = \frac{Lчер}{\lambda} = \frac{0{,}026}{1720} = 0{,}15 \text{ мкс} \quad (2.9)$$

Це значення задовольняє вимогам до затримки в ЛМ.

3 РОЗРОБКА КОРПОРАТИВНОЇ МЕРЕЖІ

3.1 Проектування логічної топології мережі

Топологія корпоративної мережі організована з використанням комутаторів та маршрутизаторів, що забезпечують надійні з'єднання між різними відділами та мережевими сегментами. Ключовим елементом цієї топології є інтеграція VLAN (Virtual Local Area Network), яка дозволяє ефективно розділити мережеві ресурси відповідно до функціональних потреб без необхідності зміни фізичної структури мережі. Це рішення забезпечує високий рівень безпеки та оптимізацію трафіку, що є критично важливим для корпоративних мереж великих масштабів.

Інтеграція VLAN дозволяє ізолювати різні підрозділи компанії, забезпечуючи при цьому контроль доступу до чутливих даних та мінімізуючи ризики внутрішніх загроз. Наприклад, фінансовий відділ може бути відокремлений від загальної мережі, що значно підвищує рівень безпеки.

На рисунку 3.1 представлена топологічна схема корпоративної мережі ТОВ ВФ «ЛІБЕРТА». Схема включає основну мережу, віддалені підмережі та мережу провайдера. Основна мережа складається з центрального комутатора, до якого підключені комутатори різних відділів. Віддалені підмережі з'єднані з основною мережею за допомогою маршрутизаторів через канали зв'язку SerialEthernet та GigabitEthernet, що забезпечує високу пропускну здатність і надійність з'єднань. Мережа провайдера забезпечує зовнішній доступ до Інтернету та інших ресурсів, необхідних для функціонування компанії.

Крім того, використання різних типів з'єднань, таких як SerialEthernet та GigabitEthernet, дозволяє досягти баланс між швидкістю передачі даних та вартістю інфраструктури. SerialEthernet забезпечує стабільні з'єднання для критично важливих даних, тоді як GigabitEthernet використовується для високошвидкісної передачі великих обсягів інформації.

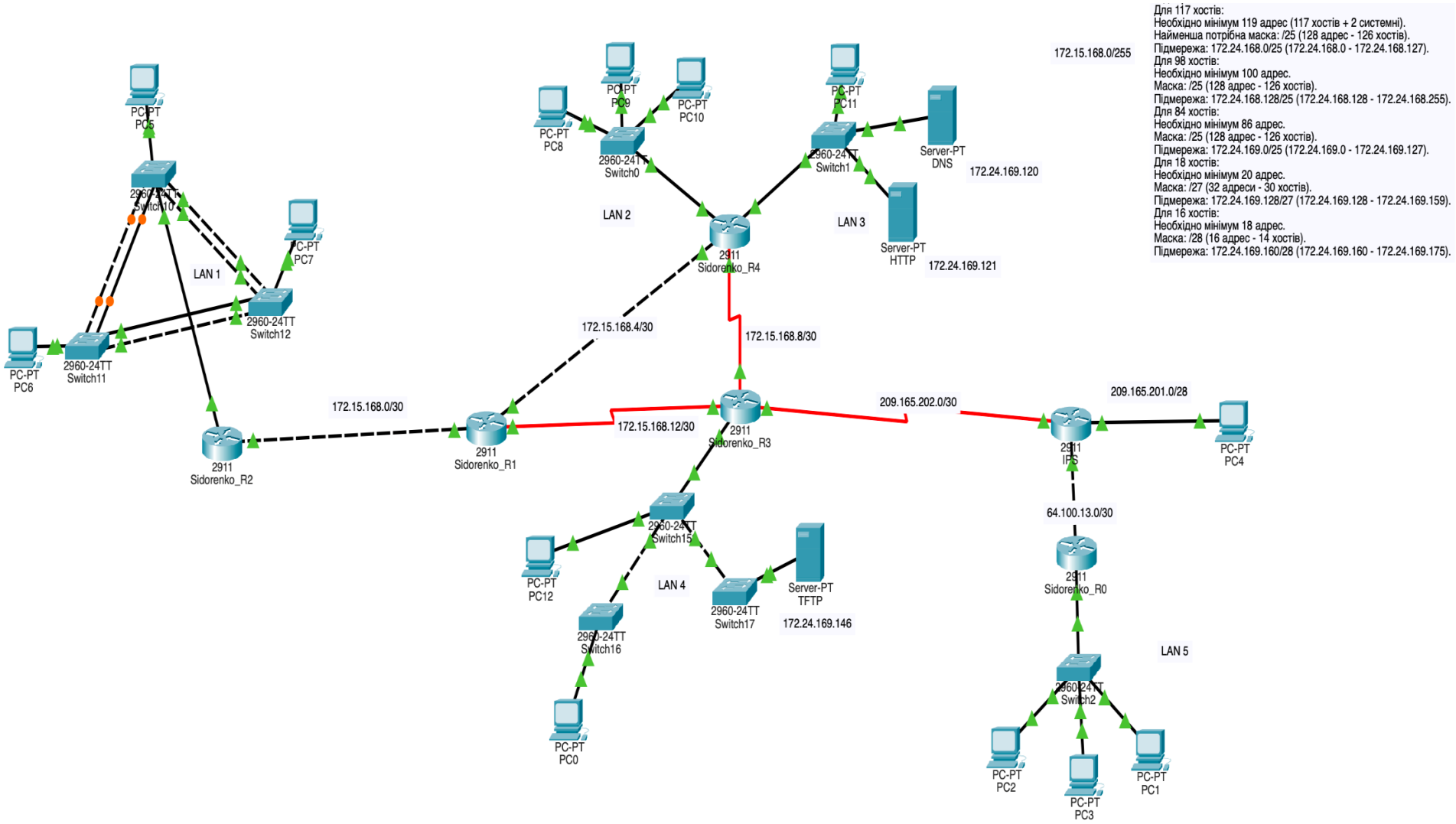

Рисунок 3.1 – Топологічна схема корпоративної мережі

3.2 Вибір та опис мережного обладнання

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

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

Маршрутизатори Cisco 2911: Ці маршрутизатори належать до серії Cisco ISR (Integrated Services Routers) і призначені для забезпечення високої продуктивності при роботі в складних мережах з великою кількістю мережевих сервісів. Модель 2911 підтримує модульність, що дозволяє додавати нові інтерфейси та сервіси без необхідності заміни обладнання. Маршрутизатори Cisco 2911 забезпечують високу безпеку передачі даних завдяки вбудованим засобам шифрування та підтримці VPN, що критично важливо для забезпечення захищеного зв'язку між різними локаціями компанії. Вони також підтримують функції оптимізації трафіку та якість обслуговування (QoS), що забезпечує стабільну роботу додатків з високими вимогами до пропускної здатності та надійності.

Вибір такого обладнання для мережі ТОВ ВФ «ЛІБЕРТА» виправданий їх високою надійністю, легкістю управління та можливістю розширення функціональності. Це дозволяє компанії ефективно масштабувати мережеві ресурси згідно зі зростанням бізнесу та новими вимогами, забезпечуючи при цьому високу безпеку та стабільність роботи мережі. Зокрема, використання

комутаторів та маршрутизаторів Cisco надає можливість швидко адаптувати мережеву інфраструктуру до нових викликів, зменшуючи ризики простоїв та втрат даних.

3.3 Розрахунок схеми адресації корпоративної мережі

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

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

№	Блок адрес	LAN1	LAN2	LAN3	LAN4	LAN5
15	172.24.168.0/21	16	84	98	28	117

Для проектування мережі компанії ТОВ ВФ «ЛІБЕРТА» необхідно створити п'ять підмереж для загальної кількості 331 користувача, використовуючи технологію VLSM (Variable Length Subnet Masking). Цей метод дозволяє створювати підмережі з різними довжинами масок, що підвищує ефективність використання ресурсів та збереження IP-адрес. Завдяки VLSM покращуються масштабованість та управління мережею.

1. Підмережа для 117 хостів

Потрібна кількість адрес: мінімум 119 (117 хостів + 2 системні)

Маска підмережі: /25 (128 адрес - 126 хостів)

Діапазон адрес: 172.24.168.0 - 172.24.168.127

Розрахунок маски: Маска /25 означає, що перші 25 бітів використовуються для адресації мережі, а решта 7 бітів — для хостів. Бітова адресація: 11111111.11111111.11111111.10000000 (255.255.255.128 у десятковій системі).

2. Підмережа для 98 хостів

Потрібна кількість адрес: мінімум 100

Маска підмережі: /25 (128 адрес - 126 хостів)

Діапазон адрес: 172.24.168.128 - 172.24.168.255

Розрахунок маски: Маска /25 має бітову адресацію: 11111111.11111111.11111111.10000000 (255.255.255.128 у десятковій системі).

3. Підмережа для 84 хостів

Потрібна кількість адрес: мінімум 86

Маска підмережі: /25 (128 адрес - 126 хостів)

Діапазон адрес: 172.24.169.0 - 172.24.169.127

Розрахунок маски: Маска /25 має бітову адресацію: 11111111.11111111.11111111.10000000 (255.255.255.128 у десятковій системі).

4. Підмережа для 18 хостів

Потрібна кількість адрес: мінімум 20

Маска підмережі: /27 (32 адреси - 30 хостів)

Діапазон адрес: 172.24.169.128 - 172.24.169.159

Розрахунок маски: Маска /27 означає, що перші 27 бітів використовуються для адресації мережі, а решта 5 бітів — для хостів. Бітова адресація: 11111111.11111111.11111111.11100000 (255.255.255.224 у десятковій системі).

5. Підмережа для 16 хостів

Потрібна кількість адрес: мінімум 18

Маска підмережі: /28 (16 адрес - 14 хостів)

Діапазон адрес: 172.24.169.160 - 172.24.169.175

Розрахунок маски: Маска /28 означає, що перші 28 бітів використовуються для адресації мережі, а решта 4 біти — для хостів. Бітова адресація: 11111111.11111111.11111111.11110000 (255.255.255.240 у десятковій системі).

Таблиця 3.1 – Схема адресації мережі

Назва підмережі	**Необхідна кількість**	**Адреса підмережі**	**Маска .**	**Маска підмережі у десятковому форматі**	**Діапазон допустимих IP-адрес вузлів**
LAN1	117	172.24.168.0	/25	255.255.255.128	172.24.168.1 - 172.24.168.126
LAN2	98	172.24.168.128	/25	255.255.255.128	172.24.168.129 - 172.24.168.254
LAN3	84	172.24.169.0	/25	255.255.255.128	172.24.169.1 - 172.24.169.126
LAN4	18	172.24.169.128	/27	255.255.255.224	172.24.169.129 - 172.24.169.158
LAN5	16	172.24.169.160	/28	255.255.255.240	172.24.169.161 - 172.24.169.174

Для з'єднань між маршрутизаторами буде використано адресний блок 172.15.168.0/24. Застосовуючи метод VLSM, мережа буде поділена на п'ять підмереж, кожна з яких міститиме по два вузли. В таблиці 3.3 наведено схему адресації цих з'єднань між маршрутизаторами.

Таблиця 3.2 – Схема адресації каналів між маршрутизаторами

Назва мережі	Кількість вузлів	Номер мережі	Маска мережі	Початкове значення діапазону	Кінцеве значення діапазону
WAN1	2	172.15.168.0	/30	172.15.168.1	172.15.168.2
WAN2	2	172.15.168.4	/30	172.15.168.5	172.15.126.6
WAN3	2	172.15.168.8	/30	172.15.168.9	172.15.168.10
WAN4	2	172.15.168.12	/30	172.15.168.13	172.15.168.14

3.4 Вибір та налаштування способу маршрутизації

3.4.1 Базове налаштування конфігурації пристроїв

Базове налаштування конфігурації пристроїв на прикладі Sidorenko_R2 (рис. 3.2).

```
Router>en
Router#conf
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname Sidorenko_R2
Sidorenko_R2(config)#line console 0
Sidorenko_R2(config-line)#password cisco
Sidorenko_R2(config-line)#login
Sidorenko_R2(config-line)#line vty 0 15
Sidorenko_R2(config-line)#password cisco
Sidorenko_R2(config-line)#login
Sidorenko_R2(config-line)#enable secret class
Sidorenko_R2(config)#service password-encryption
Sidorenko_R2(config)#banner motd #Sidorenko_R2#
Sidorenko_R2(config)#line vty 0 15
Sidorenko_R2(config-line)#transport input ssh
Sidorenko_R2(config-line)#login local
Sidorenko_R2(config-line)#username 12321ck_Sidorenko password admincisco
Sidorenko_R2(config)#ip domain-name Sidorenko_R2
Sidorenko_R2(config)#crypto key generate rsa
The name for the keys will be: Sidorenko_R2.Sidorenko_R2
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
```

Рисунок 3.2 – Налаштування конфігурації маршрутизатора

У мережі LAN_1 застосовується технологія EtherChannel, яка дозволяє об'єднати кілька фізичних інтерфейсів мережевого пристрою в один логічний канал. Це значно підвищує пропускну здатність і покращує надійність мережі шляхом балансування навантаження та резервування каналів.

Налаштування EtherChannel представлено на рисунку 3.3.

```
Switch(config)#interface range fa0/1-2
Switch(config-if-range)#channel-group 1 mode active
Switch(config-if-range)#interface port-channel 1
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan all
Switch(config-if)#interface range fa0/3-4
Switch(config-if-range)#channel-group 2 mode active
Switch(config-if-range)#interface port-channel 2
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan all
```

Рисунок 3.3 – Налаштування Etherchannel

3.4.2 Налаштування протоколу OSPF та DHCP для маршрутизаторів корпоративної мережі

Протокол DHCP (Dynamic Host Configuration Protocol) використовується для автоматичного призначення IP-адрес комп'ютерам та іншим пристроям у мережі. Це значно полегшує процес адміністрування мережі та налаштування пристроїв, оскільки адміністратори не повинні вручну налаштовувати кожен пристрій окремо. DHCP дозволяє автоматично призначати не тільки IP-адреси, але й інші параметри мережі, такі як шлюз за замовчуванням, DNS-сервери та інші важливі налаштування, що забезпечує безперебійну та коректну роботу мережевих сервісів.

Автоматизація процесу призначення IP-адрес за допомогою DHCP також підвищує ефективність використання мережевих ресурсів. Замість того, щоб фіксовано призначати IP-адреси, DHCP динамічно розподіляє їх серед пристроїв у міру їх підключення до мережі. Це дозволяє оптимізувати використання доступного адресного простору та запобігти конфліктам IP-адрес, які можуть виникнути при ручному налаштуванні. Крім того, автоматичне призначення адрес за допомогою DHCP зменшує ймовірність помилок, які можуть виникнути при ручному конфігуруванні, що робить процес налаштування більш надійним та зручним для мережевих адміністраторів.

Налаштування DHCP приведено на рисунку 3.4.

```
Sidorenko_R2(config)#ip dhcp excluded-address 172.24.168.1 172.24.168.5
Sidorenko_R2(config)#ip dhcp pool LAN-1
Sidorenko_R2(dhcp-config)# network 172.24.168.0 255.255.255.128
Sidorenko_R2(dhcp-config)# default-router 172.24.168.1
Sidorenko_R2(dhcp-config)# dns-server 172.24.169.120
Sidorenko_R2(dhcp-config)#
```

Рисунок 3.4 – Налаштування DHCP

Для забезпечення взаємодії користувачів з різних підмереж необхідно встановити маршрутизацію між цими мережами, що може бути реалізовано двома способами: статичною або динамічною маршрутизацією. Статична маршрутизація вимагає ручного налаштування маршрутів, тоді як динамічна маршрутизація автоматично оновлює маршрути, забезпечуючи гнучкість та

автоматизацію. У цьому проекті ми використовуватимемо протокол динамічної маршрутизації OSPF, який є одним з найпопулярніших завдяки своїй масштабованості, високому рівню безпеки, підтримці VLSM та сумісності з обладнанням різних виробників. OSPF використовує алгоритм SPF для знаходження найкоротших маршрутів, що підвищує швидкодію мережі та забезпечує ефективне керування мережевим трафіком, забезпечуючи стабільність та продуктивність мережі.

Налаштування протоколу OSPF наведено на рисунку 3.5.

```
Sidorenko_R2(config)#router ospf 1
Sidorenko_R2(config-router)# log-adjacency-changes
Sidorenko_R2(config-router)# passive-interface default
Sidorenko_R2(config-router)# no passive-interface GigabitEthernet0/0
Sidorenko_R2(config-router)# no passive-interface GigabitEthernet0/1
Sidorenko_R2(config-router)# auto-cost reference-bandwidth 1000
Sidorenko_R2(config-router)# network 172.24.168.0 0.0.0.127 area 0
Sidorenko_R2(config-router)# network 172.15.168.0 0.0.0.3 area 0
```

Рисунок 3.5 – Налаштування протоколу OSPF

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

ip route 0.0.0.0 0.0.0.0 209.165.202.2 // налаштовуємо маршрут за замовчуванням

router ospf 1 // увімкнення протоколу

redistribute static subnets // увімкнення розповсюдження статичних маршрутів через протокол OSPF

Додаємо статичний маршрут до мережі провайдера ISP:

ip route 209.165.201.0 255.255.255.240 209.165.202.2

3.4.3 Налаштування роботи Інтернет

Для доступу системи до Інтернету потрібно налаштувати технологію перетворення мережевих адрес NAT (Network Address Translation). NAT дозволяє трансформувати внутрішні IP-адреси на публічні та навпаки, а також змінювати номери портів. Це дає змогу багатьом пристроям одночасно використовувати Інтернет через обмежену кількість публічних IP-адрес.

Для реалізації NAT потрібно створити пул NAT-адрес, який міститиме діапазон публічних IP-адрес. Наприклад, пул може охоплювати адреси від 209.165.202.5 до 209.165.202.30. Цей діапазон буде використовуватись для трансляції внутрішніх адрес у публічні під час доступу до Інтернету і навпаки.

Переглянемо налаштування NAT на рисунку 3.6.

```
ip nat pool Internet 209.165.200.6 209.165.200.30 netmask 255.255.255.224
ip nat inside source list NAT12 pool Internet
ip nat inside source static 172.24.169.120 209.165.200.3
ip nat inside source static 172.24.169.146 209.165.200.4
ip nat inside source static 172.24.169.121 209.165.200.5
ip classless
!
ip flow-export version 9
!
!
ip access-list extended NAT15
 deny ip 172.24.168.0 0.0.0.127 172.24.169.160 0.0.0.15
 deny ip 172.24.168.128 0.0.0.127 172.24.169.160 0.0.0.15
 deny ip 172.24.169.0 0.0.0.127 172.24.169.160 0.0.0.15
 deny ip 172.24.169.128 0.0.0.31 172.24.169.160 0.0.0.15
 deny ip 172.15.168.0 0.0.0.255 172.24.169.160 0.0.0.15
 permit ip 172.24.168.0 0.0.0.127 any
 permit ip 172.24.168.128 0.0.0.127 any
 permit ip 172.24.169.0 0.0.0.127 any
 permit ip 172.24.169.128 0.0.0.31 any
 permit ip 172.15.168.0 0.0.0.255 any
```

Рисунок 3.6 – Налаштований NAT

3.5 Налаштування мереж VLAN, маршрутизації між VLAN

Технологія VLAN (Virtual Local Area Network) дозволяє логічно розділити одну фізичну мережу на кілька віртуальних підмереж, які функціонують незалежно одна від одної. Це дає змогу ефективно керувати трафіком відповідно до потреб різних груп користувачів або пристроїв у мережі. Кожна VLAN має свої власні правила доступу та політики безпеки, що забезпечує високий рівень захисту всієї мережі.

Однією з основних переваг використання VLAN є зменшення необхідності у фізичному розташуванні пристроїв та кабелів. Замість того, щоб створювати окремі фізичні мережні сегменти для кожної групи користувачів, VLAN дозволяє логічно розділити мережу, спрощуючи її управління та обслуговування. Це також

знижує витрати на обладнання та кабелі. Крім того, VLAN підвищує безпеку мережі, ізолюючи трафік між різними групами користувачів, що зменшує ризик несанкціонованого доступу до чутливої інформації та можливість внутрішніх атак. Таким чином, використання VLAN є важливим аспектом для покращення ефективності, безпеки та контролю в сучасних комп'ютерних мережах.

Таблиця 3.3 – Адресація мереж VLAN

Назва	Мережева адреса	Маска
VLAN10	172.24.169.136	/30
VLAN20	172.24.169.140	/30
VLAN30	172.24.169.144	/30
VLAN99	172.24.169.128	/30

Налаштування VLAN на прикладі комутатора наведено на рисунку 3.7.

```
int range fa0/5-10
switchport mode access
switchport access vlan 10
int range fa0/11-16
switchport mode access
switchport access vlan 20
int range fa0/17-24
switchport mode access
switchport access vlan 30
int range fa0/1-4
switchport mode trunk
switchport trunk native vlan 100
switchport trunk allowed vlan 42,22,32,99-100
int vlan 99
ip address 172.24.169.129 255.255.255.252
ip default-gateway 172.24.169.140
```

Рисунок 3.7 – Налаштування на комутаторі

```
int g0/1.10
encapsulation dot1Q 10
ip address 172.24.169.136 255.255.255.252
int g0/1.20
encapsulation dot1Q 20
ip address 172.24.169.140  255.255.255.252
int g0/1.30
encapsulation dot1Q 30
ip address 172.24.169.144 255.255.255.252
int g0/1.99
encapsulation dot1Q 99
ip address 172.24.169.129 255.255.255.252
```

Рисунок 3.8 – Налаштування віртуальних інтерфейсів

```
.
ip dhcp excluded-address 172.24.169.136
ip dhcp excluded-address 172.24.169.141
ip dhcp excluded-address 172.24.169.145
!
ip dhcp pool LAN3-VLAN10
 network 172.24.169.136 255.255.255.252
 default-router 172.24.169.137
 dns-server 172.24.169.120
ip dhcp pool LAN3-VLAN20
 network 172.24.169.140 255.255.255.252
 default-router 172.24.169.141
 dns-server 172.24.169.120
ip dhcp pool LAN3-VLAN30
 network 172.24.169.144 255.255.255.252
 default-router 172.24.169.145
 dns-server 172.24.169.120
!
```

Рисунок 3.9 – DHCP для VLAN

3.6 Налаштування віртуальної приватної мережі VPN

VPN (Virtual Private Network) - це технологія, яка забезпечує безпечне тунелювання даних через незахищені мережі, такі як Інтернет. Використовуючи VPN, інформація передається через зашифроване з'єднання, що гарантує конфіденційність і цілісність даних між вузлами мережі. У нашому випадку VPN буде використовуватися для безпечного підключення віддалених мереж до основної корпоративної мережі, забезпечуючи захист даних під час їх передачі.

Окрім захисту даних, VPN дозволяє створювати з'єднання між віддаленими мережами або пристроями, які знаходяться в різних географічних регіонах. Це робить VPN ідеальним рішенням для організацій з розподіленими командами або філіями, які потребують безпечного зв'язку між своїми мережами. Важливо належним чином налаштувати та керувати доступом до мережевих ресурсів, включаючи аутентифікацію користувачів, контроль доступу та моніторинг активності, щоб забезпечити безпеку та прозорість використання мережевих ресурсів.

Налаштування VPN розглянемо наведено на рисунку 3.10.

```
license boot module c2900 technology-package securityk9
ip access-list extended VPN12
permit ip 172.24.168.0 0.0.0.127
permit ip 172.24.168.128 0.0.0.127
permit ip 172.24.169.0 0.0.0.127
permit ip 172.24.169.128 0.0.0.31
permit ip 172.15.168.0 0.0.0.255
crypto isakmp policy 10
encr 3des
hash md5
authentication pre-share
group 2
crypto isakmp key cisco address 209.165.202.1
crypto ipsec transform-set TS esp-3des esp-md5-hmac
crypto map MAP 10 ipsec-isakmp
set peer 209.165.202.1
set transform-set TS
match address VPN12
int GigabitEthernet0/1
crypto map MAP
```

Рисунок 3.10 – Налаштування VPN

3.7 Налаштування маршрутизаторів на підтримку служби AAA

Модель AAA (Authentication, Authorization, and Accounting) використовується для управління доступом і контролю над мережевими ресурсами. Ця модель включає процеси аутентифікації (перевірка особи користувача), авторизації (визначення прав доступу користувача) та обліку (реєстрація дій користувача). Використання AAA дозволяє організаціям встановлювати політики доступу, що забезпечує контроль над тим, хто може отримати доступ до мережевих ресурсів і як ці ресурси можуть бути використані.

Ключовим компонентом моделі AAA є RADIUS-сервер (Remote Authentication Dial-In User Service), який забезпечує централізовану аутентифікацію та авторизацію користувачів. RADIUS-сервер перевіряє ідентифікаційні дані користувачів та визначає їх права доступу на основі заданих політик безпеки. Це гарантує, що тільки авторизовані користувачі можуть отримати доступ до мережевих ресурсів, відповідно до встановлених правил.

Важливим аспектом моделі AAA є облік, який дозволяє вести детальний журнал активності користувачів у мережі. Цей журнал включає інформацію про входи, використані ресурси та час, проведений у мережі. Завдяки обліку можна

не лише відслідковувати дії користувачів, але й виявляти можливі проблеми безпеки або порушення політик мережі. Використання моделі AAA з RADIUS-сервером дозволяє організаціям забезпечити високий рівень безпеки та контролю доступу до мережевих ресурсів, що особливо важливо для розподілених мереж або великих користувацьких баз.

3.8 Перевірка комп'ютерної Системи підприємства

Проведено перевірку базових налаштувань обладнання, використовуючи маршрутизатор Sidorenko_R2 як приклад. За допомогою команди show running-config у привілейованому режимі були проаналізовані кілька параметрів, включаючи ім'я пристрою, налаштування паролів для доступу до консолі та ліній vty, їх конфігурацію для використання протоколу SSH, пароль для доступу до привілейованого режиму, налаштування банера MOTD та ім'я домену.

Цей аналіз дозволяє переконатися, що всі базові налаштування маршрутизатора відповідають вимогам безпеки та функціональності мережі. Наприклад, перевірка правильності налаштування паролів і використання SSH для віддаленого доступу забезпечує захищений доступ до мережевого обладнання, тоді як налаштування банера MOTD та доменного імені сприяють кращій ідентифікації пристроїв та зручності управління мережею.

```
hostname Sidorenko_R2
```

Рисунок 3.11 – Назва пристрою

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

Рисунок 3.12 – Пароль до консольного режиму

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

Рисунок 3.13 – Пароль до ліній vty та використання на них протоколу ssh

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

Рисунок 3.14 – Пароль до привілейованого режиму

```
banner motd ^CSidorenko_R2^C
```

Рисунок 3.15 – Банер MOTD

```
ip domain-name Sidorenko_R2
!
```

Рисунок 3.16 – Ім’я домена

```
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 3.17 – Технологія EtherChannel

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

Рисунок 3.18 – Налаштований OSPF

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

Рисунок 3.19 – Зв’язок між LAN_4 та LAN_5

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

Рисунок 3.20 – Налаштований маршрут за замовчуванням на маршрутизаторі

```
User Access Verification

Username: sidorenko
Password:
Sidorenko_R2>
```

Рисунок 3.21 – Налаштований маршрутизатор на підтримку служби AAA

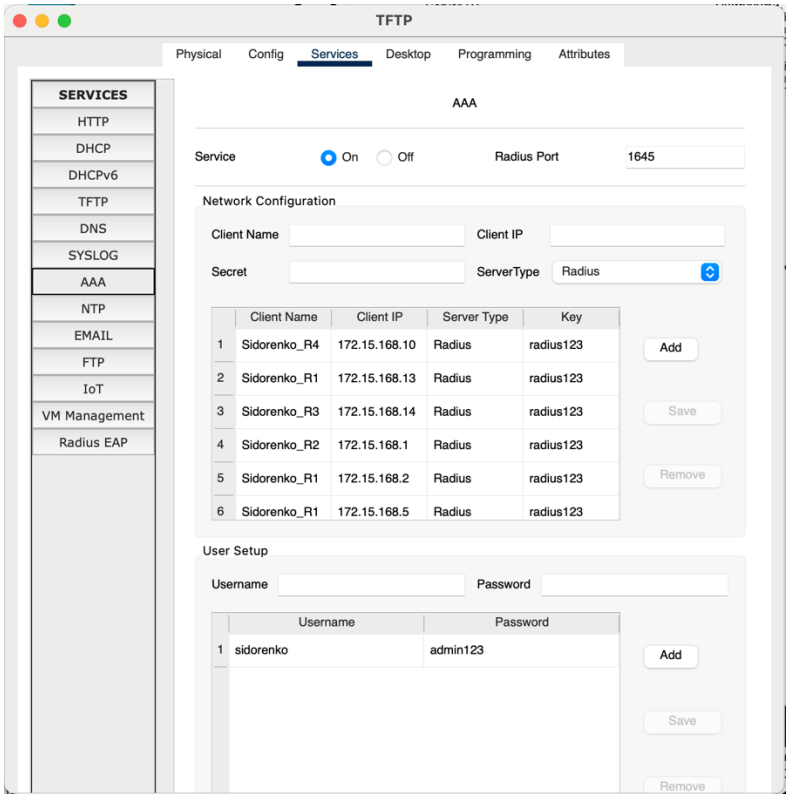

Рисунок 3.22 – Налаштування RADIUS-сервера

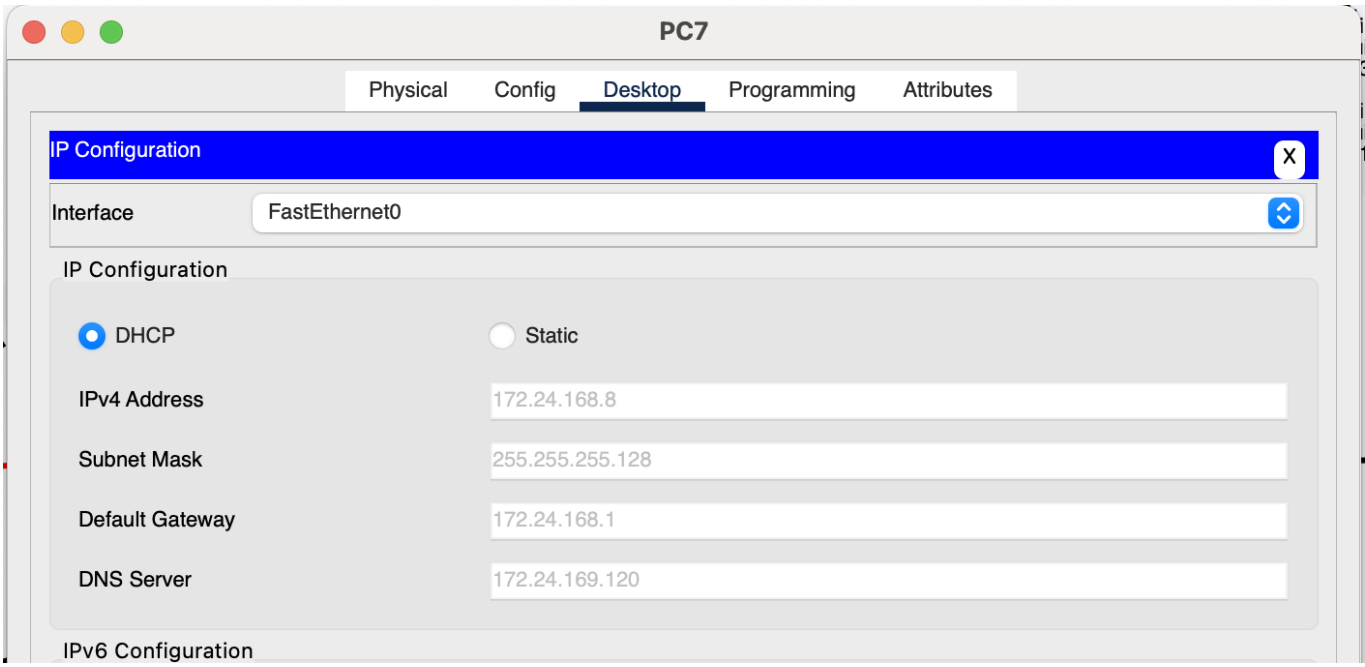

Рисунок 3.23 – IP-адреса PC4

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

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

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------

Remote SPAN VLANs
------------------------------------------------------------------------------

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
```

Рисунок 3.24 – Імена та порти VLAN

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

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

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

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

Рисунок 3.25 – Транкові порти

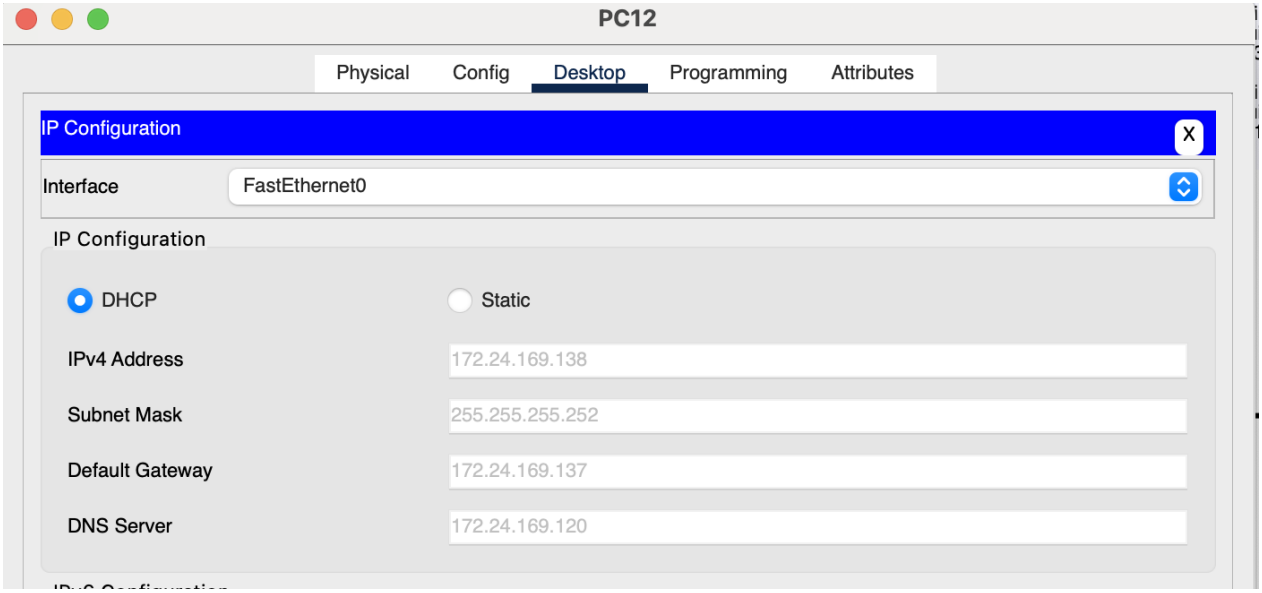

Рисунок 3.26 – IP-адреса PC12

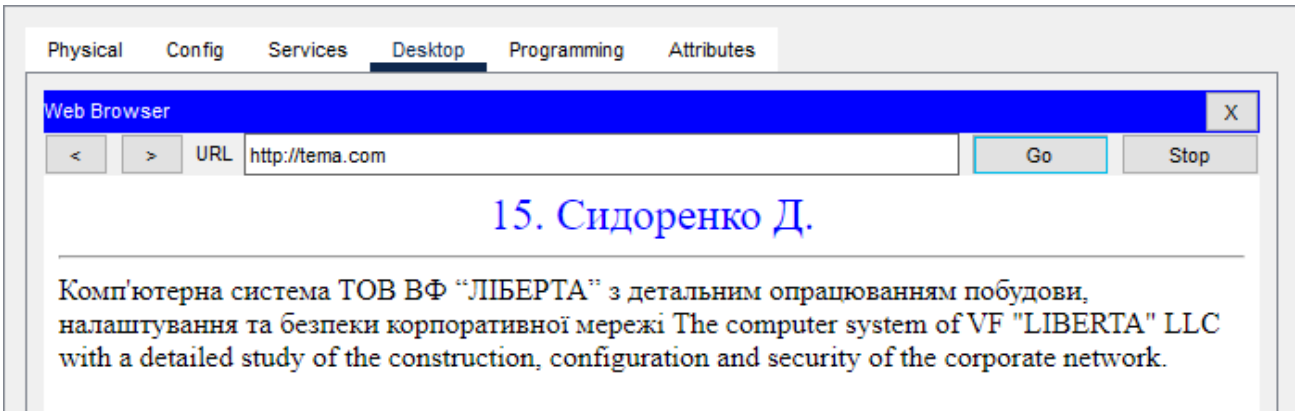

Рисунок 3.27 – Сайт з темою та призвіщем

4 РОЗРОБКА КОМПОНЕНТА СИСТЕМИ

4.1 Інженерне рішення по розробці компонента Системи

При проектуванні корпоративної мережі особлива увага була приділена розробці компонентів IoT-системи, яка забезпечує контроль клімату у певних підмережах. Ця система покликана підтримувати оптимальні умови для роботи співробітників та функціонування обладнання. Додатково, впроваджено систему пожежогасіння аргоновим газом для підмереж, де розташоване серверне обладнання, що дозволяє забезпечити високий рівень захисту та збереження серверів у випадку пожежі.

Основною метою IoT-компонента є автоматизація процесів регулювання температури та вологості для забезпечення комфорту користувачів та безперебійної роботи обладнання. Система сповіщує персонал про можливі загрози за допомогою інтегрованих засобів сигналізації. Це знижує ризик пошкодження обладнання та забезпечує своєчасну реакцію на аварійні ситуації.

Система реалізована з використанням сучасних технологій моніторингу навколишнього середовища, які включають датчики температури, кондиціонери, опалювальне обладнання та зволожувачі повітря. Всі ці компоненти працюють у тісній взаємодії для постійного моніторингу і оперативного реагування на зміну температурних показників, що гарантує стабільність умов у приміщеннях.

IoT-система інтегрована в локальну мережу компанії та використовує сучасні протоколи передачі даних для забезпечення надійної та ефективної роботи. Завдяки застосуванню IoT-технологій створено розумну систему, яка автоматично адаптується до змін зовнішніх умов та забезпечує комфортне середовище без потреби у втручанні користувачів. Це не тільки підвищує ефективність роботи, але й знижує експлуатаційні витрати на обслуговування кліматичних систем.

4.2 Налаштування обладнання та сервісів системи IoT

Для створення IoT-системи офісу, перш за все, встановлюються IoT-пристрої та датчики, які підключаються до Home Gateway. Ці датчики відповідають за збір і передачу даних про стан навколишнього середовища та інших параметрів, необхідних для функціонування системи.

На Home Gateway мережі налаштовується бездротова точка доступу. У цьому прикладі використовується мережа LAN4 з SSID «Sidorenko_Gateway_LAN4» та паролем «Sidorenko_12321ck1_LAN4». Для забезпечення безпеки мережі застосовується протокол WPA2-PSK з методом шифрування AES. Це забезпечує високий рівень захисту переданих даних та захищає мережу від несанкціонованого доступу.

Кожен IoT-пристрій налаштовується для підключення до Home Gateway, де вводяться відповідні SSID та пароль. Це дозволяє пристроям взаємодіяти з мережею та передавати дані до центрального сервера. В якості IoT-сервера використовується сервер з IP-адресою «172.24.169.120», який приймає і обробляє дані від усіх IoT-пристроїв у мережі.

Топологічна схема корпоративної мережі офісу з розміщенням IoT-пристроїв детально представлена на рисунку 4.4. На цій схемі відображено, як пристрої інтегруються у загальну мережеву інфраструктуру, забезпечуючи надійну та ефективну роботу IoT-системи. Ця схема також допомагає візуалізувати взаємозв’язок між різними компонентами мережі, що є критично важливим для її належного функціонування та обслуговування.

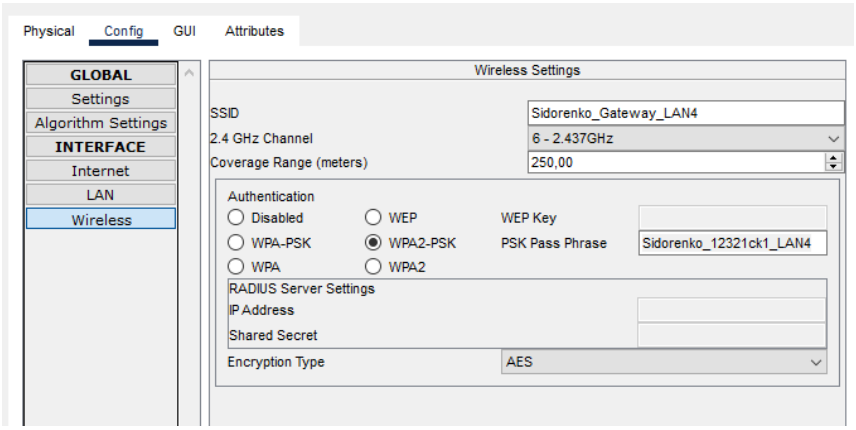

Рисунок 4.1 – Бездротова мережа

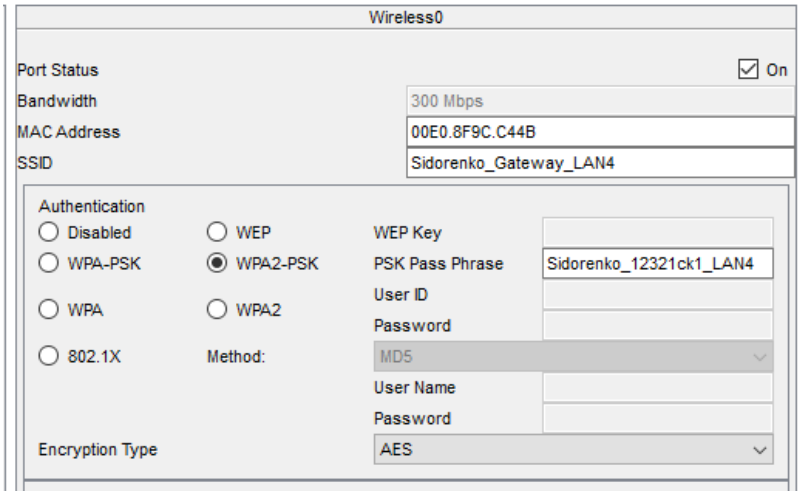

Рисунок 4.2 – Бездротова мережа на пристроях

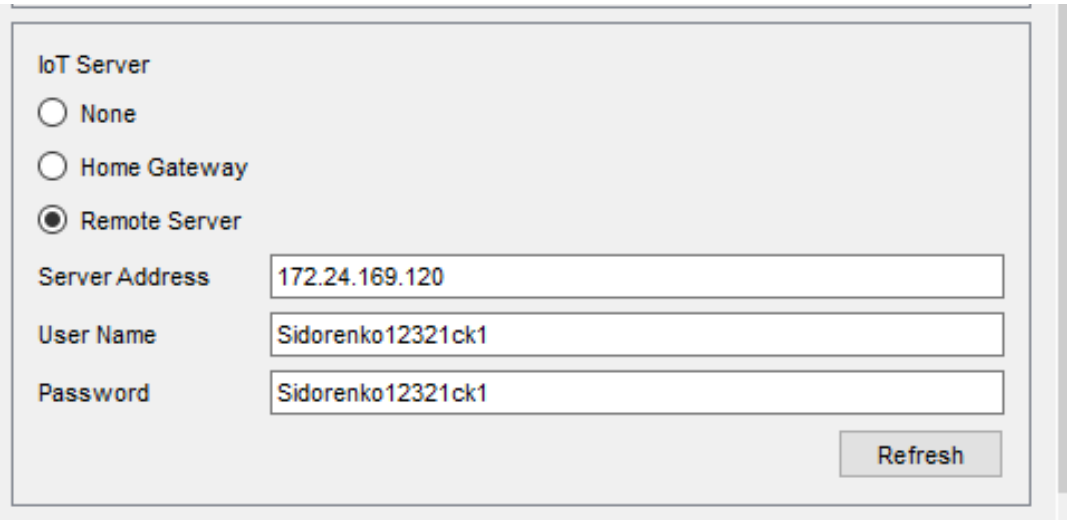

Рисунок 4.2 – Налаштування підключення до віддаленого серверу

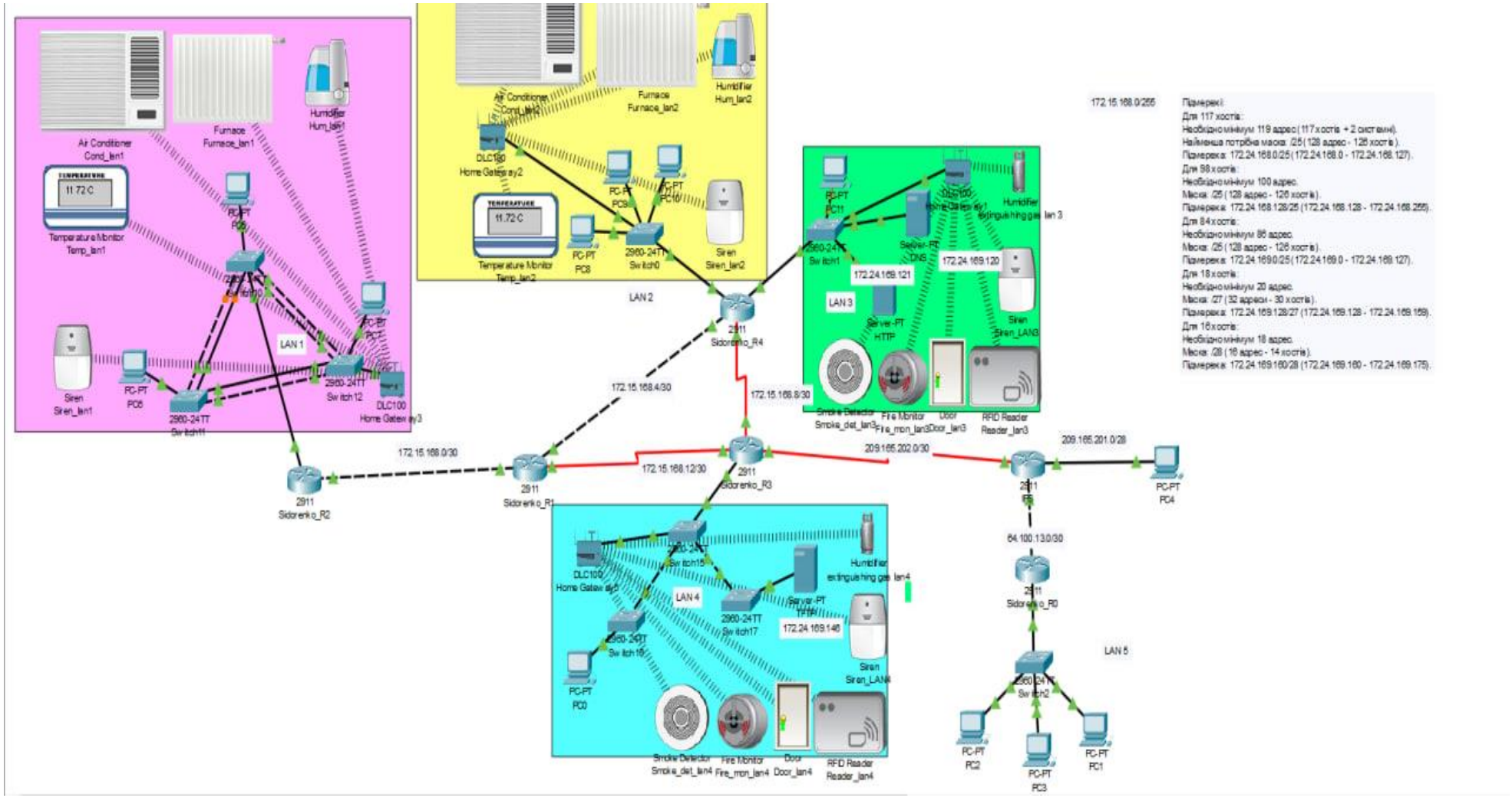

Рисунок 4.4 – Топологічна схема корпоративної мережі компанії з розміщенням IoT пристроїв

Для налаштування умов роботи IoT-системи в будь-якому вузлі мережі відкриваємо програму IoT Monitor, вводимо адресу шлюзу, логін та пароль. Після успішного входу відкривається сторінка з переліком усіх підключених IoT-пристроїв, як показано на рисунку 4.2. Ця сторінка дозволяє користувачу бачити поточний статус кожного пристрою та здійснювати необхідні налаштування.

Переходимо на вкладку «Conditions» та натискаємо «Add» для додавання умов спрацювання пристроїв. Для активації сирен потрібні умови у випадку виявлення диму або вогню у підмережі 3 або 4 у будь-якій з них. При активації цих датчиків, в підмережі, де виявлено загрозу, автоматично вмикається пристрій для вивільнення безпечного газу для пожежогасіння. Коли датчики фіксують, що загроза минула, сирена вимикається, і система повертається до нормального режиму роботи.

Для налаштування кліматичних сценаріїв система працює наступним чином: якщо температура в приміщенні перевищує 25 градусів, вмикається кондиціонер. При температурі від 20 до 25 градусів система залишається неактивною, оскільки це оптимальний температурний діапазон. Якщо температура падає нижче 20 градусів, автоматично вмикається обігрівач та зволожувач повітря. Таким чином, IoT-система забезпечує комфортні умови для роботи в офісі, автоматично реагуючи на зміни температури.

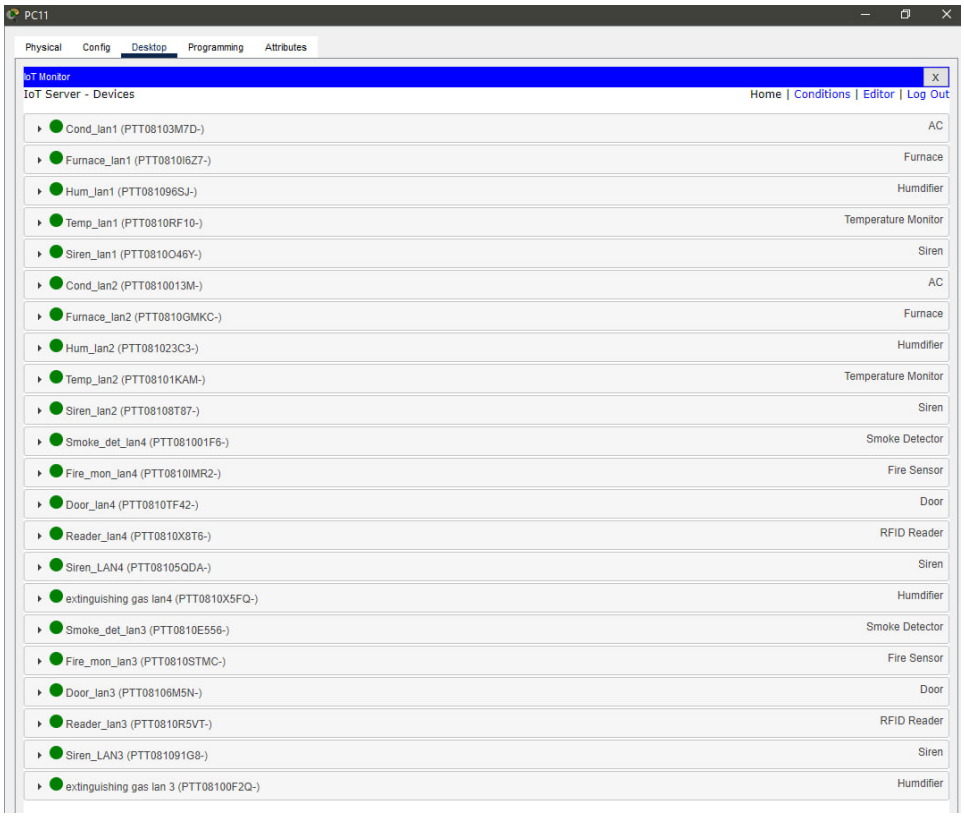

Рисунок 4.5 – Під’єднані IoT-пристрої

Actions	Enabled	Name	Condition	Actions
Edit Remove	Yes	Lan4_fire	Match any: • Smoke_det_lan4 Alarm is true • Fire_mon_lan4 Fire Detected is true	Set Siren_LAN4 On to true Set extinguishing gas lan4 Status to true Set Siren_LAN3 On to true Set Siren_lan1 On to true Set Siren_lan2 On to true
Edit Remove	Yes	Lan3_fire	Match any: • Smoke_det_lan3 Alarm is true • Fire_mon_lan3 Fire Detected is true	Set extinguishing gas lan 3 Status to true Set Siren_lan1 On to true Set Siren_lan2 On to true Set Siren_LAN4 On to true Set Siren_LAN3 On to true
Edit Remove	Yes	Siren_off	Match all: • Fire_mon_lan3 Fire Detected is false • Fire_mon_lan4 Fire Detected is false • Smoke_det_lan4 Alarm is false • Smoke_det_lan3 Alarm is false	Set Siren_lan1 On to false Set Siren_lan2 On to false Set Siren_LAN3 On to false Set Siren_LAN4 On to false Set extinguishing gas lan4 Status to false Set extinguishing gas lan 3 Status to false
Edit Remove	Yes	Door_LAN4_Open	Reader_lan4 Status is Valid	Set Door_lan4 Lock to Unlock
Edit Remove	Yes	Door_LAN3_Open	Reader_lan3 Status is Valid	Set Door_lan3 Lock to Unlock
Edit Remove	Yes	Door_LAN4_Close	Reader_lan4 Status is Waiting	Set Door_lan4 Lock to Lock
Edit Remove	Yes	Door_LAN3_Close	Reader_lan3 Status is Waiting	Set Door_lan3 Lock to Lock
Edit Remove	Yes	Reader_Valid_LAN3	Reader_lan3 Card ID = 3	Set Reader_lan3 Status to Valid
Edit Remove	Yes	Reader_Valid_LAN4	Reader_lan4 Card ID = 4	Set Reader_lan4 Status to Valid
Edit Remove	Yes	Temp_lan1_high	Temp_lan1 Temperature > 25.0 °C	Set Cond_lan1 On to true Set Hum_lan1 Status to false Set Furnace_lan1 On to false
Edit Remove	Yes	Temp_lan1_low	Temp_lan2 Temperature < 20.0 °C	Set Cond_lan1 On to false Set Furnace_lan1 On to true Set Hum_lan1 Status to true
Edit Remove	Yes	Temp_lan1_betw	Temp_lan1 Temperature is between 20.0 °C and 25.0 °C	Set Cond_lan1 On to false Set Hum_lan1 Status to false Set Furnace_lan1 On to false
Edit Remove	Yes	Temp_lan2_high	Temp_lan2 Temperature > 25.0 °C	Set Cond_lan2 On to true Set Hum_lan2 Status to false Set Furnace_lan2 On to false
Edit Remove	Yes	Temp_lan2_low	Temp_lan2 Temperature < 20.0 °C	Set Cond_lan2 On to false Set Furnace_lan2 On to true Set Hum_lan2 Status to true
Edit Remove	Yes	Temp_lan2_betw	Temp_lan2 Temperature is between 20.0 °C and 25.0 °C	Set Cond_lan2 On to false Set Hum_lan2 Status to false Set Furnace_lan2 On to false

Рисунок 4.6 – Розроблені сценарії

4.3 Перевірка роботи компонента Системи

Для перевірки роботи IoT-системи було налаштовано середовище Cisco Packet Tracer. У цьому середовищі було створено сценарії для періодичної зміни температури, а також додано елемент, що симулює задимленість. Це дозволяє перевірити, як система реагує на різні умови і чи відповідає її робота заданим параметрам.

Під час тестування системи при температурі нижчій за 25 градусів на рисунку 4.7, було проведено декілька експериментів для перевірки роботи кліматичних сценаріїв. При температурі нижче 20 градусів на рисунку 4.8 автоматично активується обігрівач та зволожувач повітря, що забезпечує комфортні умови в приміщенні. Якщо ж температура знаходиться в діапазоні від 20 до 25 градусів на рисунку 4.9, система залишається в неактивному стані, оскільки такі умови вважаються оптимальними для роботи. Крім того, додана симуляція задимленості дозволила перевірити, як система реагує на виявлення диму, активуючи відповідні тривожні сигнали та механізми пожежогасіння

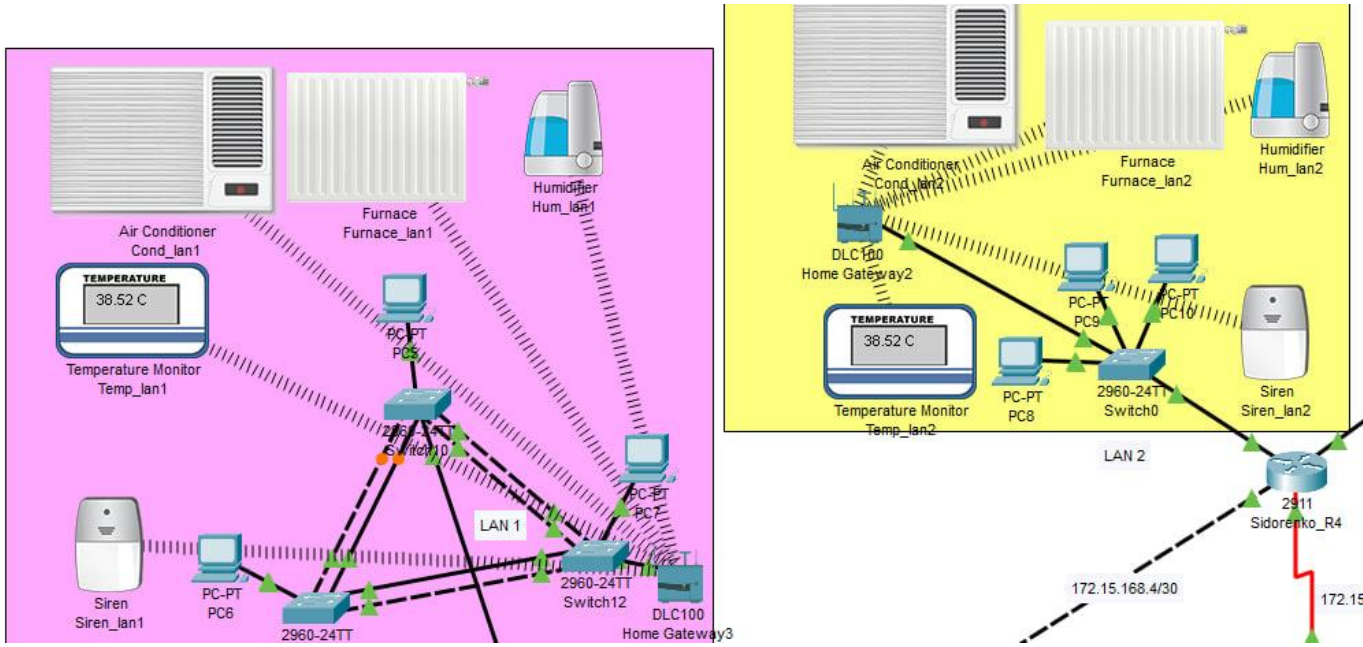

Рисунок 4.7 – Поведінка системи при температурі > 25

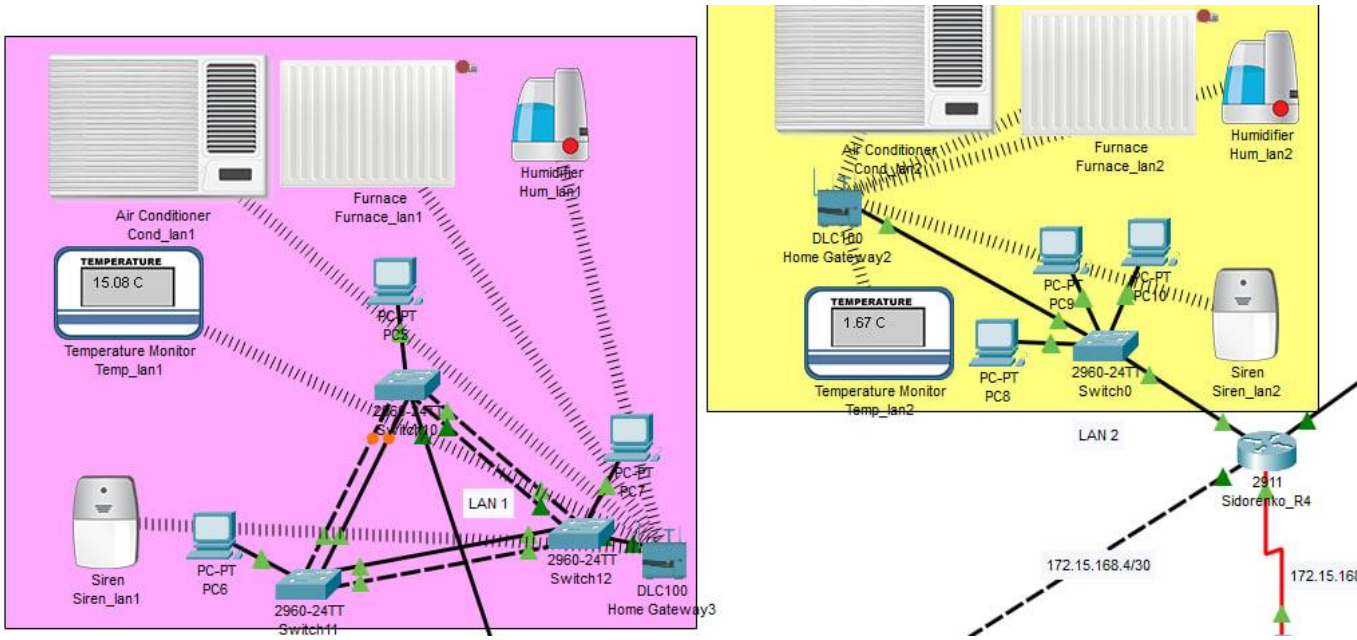

Рисунок 4.8 – Поведінка системи при температурі > 25

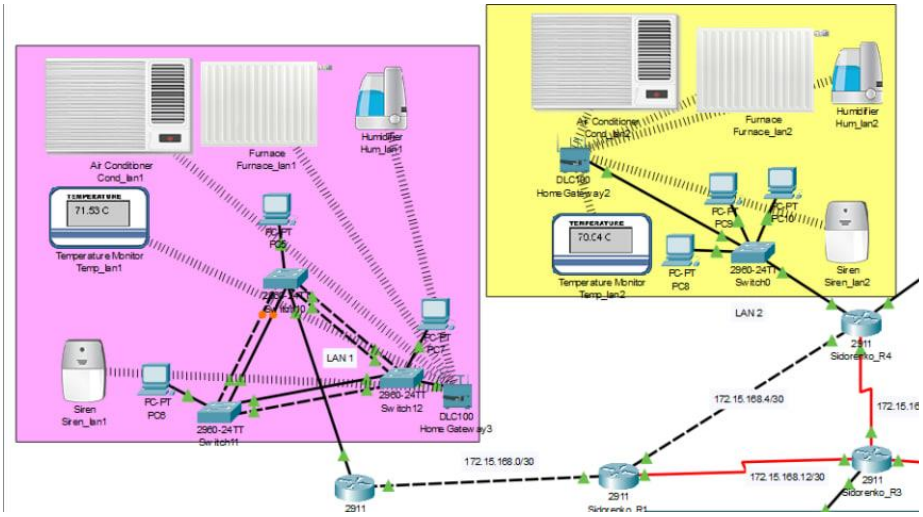

Рисунок 4.9 – Поведінка системи при температурі < 20

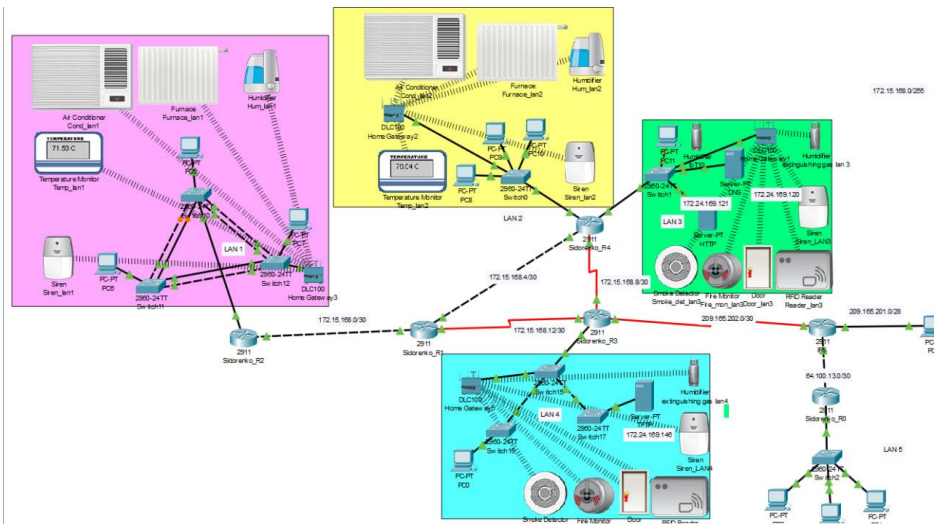

Рисунок 4.10 – Система у спокої

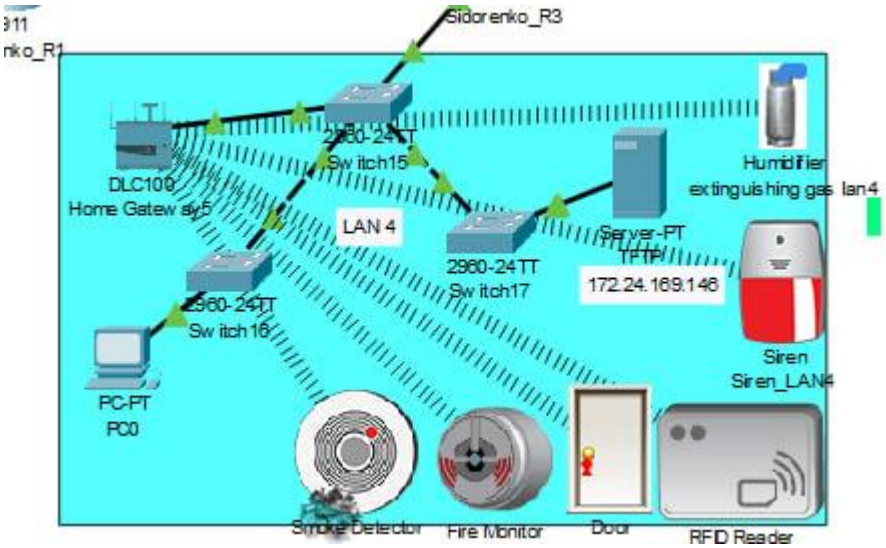

Рисунок 4.11 – Наявність диму у Lan4

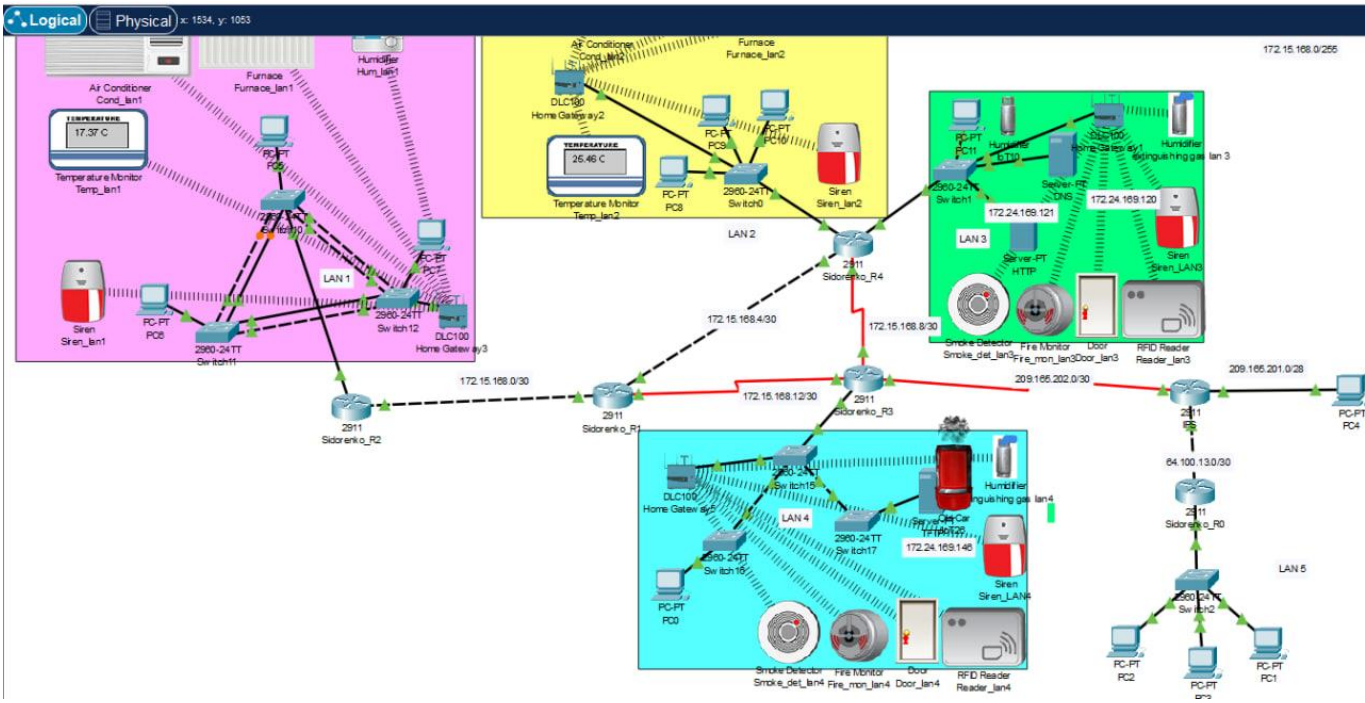

Рисунок 4.12 – Наявність диму у двох підмережах

Для перевірки доступу на прикладі підмережі 3 до зчитувача карток піднесено спочатку валідну та потім невалідну картку (рис. 4.13-14).

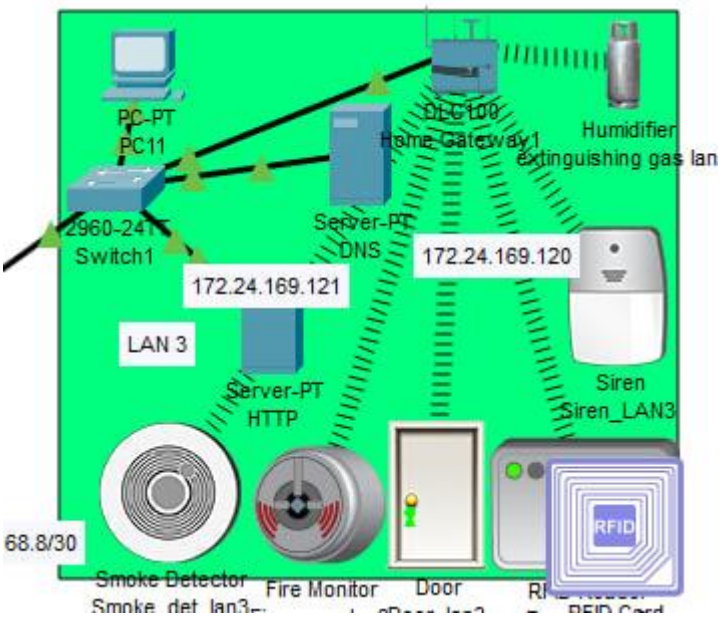

Рисунок 4.13 – Піднесення валідної картки

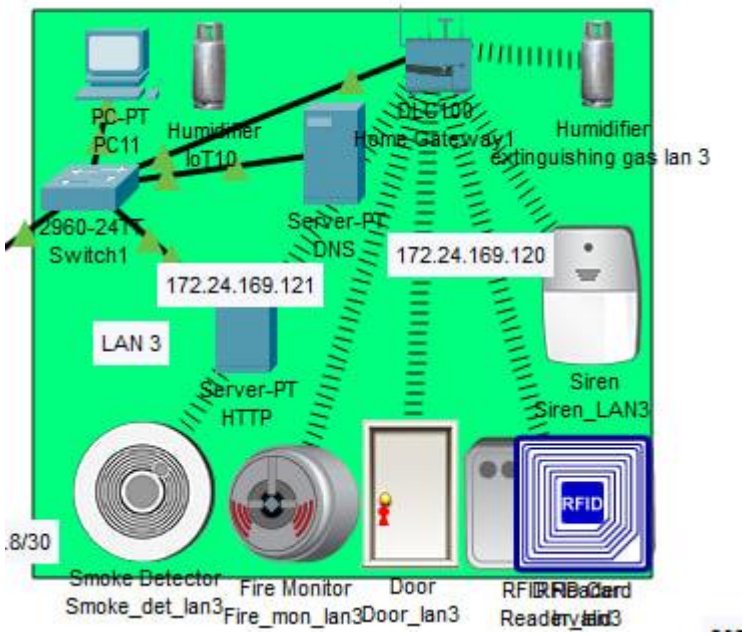

Рисунок 4.14 – Піднесення не валідної картки

ВИСНОВКИ

Детальне опрацювання конструкції, конфігурації та безпеки корпоративної мережі компанії ТОВ ВФ "ЛІБЕРТА" є важливим етапом у забезпеченні ефективної та безпечної роботи виробничого підприємства. Цей процес дозволяє виявити потенційні ризики та визначити шляхи їх мінімізації, а також покращити ефективність виробничих процесів.

Одним з ключових аспектів розгляду цієї теми є аналіз конструкції комп'ютерної системи, яка використовується на підприємстві. Ретельне вивчення архітектури системи дозволяє зрозуміти її потужності та обмеження, а також виявити можливості для оптимізації та покращення її продуктивності. Крім того, аналіз конфігурації та управління корпоративною мережею допомагає забезпечити стабільну та безперебійну роботу всіх пристроїв і зв'язків у мережі, що є важливим для нормального функціонування виробничого процесу.

Також для мережі інтегровано IoT системи пожаротушіння у серверних приміщеннях клімат контроль окремих зон та система доступу до кімнат з обладнанням.

Отже, детальне опрацювання конструкції, конфігурації та безпеки корпоративної мережі ТОВ ВФ "ЛІБЕРТА" є необхідним для забезпечення стабільної та ефективної роботи підприємства. Впровадження відповідних заходів та стратегій дозволить забезпечити надійність, безпеку та продуктивність комп'ютерної системи, що є ключовими факторами успіху у виробничому бізнесі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Методичні рекомендації до виконання кваліфікаційної роботи бакалавра студентами галузі знань 12 Інформаційні технології спеціальності 123 Комп’ютерна інженерія / Л.І. Цвіркун, С.М. Ткаченко, Я.В. Панферова, Д.О. Бешта, Л.В. Бешта. – Д.: НТУ «ДП», 2024. – 62 с.

2. Cisco. Cisco Packet Tracer – Education [Електронний ресурс]. – Режим доступу до ресурсу: https://www.netacad.com/courses/packet-tracer (дата звернення 1.06.2024р.)

3. Бачинський, А. І. Мережеві технології та інтернет речей (IoT). Київ: Техніка, 2018. – 224 с.

4. Степаненко, О. В. Інформаційна безпека корпоративних мереж. Харків: ХНУРЕ, 2019. – 320 с.

5. Лемешко, В. М. Моделювання та аналіз комп'ютерних мереж у Cisco Packet Tracer. Одеса: ОНПУ, 2020. – 188 с.

6. Інтернет речей: базові концепції – Education [Електронний ресурс]. – Режим доступу до ресурсу: http://surl.li/jfsrq (дата звернення 3.06.2024р.)

7. Налаштування безпеки в IoT – Education [Електронний ресурс]. – Режим доступу до ресурсу: http://surl.li/jfsrr (дата звернення 3.06.2024р.)

8. Проектування корпоративних мереж – Education [Електронний ресурс]. – Режим доступу до ресурсу: http://surl.li/jfsrt (дата звернення 3.06.2024р.)

9. Розгортання IoT в корпоративних середовищах – Education [Електронний ресурс]. – Режим доступу до ресурсу: http://surl.li/jfsrv (дата звернення 5.06.2024р.)

10. Моделювання мереж у Cisco Packet Tracer – Education [Електронний ресурс]. – Режим доступу до ресурсу: http://surl.li/jfsrw (дата звернення 6.06.2024р.)

11. Інтеграція IoT у корпоративну мережу – Education [Електронний ресурс]. – Режим доступу до ресурсу: http://surl.li/jfsrx (дата звернення 6.06.2024р.)

ДОДАТОК А

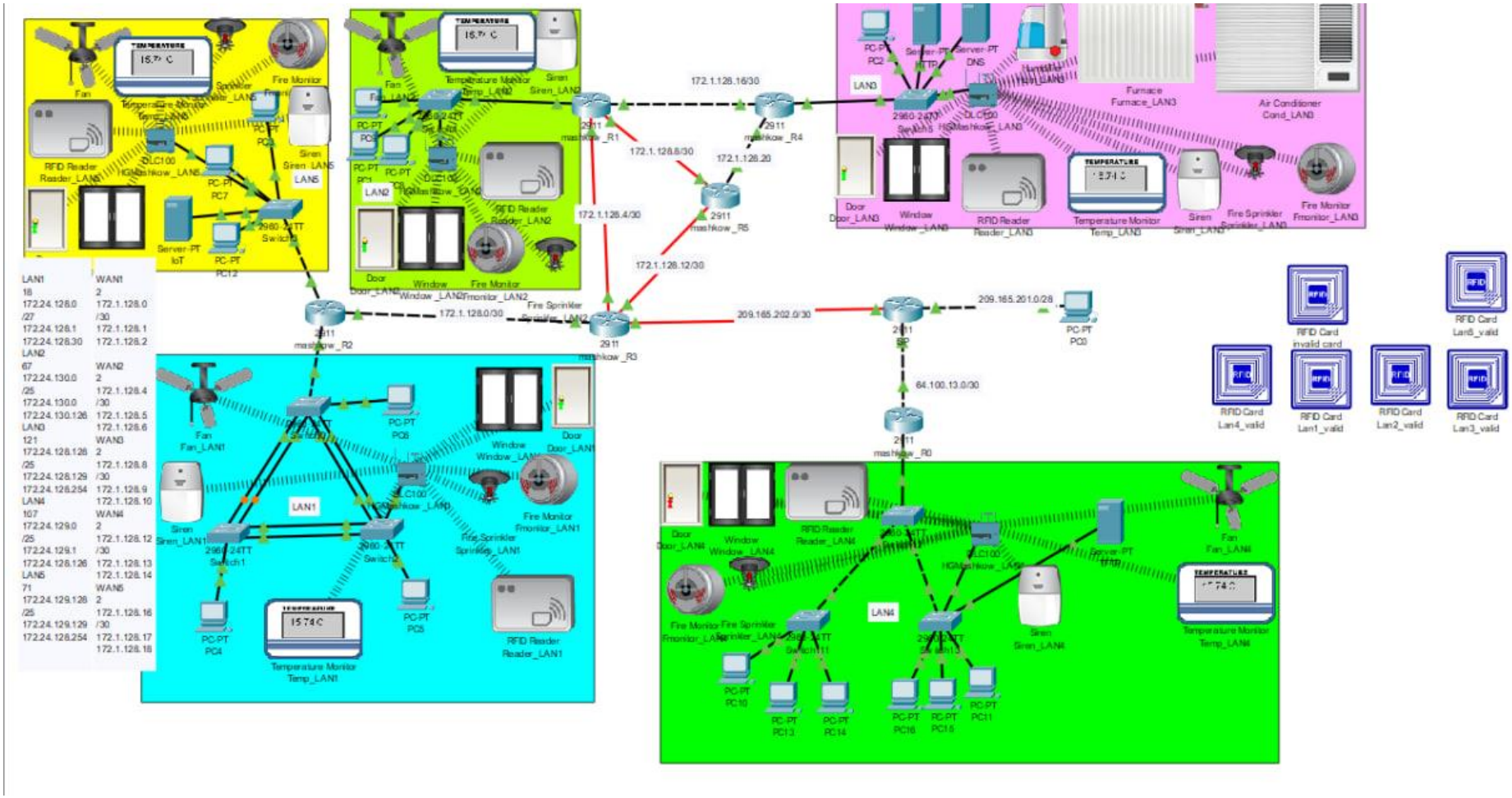

Рисунок ДА.1 – Загальна архітектура мережі

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

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ НАЛАШТУВАННЯ МЕРЕЖІ КОМП’ЮТЕРНОЇ СИСТЕМИ

Текст програми налаштування пристроїв

804.02070743.24015-01 12 01

Листів 16

2024

АНОТАЦІЯ

Ця програма включає команди для конфігурації маршрутизаторів і комутаторів у корпоративній мережі. Команди призначені для налаштування IP-адрес, базової конфігурації пристроїв, налаштування DHCP, NAT, VPN, AAA, OSPF, VLAN, статичних маршрутів, EtherChannel та безпеки портів.

ЗМІСТ

1. Sidorenko_R3

```
Building configuration...

Current configuration : 3875 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Sidorenko_R3
!
!
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
!
ip dhcp excluded-address 172.24.169.136
ip dhcp excluded-address 172.24.169.141
ip dhcp excluded-address 172.24.169.145
!
ip dhcp pool LAN3-VLAN10
network 172.24.169.136 255.255.255.252
default-router 172.24.169.137
dns-server 172.24.169.120
ip dhcp pool LAN3-VLAN20
network 172.24.169.140 255.255.255.252
default-router 172.24.169.141
dns-server 172.24.169.120
ip dhcp pool LAN3-VLAN30
network 172.24.169.144 255.255.255.252
default-router 172.24.169.145
dns-server 172.24.169.120
!
!
aaa new-model
!
aaa authentication login console group radius local
aaa authentication login default local
!
!
!
!
!
!
!
no ip cef
no ipv6 cef
!
```

```
!
!
username Sidorenko password 7 082048430017544541
!
!
license udi pid CISCO2911/K9 sn FTX15246W94-
!
!
!
!
!
!
!
!
!
ip domain-name Sidorenko_R3
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface GigabitEthernet0/0
no ip address
ip nat inside
duplex auto
speed auto
!
interface GigabitEthernet0/0.10
encapsulation dot1Q 10
ip address 172.24.169.137 255.255.255.252
!
interface GigabitEthernet0/0.20
encapsulation dot1Q 20
ip address 172.24.169.141 255.255.255.252
!
interface GigabitEthernet0/0.30
encapsulation dot1Q 30
ip address 172.24.169.145 255.255.255.252
!
interface GigabitEthernet0/0.99
encapsulation dot1Q 99
ip address 172.24.169.129 255.255.255.248
!
interface GigabitEthernet0/1
no ip address
duplex auto
```

```
speed auto
shutdown
!
interface GigabitEthernet0/2
no ip address
duplex auto
speed auto
shutdown
!
interface Serial0/0/0
ip address 209.165.202.1 255.255.255.252
ip nat outside
!
interface Serial0/0/1
ip address 172.15.168.14 255.255.255.252
ip nat inside
!
interface Serial0/1/0
ip address 172.15.168.9 255.255.255.252
ip nat inside
!
interface Serial0/1/1
no ip address
clock rate 2000000
shutdown
!
interface Vlan1
no ip address
shutdown
!
router ospf 1
log-adjacency-changes
passive-interface default
no passive-interface GigabitEthernet0/0
no passive-interface Serial0/0/0
no passive-interface Serial0/0/1
no passive-interface Serial0/1/0
auto-cost reference-bandwidth 1000
network 172.15.168.12 0.0.0.3 area 0
network 209.165.202.0 0.0.0.3 area 0
network 172.15.168.8 0.0.0.3 area 0
network 172.24.169.136 0.0.0.3 area 0
network 172.24.169.140 0.0.0.3 area 0
network 172.24.169.144 0.0.0.3 area 0
network 172.24.169.128 0.0.0.7 area 0
!
ip nat pool Internet 209.165.200.6 209.165.200.30 netmask 255.255.255.224
ip nat inside source list NAT12 pool Internet
ip nat inside source static 172.24.169.120 209.165.200.3
ip nat inside source static 172.24.169.146 209.165.200.4
```

```
ip nat inside source static 172.24.169.121 209.165.200.5
ip classless
!
ip flow-export version 9
!
!
ip access-list extended NAT15
deny ip 172.24.168.0 0.0.0.127 172.24.169.160 0.0.0.15
deny ip 172.24.168.128 0.0.0.127 172.24.169.160 0.0.0.15
deny ip 172.24.169.0 0.0.0.127 172.24.169.160 0.0.0.15
deny ip 172.24.169.128 0.0.0.31 172.24.169.160 0.0.0.15
deny ip 172.15.168.0 0.0.0.255 172.24.169.160 0.0.0.15
permit ip 172.24.168.0 0.0.0.127 any
permit ip 172.24.168.128 0.0.0.127 any
permit ip 172.24.169.0 0.0.0.127 any
permit ip 172.24.169.128 0.0.0.31 any
permit ip 172.15.168.0 0.0.0.255 any
!
banner motd ^CSidorenko_R3^C
!
radius server host
address ipv4 172.24.169.146 auth-port 1645
key radius123
radius server 172.24.169.146
address ipv4 172.24.169.146 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. Sidorenko_R2

```
Sidorenko_R2#show run
Building configuration...

Current configuration : 1804 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Sidorenko_R2
!
!
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
!
ip dhcp excluded-address 172.24.168.1 172.24.168.5
!
ip dhcp pool LAN-1
network 172.24.168.0 255.255.255.128
default-router 172.24.168.1
dns-server 172.24.169.120
!
!
aaa new-model
!
aaa authentication login console group radius local
aaa authentication login default local
!
!
!
!
!
!
!
ip cef
no ipv6 cef
!
!
!
username Sidorenko password 7 082048430017544541
!
!
license udi pid CISCO2911/K9 sn FTX15247V16-
!
!
!
```

```
!
!
!
!
!
!
ip domain-name Sidorenko_R2
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface GigabitEthernet0/0
ip address 172.24.168.1 255.255.255.128
duplex auto
speed auto
!
interface GigabitEthernet0/1
ip address 172.15.168.1 255.255.255.252
duplex auto
speed auto
!
interface GigabitEthernet0/2
no ip address
duplex auto
speed auto
shutdown
!
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
auto-cost reference-bandwidth 1000
network 172.24.168.0 0.0.0.127 area 0
network 172.15.168.0 0.0.0.3 area 0
!
ip classless
!
ip flow-export version 9
!
!
```

```
!
banner motd ^CSidorenko_R2^C
!
radius server host
address ipv4 172.24.169.146 auth-port 1645
key radius123
radius server 172.24.169.146
address ipv4 172.24.169.146 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. Sidorenko_R1

```
Sidorenko_R1#show run

Building configuration...

Current configuration : 1867 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Sidorenko_R1
!
!
!
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 Sidorenko password 7 082048430017544541
!
!
license udi pid CISCO2911/K9 sn FTX1524CQ21-
!
!
!
!
!
!
!
!
!
ip domain-name Sidorenko_R1
!
!
spanning-tree mode pvst
!
!
!
!
!
!
!
interface GigabitEthernet0/0
ip address 172.15.168.5 255.255.255.252
duplex auto
speed auto
!
interface GigabitEthernet0/1
```

```
ip address 172.15.168.2 255.255.255.252
duplex auto
speed auto
!
interface GigabitEthernet0/2
no ip address
duplex auto
speed auto
shutdown
!
interface Serial0/0/0
no ip address
clock rate 2000000
shutdown
!
interface Serial0/0/1
ip address 172.15.168.13 255.255.255.252
clock rate 128000
!
interface Vlan1
no ip address
shutdown
!
router ospf 1
log-adjacency-changes
passive-interface default
no passive-interface GigabitEthernet0/0
no passive-interface GigabitEthernet0/1
no passive-interface Serial0/0/1
auto-cost reference-bandwidth 1000
network 172.15.168.12 0.0.0.3 area 0
network 172.15.168.0 0.0.0.3 area 0
network 172.15.168.4 0.0.0.3 area 0
!
ip classless
!
ip flow-export version 9
!
!
!
banner motd ^CSidorenko_R1^C
!
radius server host
address ipv4 172.24.169.146 auth-port 1645
key radius123
radius server 172.24.169.146
address ipv4 172.24.169.146 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
```