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 Руденка Володимира Володимировича
(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 «ПАНТАЗІЇВСЬКЕ» з детальним опрацюванням побудови та налаштування корпоративної мережі»
(назва за наказом ректора)

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи				
спеціальної частини	Доц. Шедловський І.А			
розділів:				
розробка апаратної частини	Доц. Бешта Д.О			
розробка корпоративної мережі	Ас. Панфьорова 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 Руденка Володимира Володимировича **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 «ПАНТАЗІЇВСЬКЕ» з детальним опрацюванням побудови та налаштування 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 обгрунтувати необхідність модернізації комп'ютерної системи ТОВ «ПАНТАЗІЇВСЬКЕ» з детальною розробкою комп'ютерної мережі.*	15.03.2024
Розробка апаратної частини	*На основі аналізу особливостей і потреб підприємства сформулювати технічні вимоги до розробки комп'ютерної мережі*	04.04.2024
Розробка корпоративної мереж	*Побудувати в Packet Tracer модель корпоративної мережі компанії, виконати налаштування та перевірку роботи системи*	15.05.2024
Розробка компонента системи	*Розробити систему безпеки*	30.05.2024

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

Дата видачі _____

Дата подання до екзаменаційної комісії 04.06.24

Прийнято до виконання _____ Руденко В.В
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 65 с., 40 рис., 4 табл., 1 додатки, 10 джерел.

КОМП’ЮТЕРНА СИСТЕМА, ІНТЕРНЕТ РЕЧЕЙ, МАРШРУТИЗАТОР, КОМУТАТОР, CISCO, CISCO PACKET TRACER, NAT, VPN, DHCP, VLAN.

Об’єкт розробки – комп’ютерна система ТОВ "Пантазіївське" з реалізацією побудови та налаштування корпоративної мережі.

Мета роботи − створення комп’ютерної системи ТОВ "Пантазіївське".

Була розроблена комп'ютерна мережа, яка може гнучко змінювати свій зовнішній вигляд і набір функцій шляхом перепрограмування.

Розроблені технічні вимоги до компютерної мережі та інформаційної системи підприємства.

Проведено аналіз сучасного мережевого обладнання та тенденцій розвитку мережевих технологій. На основі чого обрано технічні засоби організації компютерної мережі.

Розроблена адресація усіх пристроїв інформаційної системи. Виконано моделювання розробленої мережі в середовищі Cisco Packet Tracer. Симуляція роботи мережі підтвердила що виконані розрахунки та налаштування вірні і мережа працездатна.

Робота виконана відповідно до вимог і завдання.

Результати перевірки у вигляді таблиць, графіків описані і наводяться у пояснювальній записці та додатках.

ЗМІСТ

ВСТУП

У сучасному світі впровадження комп'ютерних систем та впровадження інформаційних технологій стають невід'ємною частиною успішної діяльності підприємств у різних галузях. Фермерське господарство ТОВ "ПАНТАЗІЇВСЬКЕ" не є винятком. У світлі постійного розвитку та конкурентного середовища виробництва, впровадження комп'ютерних систем стає необхідністю для оптимізації процесів та підвищення продуктивності роботи.

Серед ключових аспектів оптимізації є побудова та налаштування корпоративної мережі. Цей звіт присвячений детальному опрацюванню процесу побудови та налаштування комп'ютерної системи для ТОВ "ПАНТАЗІЇВСЬКЕ". Він включає в себе аналіз потреб компанії, проектування інфраструктури, вибір необхідного обладнання та програмного забезпечення, а також налаштування параметрів мережі для забезпечення ефективного функціонування та безпеки інформації.

Розглядаючи цей процес, ми візьмемо до уваги унікальні особливості фермерського господарства, визначимо специфічні потреби компанії та запропонуємо оптимальні рішення для створення інтегрованої та надійної корпоративної мережі. Побудова та налаштування комп'ютерної системи для ТОВ "ПАНТАЗІЇВСЬКЕ" є ключовим кроком у підвищенні її конкурентоспроможності та досягненні високих результатів у вирощуванні сільськогосподарської продукції.

1 СТАН ПИТАННЯ ТА ПОСТАНОВКА ЗАВДАННЯ

1.1 Стисла характеристика галузі та умов застосування комп’ютерної системи, що проектується.

Фермерське господарство ТОВ "Пантазіївське" націлене на вирощування сільськогосподарської продукції, зокрема зернових, овочів, та фруктів. Основні процеси включають обробку ґрунту, посів, полив, догляд за рослинами, збір урожаю, зберігання та транспортування продукції.

Умови застосування комп'ютерної системи:

–Моніторинг та управління поливом: Комп'ютерна система дозволить автоматизувати процес поливу, аналізувати рівень вологості ґрунту та прогнозувати погодні умови для оптимального зрошення.

–Управління виробничими процесами: Система буде використовуватися для планування посівних площ, ведення обліку рослин, контролю якості ґрунту та виробничих процесів.

–Моніторинг врожаю: Комп'ютерна система допоможе вести облік врожаю, оцінювати його обсяг та якість, а також прогнозувати потенційні врожаї.

Застосування комп'ютерної системи у фермерському господарстві ТОВ "Пантазіївське" сприятиме підвищенню ефективності виробничих процесів, зменшенню витрат ресурсів та оптимізації управління сільськогосподарською діяльністю.

1.2 Характеристика і структура компанії

Об’єкт впровадження – ТОВ "Пантазіївське".

ТОВ "Пантазіївське" є фермерським господарством, спеціалізованим у вирощуванні сільськогосподарської продукції. Заснована з метою поєднання сучасних технологій з традиційними методами сільського господарства для досягнення високої якості продукції та оптимального використання ресурсів.

Структура компанії:

1. Керівництво:

–Директор: відповідає за загальне керівництво компанією, стратегічне планування та прийняття рішень.

–Заступник директора: надає підтримку директору у різних аспектах управління та координації діяльності.

2. Виробничі підрозділи:

–Відділ агротехніки: відповідає за проведення сільськогосподарських робіт, включаючи обробку ґрунту, посів, догляд та збір врожаю.

–Відділ збуту: здійснює продаж продукції, веде взаємодію з покупцями та партнерами.

–Відділ логістики: відповідає за організацію транспортування та зберігання вирощеної продукції.

–Фінансовий відділ: веде облік фінансової діяльності, розрахунки з постачальниками та клієнтами, складання фінансових звітів.

–Відділ інформаційних технологій: забезпечує підтримку комп'ютерної інфраструктури, використання програмних систем та розробку нових інформаційних технологій.

–Відділ кадрів: відповідає за підбір, навчання та розвиток персоналу.

3. Робочі групи та бригади:

–Агрономи: займаються плануванням та контролем за вирощуванням рослин.

–Механізатори: відповідають за обслуговування та ремонт сільськогосподарської техніки.

–Пакувальний персонал: забезпечує упаковку та маркування продукції перед відправленням.

Така структура дозволяє ТОВ "Пантазіївське" ефективно виконувати свої функції, забезпечуючи виробництво високоякісної сільськогосподарської продукції і задовольняючи потреби ринку.

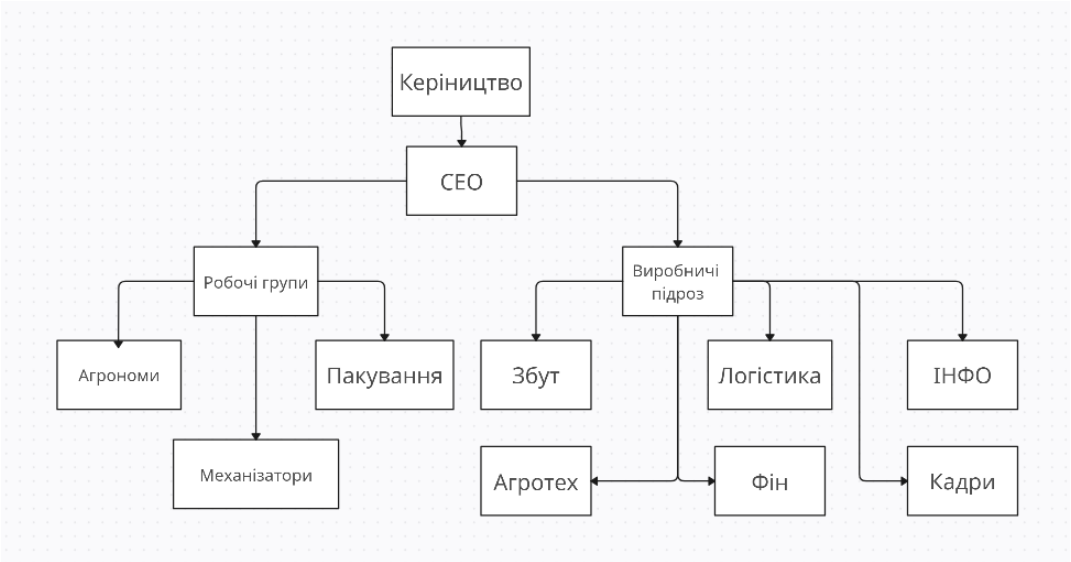

Рисунок 1.1 – Схема організаційної структури

1.3 Стислі відомості про топологічне розміщення структурних підрозділів

Топографічне розміщення структурних підрозділів скається з однієї будівлі. Це будівля на 7-м кімнат та частиною територією. Знаходиться будівля за адессою:вул. Центральна, 21, Олександрія, Кіроаоградська область, 49000(рис 1.)[1].

Топографічна схема розміщення структурних підрозділів показана на рис. 1.2

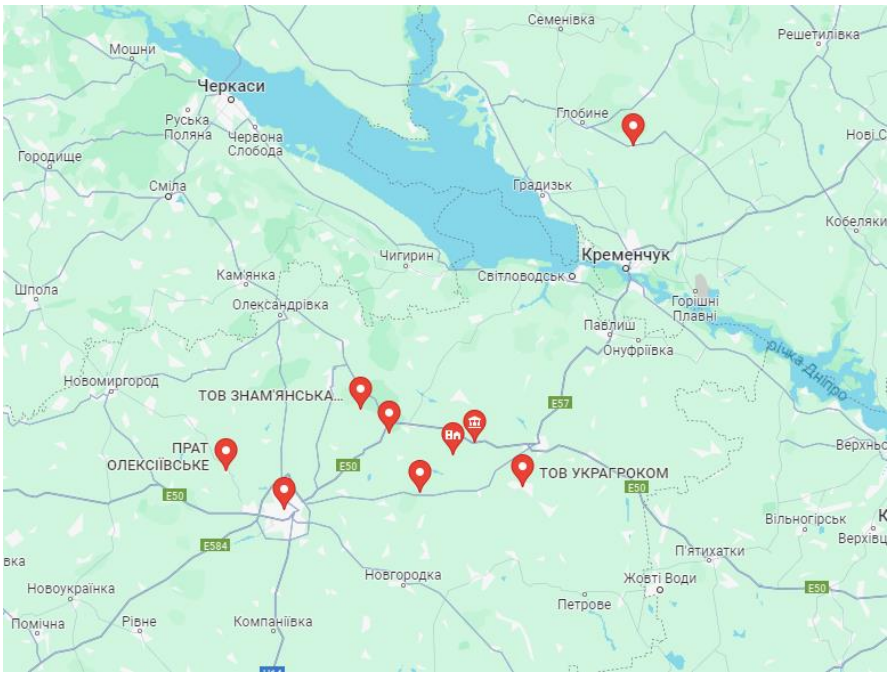

Рисунок 1.2 – Топографічна схема розміщення структурних підрозділів ТОВ"Пантазіївське"

Структурна схема розміщення підрозділів наведена на рисунку 1.3.

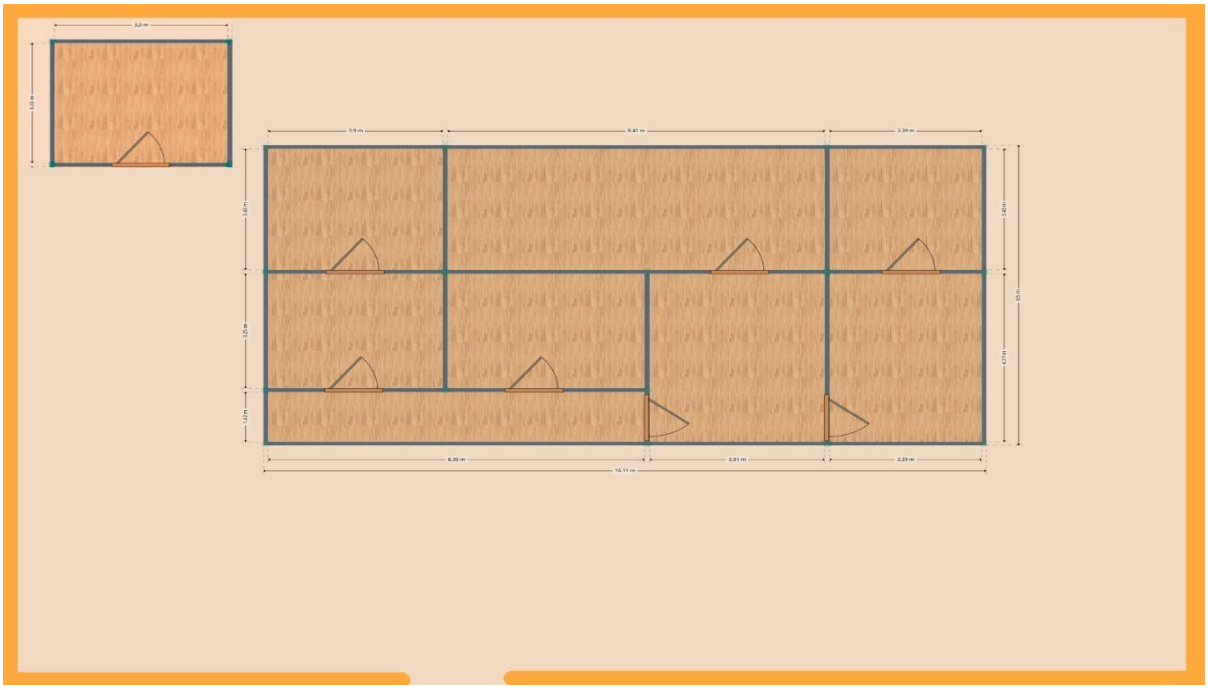

Рисунок 1.3 – Структурна схема розміщення підрозділів у будівлі

1.4 Принципи та технічні способи інформаційного забезпечення об’єктавпровадження

В аграрній сфері існує безліч технічних засобів та методів інформаційного забезпечення, які розвиваються, ось декілька:

–Цілісність даних: Забезпечення доступу до повної та достовірної інформації про всі аспекти діяльності господарства, включаючи вирощування, врожайність,витрати, фінансові показники тощо.

–Автоматизація процесів: Використання спеціалізованих програмних засобів та технологій для автоматизації виробничих процесів, обліку виробництва, управління запасами та іншими аспектами діяльності.

–Моніторинг та аналіз: Впровадження систем моніторингу та аналізу, які дозволяють в реальному часі відстежувати стан рослин, ґрунту, а також ефективність використання ресурсів і управління процесами на основі отриманих даних.

–Забезпечення безпеки даних: Використання заходів для захисту конфіденційності, цілісності та доступності інформації, включаючи застосування шифрування, системи резервного копіювання та заходи з протидії кіберзлочинності.

–Інтеграція та взаємодія: Забезпечення можливості взаємодії та обміну данимиз іншими системами, такими як системи обліку та управління, програми аналізу ринкута прогнозування погоди, для забезпечення більш ефективного управління та прийняття рішень.

–Доступність та мобільність: Забезпечення можливості доступу до інформації з будь-якого місця та пристрою за допомогою відповідних мобільних додатків або веб-інтерфейсів.

Ці принципи та технічні способи інформаційного забезпечення допомагають підвищити ефективність та конкурентоспроможність фермерського господарства, забезпечуючи оптимальне використання ресурсів та забезпечення якості продукції.

1.5 Завдання і мета роботи

Метою роботи є розробка Комп'ютерної системи для ТОВ "Пантазіївське" здетальним опрацюванням побудови та налаштування корпоративної мережі.

Завдання поставлене замовником:

–Побудувати корпоративну мережу для забезпечення ефективного обміну даними та спільної роботи між різними підрозділами та співробітниками компанії.

–Налаштувати і забезпечити безпеку мережі для захисту конфіденційності тацілісності даних компанії.

–Оптимізувати робочі процеси та забезпечити швидкий доступу до необхідноїінформації.

Кроки виконання:

–Визначення потреб компанії у корпоративній мережі та розробка відповідноїархітектури мережі.

–Побудова мережевої інфраструктури, включаючи встановлення серверів, комутаторів, маршрутизаторів та іншого необхідного обладнання.

–Налаштування параметрів мережі, включаючи мережеві протоколи, безпеку,розділення прав доступу та моніторинг мережевого трафіку.

–Впровадження засобів резервного копіювання та відновлення даних для забезпечення надійності інформації.

–Навчання персоналу щодо користування корпоративною мережею та заходівбезпеки даних.

Виконання цих завдань та досягнення мети допоможуть забезпечити ефективнуроботу компанії, підвищити продуктивність праці та забезпечити безпеку та надійність обміну інформацією всередині організації.

.

2 РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ КОМП'ЮТЕРНОЇ СИСТЕМИ

2.1 Технічні вимоги до комп'ютерної системи компанії ТОВ «ПАНТАЗІЇВСЬКЕ»

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

Комп'ютерна система розроблена та призначена для забезпечення обміну інформацією з управлінням компанії.

Для цього проекту потрібно створити п'ять локальних мереж за завданням замовника. Для відповідності вимогам, рекомендується використовувати Ір-блок-адресу для призначення підмережі.

Корпоративна мережа складається з 5 підмереж:

Потрібно розбити IP-адресу 172.24.152.0/21 на 5 підмереж враховуючи кількість вузлів для LAN:

LAN1 – 35 вузлів; LAN2 – 115 вузлів;LAN3 – 154 вузлів;LAN4 – 93 вузлів; LAN5 – 56 вузлів.

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

Пропускна здатність і швидкість передачі даних: Мережеві компоненти мають забезпечувати достатню пропускну здатність для ефективної обробки передбачуваних обсягів даних без затримок, тим самим гарантуючи оперативне обслуговування запитів користувачів і системних процесів.

Надійність зв'язку: Канали зв'язку між компонентами повинні забезпечувати високу надійність, знижуючи ризик відмов у критичні моменти.

Масштабованість: Система повинна бути спроможна до збільшення обсягу даних і кількості користувачів, дозволяючи легке додавання нових компонентів без зниження загальної продуктивності.

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

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

Сумісність інтерфейсів: Всі системи повинні використовувати взаємосумісні або стандартизовані інтерфейси, щоб забезпечити безперешкодну інтеграцію.

Обмін даними: Системи мають забезпечувати обмін даними в реальному часі або за визначеними інтервалами, відповідно до потреб бізнесу.

Єдність протоколів: Використання єдиних протоколів зв'язку дозволяє уникнути проблем із сумісністю та підвищити ефективність інтеграції систем.

Контроль доступу: Належні механізми управління доступом і правила, що визначають, хто і як може взаємодіяти з системою, забезпечують безпеку та контроль.

Ці вимоги гарантують, що мережа ТОВ «Пантазіївське» зможе ефективно інтегруватися з наявними та майбутніми системами, підтримуючи стабільність бізнес-процесів та забезпечуючи високий рівень обслуговування.

2.1.1.1.4 Вимоги до режимів функціонування системи

– Нормальний режим роботи: Система повинна безперервно функціонувати протягом робочого часу, забезпечуючи користувачам доступ до всіх необхідних функцій.

– Аварійний режим відновлення: У випадку технічних проблем або аварійних ситуацій система повинна мати можливість переходити в аварійний режим відновлення, мінімізуючи вплив на бізнес-процеси.

– Режим резервного копіювання і відновлення: Система повинна включати механізми регулярного резервного копіювання даних і можливості їх відновлення у випадку втрати або пошкодження, що гарантує цілісність та доступність інформації.

– Безперервна підтримка та оновлення: Система повинна мати підтримку IT-спеціалістів для швидкого вирішення проблем та оновлення програмного забезпечення, що забезпечить безперебійну роботу та захист від можливих загроз.

2.1.1.1.5 Вимоги до діагностування системи

Інтегровані засоби моніторингу: Система повинна містити вбудовані інструменти для спостереження за станом апаратного і програмного забезпечення.

Протоколювання подій: Автоматичне фіксування всіх системних подій і збереження журналів для аналізу, відстеження змін і виявлення помилок.

Інтерфейси для віддаленого доступу: Можливість віддаленого доступу до системи для проведення діагностики та усунення несправностей.

Система сповіщення: Автоматичне сповіщення технічної служби про критичні помилки або збої в системі.

2.1.1.1.6 Перспективи розвитку, модернізації системи

Масштабованість: Архітектура системи має дозволяти легко додавати нові компоненти та підвищувати її продуктивність без необхідності повного перепроектування.

Технологічні оновлення: Система повинна забезпечувати інтеграцію з сучасними технологіями та стандартами, щоб залишатися конкурентоспроможною на ринку.

Заміна застарілих компонентів: Програма оновлення передбачає заміну обладнання та програмного забезпечення, які більше не підтримуються.

2.1.1.2 Вимоги до показників призначення

Продуктивність: Характеристики, що визначають ефективність обробки запитів та виконання функцій системою.

Надійність: Оцінка частоти виникнення помилок та середнього часу між відмовами.

Масштабованість: Здатність системи розширюватися відповідно до збільшення обсягів даних чи кількості користувачів.

2.1.1.3 Вимоги до патентної чистоти

Устаткування та програмне забезпечення, що використовуються в комп'ютерній системі, мають відповідати патентним вимогам.

Для цього необхідно застосовувати ліцензійне програмне забезпечення, ретельно досліджувати компоненти системи для виявлення можливих патентів,

звертатися за юридичною консультацією та вести документацію з проектування компонентів системи. Це дозволить мати доказову базу щодо патентної чистоти у випадку претензій від виробників.

2.1.1.4 Вимоги до задач (налаштувань), які виконує КС

Під час розробки адресації підмереж потрібно враховувати наступні вимоги:

–корпоративна мережа повинна складатися з 5 підмереж LAN1-LAN5;

–блок адрес для виділення підмереж повинен бути 172.24.152.0/21;

–середня інтенсивність вихідного трафіку в найбільшій мережі повинна дорівнювати μ =222 кадрів/с;

–середня довжина вихідного повідомлення в найбільшій мережі повинна дорівнювати 650 байт;

–затримка передачі пакету в найбільшій мережі повинна бути ≤6 мс.

Для виконання базового налаштування конфігурації пристроїв необхідно враховувати наступні вимоги:

–потрібно назначити назви пристроям за наступним правилом: Прізвище студента_тип пристрою_номер пристрою;

–на всіх пристроях повинен бути назначений пароль cisco до консолі і vty;

–на всіх пристроях повинен бути назначений пароль class до привілейованогорежиму;

–усі паролі, що зберігаються у відкритому вигляді, потрібно зашифрувати;

–потрібно розробити банер MOTD;

–потрібно назначити на усіх лініях vty використання протоколу ssh;

–потрібно призначити ім’я користувача та пароль на всіх пристроях за правилом: група_прізвище з паролем admincisco;

–в якості імені домена потрібно використати ім'я пристрою. Для шифруванняданих потрібно створювати ключ RSA завдовжки 1024 біт;

–на DCE-інтерфейсах маршрутизаторів потрібно призначити встановлення значення тактової частоти – 128000;

– потрібно налаштувати аудит і відправку повідомлень про початок ізавершення процесу exec, з використанням локальної бази;

−з метою збільшення пропускної здатності і надійності каналів в мережі LAN_1 на комутаторах потрібно виконати об'єднання фізичних ліній. [3]

На маршрутизаторах повинен використовуватися протокол динамічної маршрутизації OSPF, що підтримує множинні шляхи, має малий час збіжності і реагування та створює мінімальний службовий трафік. Під час налаштування маршрутизаторів потрібно враховувати наступні вимоги:

−потрібно оголосити безпосередньо підключені мережі і відключити поширення оновлень маршрутизації на інтерфейси в локальні мережі;

−для VLAN мереж потрібно налаштувати сумарний маршрут і оголосити йогоіншим маршрутизаторам;

−потрібно налаштувати маршрут за умовчанням на маршрутизаторі з прямим підключенням до інтернет-провайдера (ISP) і розповсюдити його через оновлення маршрутизації.

Під час налаштування всіх маршрутизаторів на підтримку служби AAA необхідно враховувати наступні вимоги:

−для перевірки підключень до VTY ліній на маршрутизаторі потрібно використовувати локальну базу даних користувачів;

−для доступу до консолі потрібно використовувати аутентифікацію на основіпротоколу RADIUS і якщо немає − локальну базу даних;

−RADIUS-сервер потрібно налаштувати наступним чином: ключове слово – radius123; в якості облікового запису користувачів потрібно використовувати ім’я пристрою з паролем admin123. [3]

При налаштуванні роботи Інтернет в Системі необхідно враховувати наступні вимоги:

−потрібно встановити одного провайдера послуг доступу до Інтернет (ISP);

−для виходу робочих станцій в Інтернет необхідно настроїти пограничний маршрутизатор з динамічним NAT за такими даними: ім’я пула: Internet, пул адресів: 209.165.200.5 по 209.165.200.30, номер списку доступу 12;

−потрібно налаштувати сервер HTTP, щоб на вузлах при вводі в рядку браузера http://123.dnipro.ua (http://209.165.200.4) відкривався веб-сайт з відомостями про тему та завдання на кваліфікаційну роботу студента;

–потрібно налаштувати віртуальну приватну мережу site-to-site VPN з використанням IPsec для трафіку, що проходить між «Підмережою підрозділу підприємства» та віддаленою мережею організації через Internet. [3]

Під час налаштування мереж VLAN і маршрутизації між ними потрібно враховувати наступні вимоги:

–потрібно налаштувати транкові порти і порти доступу, а також вимкнути усіневикористовувані фізичні порти комутаторів;

–потрібно налаштувати SVI-інтерфейси на комутаторах, призначивши IPv4-адреси з мережі Management VLAN;

–потрібно налаштувати маршрутизацію між мережами VLAN. [3]

При налаштуванні адресації ПК в мережах VLAN необхідно враховувати наступні вимоги:

–потрібно налаштувати маршрутизатор, що здійснює маршрутизацію між VLAN, в якості сервера DHCP для мереж VLAN;

–потрібно створити пули DHCP під назвою pollvlan№, де № − номер VLAN;

–потрібно виключити з пулу перші 10 адрес і для кожного пулу вказати адресуDNS-сервера і шлюз за замовчуванням. [3]

На портах комутаторів, підключених до серверів, потрібно налаштувати функцію безпеки портів, враховуючи наступні вимоги:

–тільки двом унікальним пристроям повинен бути дозволений доступ до порту;

–MAC-адрес пристрою повинен розпізнаватися динамічно і додаватися в поточну конфігурацію;

–під час порушенні системи безпеки повинно з’являтися повідомлення, а портповинен залишатися включеним. [3]

2.1.1.5 Додаткові вимоги

Умови експлуатації: Гарантування стабільної роботи системи відповідно

до кліматичних особливостей регіону.

Обладнання: Визначення технічних параметрів активного обладнання, таких як потужність, кількість портів та варіанти монтажу.

Кабель-канали та розетки: Встановлення специфікацій для типів та розташування кабель-каналів і розеток.

Комунікаційне обладнання: Вимоги до розміщення та типів шаф і кабельних трас.

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

2.1.2 Вимоги функцій, виконуваним системою

Перелік функцій: Опис ключових завдань, які система має виконувати, включаючи обробку даних, забезпечення безпеки і взаємодію з іншими системами.

Часовий регламент: Встановлення максимально припустимих часів на виконання кожної функції системи.

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

2.1.3 Вимоги до видів забезпечення КС

2.1.3.1 Вимоги до математичного забезпечення

– Склад математичних методів і моделей:

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

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

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

Область застосування та обмеження:

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

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

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

– Способи використання:

Інтеграція з IT-системами: Інтеграція математичних моделей та алгоритмів з існуючими IT-системами для забезпечення їх ефективної роботи.

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

Динамічне оновлення: Підтримка можливості легкого оновлення моделей та алгоритмів відповідно до змін у даних або в операційному середовищі.

Алгоритми, що підлягають розробці:

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

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

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

2.1.3.2 Вимоги до інформаційного забезпечення

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

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

– Доступність: Забезпечення безперебійної роботи системи цілодобово.

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

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

2.1.3.3 Вимоги до лінгвистичного забезпечення

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

2.1.3.4 Вимоги до технічного забезпечення

Для ефективної роботи кожне робоче місце повинно бути оснащене комп'ютером з такою конфігурацією:

−процесор з мінімум чотирма ядрами з тактовою частотою не нижче 2 Ггц;

об'єм опертивної пам'яті не нижче 8 Гб;

−дискретний відеоадаптер;

−об'єм пам'яті не менше 256 Гб;

−операційна система Windows 10 або Windows 11.Сервер повинен відповідати вимогам:

−процесор не нижче 1,5 Ггц;

−об'єм опертивної пам'яті не нижче 8 Гб.Комутатор повинен відповідати вимогам:

−24 порти FastEthernet та порт GigabitEthernet;

−підтримка Etherchannel, VLAN. Маршрутизатор повинен відповідати вимогам:

−мінімум 2 порти GigabitEthernet, 4 EHWIC слоти;

−підтримка DHCP, NAT, VPN та AAA моделі.

2.1.3.5 Вимоги до організаційного забезпечення

Працівники ІТ-відділу повинні мати доступ до технічного приміщення за допомогою методів аутентифікації наприклад ключ-картками.

2.1.3.6 Вимоги до методичного забезпечення

Склад нормативно-технічної документації:

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

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

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

2.2 Розробка апаратної частини комп'ютерної Системи

2.2.1 Розробка структурної схеми комплексу технічних засобів

З'єднання між маршрутизаторами виконується кабелями Serial DTE або крос- кабелі, маршрутизатори з комутаторами поєднаються між собою за допомогою прямого кабеля так само як і комп'ютери до комутаторів, для з'єднання комутаторів використовується крос-кабель.

На основі загальної характеристики компанії, її архітектури, кількості підмереж та завдання, розроблено структурну схему комплексу технічних засобів комп'ютерноїсистеми компанії яка показана на рис.2.2

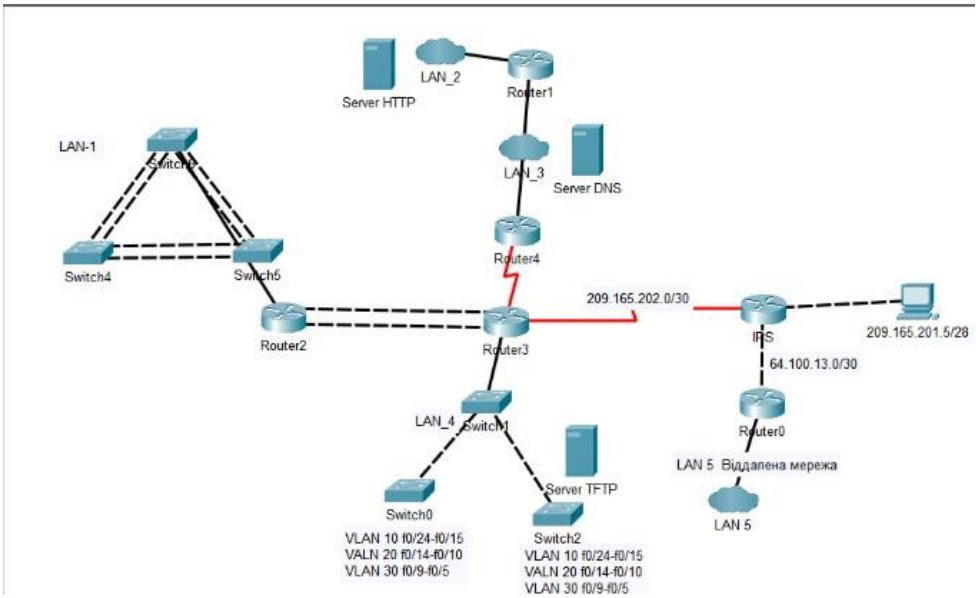

Рисунок 2.2 – Структура комп’ютерної мережі підприємства

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

Схема розміщенна на рисунку 2.2 включає:

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

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

Основні принципи вибору даної структурної схеми базуються на наступних міркуваннях:

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

Надійність: Структура мережі включає резервні з'єднання між ключовими компонентами, що забезпечує високий рівень надійності та доступності послуг навіть при відмові одного або декількох вузлів.

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

Оптимізація витрат: Структура схеми оптимізована для зменшення витрат на технічне обладнання та експлуатаційні витрати, використовуючи ефективне підключення і взаємодію компонентів системи.

2.2.3 Розробка специфікації та опису апаратних засобів комп’ютерної Системи

Вибір апаратної частини корпоративної мережі є важливим кроком для забезпечення надійності та продуктивності системи. У якості маршрутизатора було обрано Cisco ASR1001-X.

Ця модель має високу продуктивність та розширені можливості для обробки даних мережі. Технічні характеристики моделі наступні: має два WAN портів, дев’ять портів під підключення комутаторів швидкістю до 1 Gbps(9x10/1000) та мережевий екран швидкістю до 5Gbps. Маршрутизатор Cisco ASR1001-X відповідає потребам компанії для забезпечення стабільного та захищеного зв’язку між мережевими пристроями.

Для подальшої побудови локальної мережі, обрано комутатор Cisco Catalyst 2960X-24TS-L. Даний комутатор має: 24 порти Fast Ethernet (10/100 Mbps) та два порти зі швидкістю до 1 Gbps(9x10/1000). Комутатор підтримує такі функції як VLAN, Quality of Service (QoS), Spanning Tree Protocol (STP), Access Control Lists (ACLs), що дозволяють налаштовувати та керувати роботою комутатора, також він

забезпечує швидку передачу даних, надає широкі можливості управління, безпеки тамасштабованості, відповідає потребам компанії для забезпечення надійного з'єднанняробочих станцій, серверів та інших мережевих пристроїв.

Таблиця 2.1 – Специфікація обладнання

Позиція	Найменування і технічна характеристика	Тип, марка, позначення документа	Одиниці виміру	Кількість	Примітки
1	**2**	**3**	**4**	**5**	**6**
1	Cisco ASR1001-X System, Crypto, 4 built-in GE, Dual P/S, 20Gbit, 6x1000Base-X (SFP), 2x10G SFP+ інтегровані RP, SIP та ESP, 1xNIM, 1xSPA, RAM 8Gb, 2xAC	Cisco ASR1001-X	Од.	5	За структурною схемою КТЗ: Router 0-4 Детальні характеристики: https://stacksystems.com.ua/marshrutizatorcisco-ASR-1001-X
2	Комутатор 24 x Ethernet 10/100/1000 Мбіт/сек, RIP v1, RIP v2, OSPF, USB-порт, LAN Base, 4 SFP слоти	Cisco Catalyst 2960X-24TS-L	Од.	21	За структурною схемою КТЗ: Детальні характеристики: https://stacksystems.com.ua/kommutatorcisco-Catalyst- 2960-24tt-l
4	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	За структурною схемою КТЗ: Сервер HTTP, DNS, TFTP Детальні характеристики: http://surl.li/hnuad
5	Комп’ютер: AMD Ryzen 5 5600G (3.9 — 4.4 ГГц), 16 ГБ DDR4, 1 ТБ SSD, AMD Radeon Vega 7, Windows 11 Pro	ARTLINE Business B38v08Win	Од.	331	За структурною схемою КТЗ: ПК Детальні характеристики: https://comfy.ua/ua/nettopartline-business-b38-b38v08win.html

2.2.4 Розрахунок інтенсивності вихідного трафіку найбільшої локальної мережі підприємства

Пропускна здатність лінії вихідного каналу дорівнює 1000Мбіт/с.

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

Середня інтенсивність трафіку μ=222 кадрів/с, а середня довжина повідомленняскладає 650 байт.

Припустимо, що всі користувачі одночасно використовують послуги. Розрахуємо пропускну здатність LAN_3, яка складається з 154 вузлів. Пропускна здатність мережі на рівні доступу буде дорівнювати:

$$P_{р.р} = \mu * L_{пов} * N * 8 = 222 * 650 * 154 * 8 = 177{,}777 \text{ Мбіт/с}, \quad (2.1)$$

де

N – кількість вузлів в мережі

$L_{пов}$ – середня довжина повідомлення

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

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

Загальне навантаження на комутатор не повинно перевищувати:

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

Оскільки кожне джерело в середньому виробляє в середньому 145 пакетів/с, токількість приєднань, якими обмежен комутатор рівня доступу, складає максимум:

$$N = \mu_{вих}/\mu = 192308/154 = 1249 \text{ джерел} \quad (2.3)$$

Коефіцієнт затримки:

$$\rho = \lambda/\mu_{вих} = 34188/192308 = 0{,}17 \quad (2.5)$$

Коефіцієнт зайнятості комутатора рівня доступу:

$$\rho = \rho/(1-\rho) = 0{,}17/0{,}83 = 0{,}204$$

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

$$T = 1/(\mu_{вих} - \lambda) = 1/(192308 - 34188) = 5{,}32 \text{ мкс} \quad (2.7)$$

Середня довжина черги:

$$L_{чер} = \rho^2 /(1-\rho) = 0,17^2 /0,83 = 0,0348 \quad (2.8)$$

Середній час перебування пакета у черзі:

$$T_{оч} = L_{чер} / \lambda = 0,0348/34188 = 0,10 \text{ мкс} \quad (2.9)$$

Це значення менше 6 мс, що задовольняє вимогам.

3 РОЗРОБКА КОРПОРАТИВНОЇ МЕРЕЖІ

3.1 Проектування логічної топології мережі

Розробка логічної топології мережі є ключовим компонентом у створенні IT-інфраструктури будь-якої організації, оскільки основна задача полягає у створенні корпоративної мережі з добре організованою структурою, яка б забезпечувала високий рівень масштабованості та безпеки. В архітектурі мережі передбачено п'ять підмереж, чотири з яких розташовані в одному з головних офісів, а п'ята – віддалений офіс, який обладнаний технологією Etherchannel для забезпечення безперервності роботи навіть у випадку виходу з ладу одного чи кількох комутаторів.

В рамках мережі активовано важливі мережеві сервіси, такі як DNS для розв'язання імен і TFTP для передачі конфігураційних файлів. Захист даних та доступу до ресурсів мережі забезпечується за допомогою комплексної моделі AAA, яка включає аутентифікацію, авторизацію та облік дій користувачів. Основа маршрутизації здійснюється за протоколом OSPF, що забезпечує ефективний обмін маршрутною інформацією всередині мережі.

Додатково, розробка мережі враховує необхідність подальшого розширення та інтеграції нових технологій. У плануванні передбачені заходи для легкої інтеграції нових серверів, мережевих пристроїв та служб, що дозволяє компанії зростати без необхідності кардинально перебудовувати існуючу мережеву структуру. Крім того, враховуючи високі вимоги до безпеки даних, запроваджено розширені методи шифрування та ідентифікації загроз, що допомагає забезпечити надійний захист корпоративної інформації від зовнішніх та внутрішніх загроз.

.

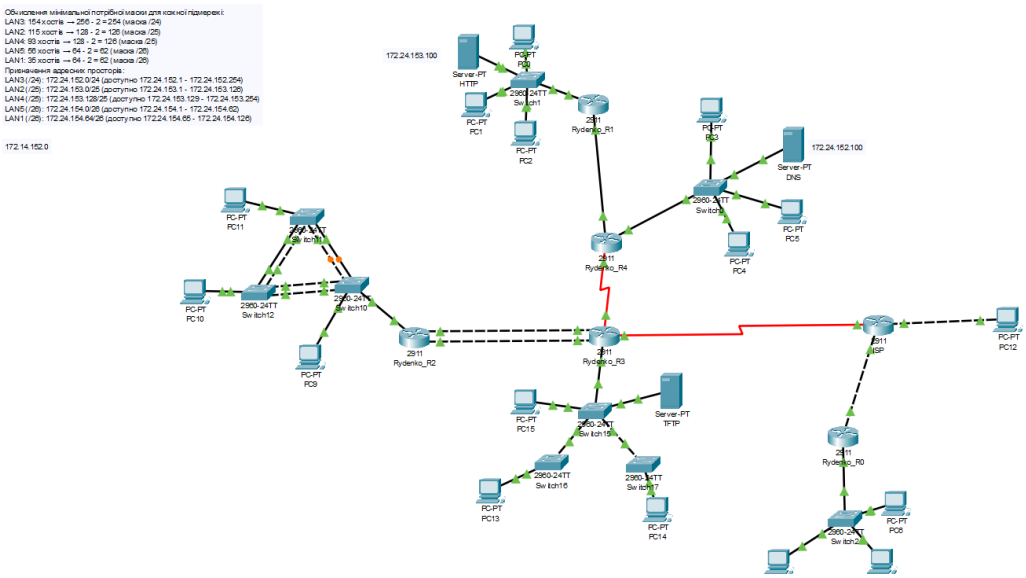

Рисунок 3.1 – Топологія мережі

3.2 Вибір та опис мережного обладнання

У сфері інформаційних технологій, правильний вибір мережевого обладнання критично важливий для забезпечення ефективності та надійності корпоративних мереж. Комплексні мережеві рішення, такі як інтегровані сервісні маршрутизатори Cisco 2911, комутатори Cisco 2960 та сервери Cisco, відіграють ключову роль у задоволенні вимог сучасних компаній до швидкості передачі даних, безпеки та стабільності.

Маршрутизатор Cisco 2911 належить до серії ISR G2 і розроблений для підтримки широкого спектру модулів, включаючи голосові, відео, безпеки, бездротові зв'язки та збереження даних. Завдяки своїй Integrated Services архітектурі, цей маршрутизатор забезпечує високу гнучкість налаштувань і можливості масштабування, дозволяючи компаніям ефективно управляти мережевими ресурсами. Технічні характеристики маршрутизатора включають пропускну спроможність до 35 Mbps при шифруванні та обладнання трьома інтегрованими 10/100/1000 Ethernet портами, а також новими слотами для додавання різних інтерфейсів.

Комутатори Cisco 2960 становлять основу для побудови ефективних корпоративних мереж, особливо в середовищах з інтенсивним мережевим

трафіком. Ці комутатори підтримують від 8 до 48 Ethernet портів з функцією PoE, що ідеально підходить для забезпечення енергією IP-телефонів та інших пристроїв. Висока пропускна здатність та низький час відгуку, а також підтримка QoS, оптимізують передачу голосу та відео. Комутатори також включають розширені функції безпеки, такі як ACL, гостьові VLAN та MAC-адресна фільтрація.

Сервери Cisco UCS, розроблені для великомасштабних обчислень в центрах обробки даних, пропонують високу продуктивність і масштабування. Вони підтримують багатоядерні процесори Intel Xeon, мають великий обсяг оперативної пам'яті для обробки великих даних і складних додатків, а інтегрована система управління спрощує взаємодію між компонентами сервера, знижуючи витрати на володіння.

3.3 Розрахунок схеми адресації корпоративної мережі

Метод VLSM дозволяє використовувати маски підмереж різної довжини в рамках однієї мережі, що забезпечує більш ефективне використання IP-адрес. Застосування VLSM дозволяє зменшити кількість невикористаних IP-адрес у мережі, що є особливо важливим при обмеженому пулі адрес.

Кроки розбиття за VLSM:

Список підмереж по спаданню кількості хостів:

– LAN3: 154 хостів
– LAN2: 115 хостів
– LAN4: 93 хостів
– LAN1: 35 хостів
– LAN5: 56 хостів

Обчислення мінімальної потрібної маски для кожної підмережі:

– LAN3: 154 хостів = 256 - 2 = 254 (маска /24)
– LAN2: 115 хостів = 128 - 2 = 126 (маска /25)
– LAN4: 93 хостів = 128 - 2 = 126 (маска /25)

– LAN5: 56 хостів = 64 - 2 = 62 (маска /26)

– LAN1: 35 хостів = 64 - 2 = 62 (маска /26)

Призначення адресних просторів:

– LAN3 (/24): 172.24.152.0/24 (доступно 172.24.152.1 - 172.24.152.254)

– LAN2 (/25): 172.24.153.0/25 (доступно 172.24.153.1 - 172.24.153.126)

– LAN4 (/25): 172.24.153.128/25 (доступно 172.24.153.129 - 172.24.153.254)

– LAN5 (/26): 172.24.154.0/26 (доступно 172.24.154.1 - 172.24.154.62)

– LAN1 (/26): 172.24.154.64/26 (доступно 172.24.154.65 - 172.24.154.126)

Перевірка загального покриття адресного простору: Блок 172.24.152.0/21 охоплює адреси від 172.24.152.0 до 172.24.159.255, тому покриття цих підмереж ефективне і знаходиться в межах вихідного діапазону.

Це базовий план розбиття на підмережі за методом VLSM. Кожна підмережа має достатньо адрес для заданих вимог і правильно розраховану маску для максимальної ефективності.

Таблиця 3.1 – Схема адресації мережі

Назва підмережі	Необхідна кіл-ть вузлів	Адреса підмережі	Маска Підмережі у Десятковому форматі	Діапазон допустимих IP-адрес вузлів
LAN 1	35	172.24.154.64	/26	172.24.154.65 - 172.24.154.126
LAN 2	115	172.24.153.0	/25	172.24.153.1 - 172.24.153.126
LAN 3	154	172.24.152.0	/25	172.24.152.1 - 172.24.152.254
LAN 4	93	172.24.153.128	/25	172.24.153.129-172.24.153.254
LAN 5	56	172.24.154.0	/26	172.24.154.1 - 172.24.154.62

У таблиці 3.2 наведено схему адресації маршрутизаторів мережі.

Пристрій	Інтерфейс	IP-адреса мережі	Маска
Rydenko_R3	Se0/0/0	172.14.152.10	255.255.255.252
	Gig0/0	172.14.152.2	255.255.255.252
	Gig0/1	172.14.152.6	255.255.255.252
	Se0/0/1	209.165.202.2	255.255.255.252
Rydenko_R2	Gig0/0	172.14.152.1	255.255.255.252
	Gig0/1	172.14.152.5	255.255.255.252
	Gig0/2	172.24.154.65	255.255.255.192
Rydenko_R1	Gig0/0	172.14.152.13	255.255.255.252
	Gig0/1	172.24.153.1	255.255.255.128
Rydenko_R4	Gig0/0	172.14.152.14	255.255.255.252
	Gig0/1	172.24.152.1	255.255.255.0
	Se0/0/0	172.14.152.9	255.255.255.252
Rydenko_R0	Gig0/0	64.100.13.1	255.255.255.252
	Gig0/1	172.24.154.1	255.255.255.192

Таблиця 3.2 – Схема адресації пристроїв

3.4 Базове налаштування конфігурації пристроїв

Початкове налаштування маршрутизаторів та комутаторів охоплює декілька ключових кроків: присвоєння імен пристроям, встановлення захисту паролів, конфігурацію доступу з адміністративними правами та використання безпечних протоколів для адміністрування мережевих ресурсів. Ці етапи є фундаментальними для забезпечення правильної та безпечної роботи мережевої інфраструктури.

При налаштуванні імен пристроїв важливо вибрати логічні та зрозумілі назви, які відображають їхнє місце та роль у мережі. Це спрощує управління мережею та допомагає у виявленні проблем.

Налаштування захисту паролів має включати використання складних паролів та встановлення обмежень на їх використання для запобігання

несанкціонованого доступу. Застосування методів шифрування для збереження паролів у конфігураційних файлах є критично важливим для забезпечення додаткового рівня безпеки.

Конфігурація доступу з підвищеними правами дозволяє адміністраторам мережі виконувати критично важливі завдання без ризику компрометації системи. Використання безпечних протоколів, таких як SSH замість Telnet, для віддаленого доступу до мережевого обладнання забезпечує шифрування всіх переданих даних, знижуючи ризик перехоплення інформації.

Також слід звернути особливу увагу на технологію Etherchannel, яка дозволяє агрегувати декілька портів для підвищення пропускної спроможності та забезпечення вищої надійності мережі. Завдяки цій технології можна збільшити загальну пропускну здатність з'єднань та забезпечити безперервність мережевого сервісу, навіть у випадку збою одного з портів.

Базове налаштування конфігурації пристроїв на прикладі

Rydenko_R3:

hostname Rydenko_R3// призначення назви пристрою

line console 0 // вхід в конфігураційний режим лінії консолі

password cisco // призначення паролю до консолі

login // вимикання анонімного доступу

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

password cisco // призначення паролю до лінії VTY

login // вимикання анонімного доступу

enable secret class // встановлення зашифрованого паролю для привілейного режиму

service password-encryption // шифрування паролів

banner motd # Rydenko_R3# // налаштування банера MOTD

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

transport input ssh // назначення використання протоколу SSH

login local // налаштування локальної аутентифікації

username 12321ck_ Rydenko password admincisco // призначення імені користувача та паролю
ip domain-name Rydenko_R3 // налаштування імені домена
crypto key generate rsa // створення ключа шфируваня
1024 // вибір довжини ключа шифрування

Налаштування Etherchannel на прикладі комутатора:
interface range fa0/1-2
channel-group 1 mode active
interface port-channel 1
switchport mode trunk
switchport trunk allowed vlan all
interface range fa0/3-4
channel-group 2 mode active
interface port-channel 2
switchport mode trunk
switchport trunk allowed vlan all

3.4.1 Вибір та налаштування способу маршрутизації

При створенні мережевої інфраструктури вибір ефективної та надійної системи маршрутизації є життєво необхідним. Вибір на користь протоколу OSPF (Open Shortest Path First) був зумовлений його високою адаптивністю до змін у мережі та здатністю динамічно вибирати найкоротші та найефективніші маршрути для передачі даних. Завдяки своїй ієрархічній структурі та можливостям масштабування, OSPF відмінно підходить для великих корпоративних мереж. Конфігурація OSPF сприяє оптимізації розподілу даних по мережі, мінімізуючи затримки та збої в передачі. Також, протокол DHCP спрощує управління мережею шляхом автоматизації розподілу IP-адрес. У мережах можливо використовувати як статичну, так і динамічну

маршрутизацію; статична вимагає ручного налаштування маршрутів, тоді як динамічна автоматично адаптується до змін, забезпечуючи більшу гнучкість в управлінні.

Налаштування DHCP на прикладі маршрутизатора Rydenko_R3:

```
ip dhcp excluded-address 172.24.153.145 172.24.153.146
ip dhcp excluded-address 172.24.153.161 172.24.153.162
ip dhcp excluded-address 172.24.153.177 172.24.153.180
ip dhcp excluded-address 172.24.153.209 172.24.153.210
ip dhcp pool LAN3-VLAN10
network 172.24.153.144 255.255.255.240
default-router 172.24.153.145
dns-server 172.24.152.100
ip dhcp pool LAN3-VLAN20
network 172.24.153.160 255.255.255.240
default-router 172.24.153.161
dns-server 172.24.152.100
ip dhcp pool LAN3-VLAN30
network 172.24.153.192 255.255.255.224
default-router 172.24.153.209
dns-server 172.24.152.100
```

Для того, щоб користувача різних підмереж могли взаємодіяти один з одним потрібно налаштувати маршрутизацію між мережами.

Налаштування протоколу OSPF на прикладі маршрутизатора Rydenko_R3:

```
router ospf 1
log-adjacency-changes
passive-interface default
no passive-interface GigabitEthernet0/0
no passive-interface GigabitEthernet0/1
no passive-interface GigabitEthernet0/2
```

no passive-interface Serial0/0/0

no passive-interface Serial0/0/1

auto-cost reference-bandwidth 1000

network 172.14.152.0 0.0.0.3 area 0

network 172.14.152.4 0.0.0.3 area 0

network 172.14.152.8 0.0.0.3 area 0

network 209.165.202.0 0.0.0.3 area 0

network 172.24.153.192 0.0.0.31 area 0

network 172.24.153.160 0.0.0.15 area 0

network 172.24.153.144 0.0.0.15 area 0

network 172.24.153.128 0.0.0.15 area 0

На граничному маршрутизаторі Rydenko_R3 налаштовуємо маршрут за замовчуванням до маршрутизатора ISP (інтернет-провайдер) і виконуємо його розповсюдження:

ip route 0.0.0.0 0.0.0.0 209.165.202.2 // налаштовуємо маршрут за замовчуванням

router ospf 1 // увімкнення протоколу

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

Додаємо статичний маршрут до мережі провайдера ISP:

ip route 209.165.201.0 255.255.255.240 209.165.202.2

3.4.2 Налаштування роботи Інтернет

Забезпечення ефективного доступу внутрішніх систем до Інтернету зазвичай включає використання технології Network Address Translation (NAT). NAT трансформує приватні IP-адреси, які застосовуються в межах організації, в публічні IP-адреси, необхідні для з'єднань із зовнішнім світом. Ця функція дозволяє багатьом пристроям в корпоративній мережі взаємодіяти з Інтернетом

через одну або декілька загальних публічних адрес, значно підвищуючи безпеку та ефективність роботи мережі.

NAT також спрощує управління портами, що є критично важливим для координації численних з'єднань через обмежену кількість доступних публічних IP-адрес. Завдяки NAT, кожне з'єднання відрізняється унікальною комбінацією порту та адреси, забезпечуючи відокремленість сесій між численними внутрішніми користувачами та зовнішніми онлайн-ресурсами.

Зокрема, у цій мережі використовується пул адрес для NAT, який варіюється від 209.165.202.5 до 209.165.202.30. Ці публічні IP-адреси використовуються для агрегування зовнішніх з'єднань, ефективно розподіляючи їх серед внутрішніх користувачів і забезпечуючи стабільний доступ до Інтернету.

Впровадження NAT у корпоративну мережу передбачає конфігурацію маршрутизаторів чи файєрволів для перекладу адрес та керування мережевим трафіком, що не лише захищає внутрішню мережу від зовнішніх загроз, але й оптимізує загальне використання мережевих ресурсів.

Давайте розглянемо налаштування NAT, використовуючи як приклад прикордонний маршрутизатор Rydenko_R3:

```
ip nat pool Internet 209.165.200.6 209.165.200.30 netmask 255.255.255.224
ip nat inside source list NAT14 pool Internet
ip nat inside source static 172.24.152.100 209.165.200.3
ip nat inside source static 172.24.153.100 209.165.200.4
ip nat inside source static 172.24.153.210 209.165.200.5
ip classless
ip access-list extended NAT14
deny ip 172.24.152.0 0.0.0.255 172.24.154.0 0.0.0.63
deny ip 172.24.153.128 0.0.0.127 172.24.154.0 0.0.0.63
deny ip 172.24.154.64 0.0.0.63 172.24.154.0 0.0.0.63
deny ip 172.14.152.0 0.0.0.255 172.24.154.0 0.0.0.63
permit ip 172.24.152.0 0.0.0.255 any
```

permit ip 172.24.153.0 0.0.0.127 any

permit ip 172.24.153.128 0.0.0.127 any

permit ip 172.24.154.64 0.0.0.63 any

permit ip 172.14.152.0 0.0.0.255 any

deny ip 172.24.153.0 0.0.0.127 172.24.154.0 0.0.0.63

3.4.3 Налаштування мереж VLAN, маршрутизації між VLAN

Для ефективного управління мережею і розділення трафіку за різними відділами або службами компанії, важливо створити добре структуровані VLAN та налаштувати маршрутизацію між ними. Для розподілу мережі 172.24.153.128/25 на чотири VLAN, включаючи VLAN 99 з 14 хостами, ми спочатку визначимо потрібні розміри підмереж для кожного VLAN. Оскільки ми знаємо, що один VLAN потребує 14 хостів, визначимо потрібні підмережі для трьох інших VLAN згідно з найкращим використанням адресного простору.

Кроки розбиття:

VLAN 99 - потреба 14 хостів:

– Найменша маска, яка забезпечує не менше 14 хостів, це /28, що дозволяє мати до 16 адрес (14 використовуваних для хостів).

– Вибрана підмережа: 172.24.153.128/28 (адреси від 172.24.153.129 до 172.24.153.142 для хостів, 172.24.153.143 - широкомовна).

VLAN 10:

– Вибрана підмережа: 172.24.153.144/28 (адреси від 172.24.153.145 до 172.24.153.158 для хостів).

VLAN 20:

– Вибрана підмережа: 172.24.153.160/28 (адреси від 172.24.153.161 до 172.24.153.174 для хостів).

VLAN 30:

– Вибрана підмережа: 172.24.153.176/27 (адреси від 172.24.153.177 до 172.24.153.206 для хостів).

Резюме розподілу:

VLAN 99: 172.24.153.128/28

– Хости: 172.24.153.129 - 172.24.153.142

– Широкомовна адреса: 172.24.153.143

VLAN 10: 172.24.153.144/28

– Хости: 172.24.153.145 - 172.24.153.158

– Широкомовна адреса: 172.24.153.159

VLAN 20: 172.24.153.160/28

– Хости: 172.24.153.161 - 172.24.153.174

– Широкомовна адреса: 172.24.153.175

VLAN 30: 172.24.153.176/27

– Хости: 172.24.153.177 - 172.24.153.206

– Широкомовна адреса: 172.24.153.207

У таблиці 3.3 наведена адресація під інтерфейсів мережі.

Таблиця 3.3 – Адресація мереж VLAN

Назва	Мережева адреса	/маска	Маска мережі	Діапазон адрес
VLAN10	172.24.153.144	/28	255.255.255.240	172.24.153.145 до 172.24.153.158
VLAN20	172.24.153.160	/28	255.255.255.240	172.24.153.161 до 172.24.153.174
VLAN30	172.24.153.176	/28	255.255.255.224	172.24.153.177 до 172.24.153.206
VLAN99	172.24.153.128	/28	255.255.255.240	172.24.153.129 до 172.24.153.142

Налаштування VLAN на комутаторі:

int range fa0/6-11 // вибір портів

switchport mode access // налаштування портів

switchport access vlan 42 // присвоювання портам влану

int range fa0/12-14

switchport mode access

switchport access vlan 22

int range fa0/15-24

switchport mode access

switchport access vlan 32

int range fa0/1-5

switchport mode trunk // налаштування портів в режим транку

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

Налаштовуємо підінтерфейси на маршрутизаторі для вказаних VLAN:

interface GigabitEthernet0/2.10

encapsulation dot1Q 10

ip address 172.24.153.145 255.255.255.240

interface GigabitEthernet0/2.20

encapsulation dot1Q 20

ip address 172.24.153.161 255.255.255.240

interface GigabitEthernet0/2.30

encapsulation dot1Q 30

ip address 172.24.153.209 255.255.255.224

interface GigabitEthernet0/2.99

encapsulation dot1Q 99

ip address 172.24.153.129 255.255.255.240

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

3.5 Захист інформації в комп’ютерній системі від несанкціонованого доступу

Для забезпечення захисту нашої мережі від неавторизованого доступу, ми застосовуємо технологію AAA (Аутентифікація, Авторизація, Облік). AAA — це інтегрований фреймворк, який допомагає контролювати доступ до мережевих ресурсів, перевіряти ідентифікацію користувачів та збирати дані про їхню активність у мережі. За допомогою протоколів, таких як RADIUS або TACACS+, система AAA забезпечує централізоване управління аутентифікацією і авторизацією користувачів, що прагнуть отримати доступ через різноманітні мережеві пристрої, включаючи комутатори та маршрутизатори.

Однією з ключових переваг використання сервера RADIUS у рамках системи AAA є можливість централізовано обробляти запити на доступ, створюючи єдину точку для аутентифікації та авторизації. Це спрощує управління безпекою мережі, адже адміністраторам не потрібно окремо налаштовувати політики безпеки на кожному пристрої. Такий підхід також покращує загальний рівень безпеки, оскільки всі політики та записи діяльності централізовано збираються та контролюються.

У нашій мережі ми впровадили AAA на всіх маршрутизаторах для створення єдиної, безпечної схеми доступу. Наприклад, на маршрутизаторі Rydenko_R3 ми сконфігурували AAA, що забезпечує не лише аутентифікацію та авторизацію, але й точне відстеження активності користувачів. Це дозволяє нам детально моніторити використання мережевих ресурсів, виявляти можливі порушення і швидко реагувати на будь-які інциденти, пов'язані з безпекою.

```
aaa new-model
radius server host
address ipv4 172.24.153.100 auth-port 1645
key radius123
```

aaa authentication login console group radius local

line console 0

login authentication console

aaa authentication login default local

username 12321ck_Rydenko password admin123

line vty 0 15

login authentication default

3.6 Налаштування віртуальної приватної мережі VPN

VPN – це технологія, яка використовується для забезпечення безпечного з’єднання в незахищених мережах, таких як Інтернет. В нашому випадку VPN буде використовуватись для підключення з віддаленої мережі до основної.

Налаштування VPN розглянемо на прикладі Rydenko_R0:

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

ip access-list extended VPN14 // створення ACL-списку VPN12, щоб визначити трафік з основної мережі до віддаленої

permit ip 172.24.154.0 0.0.0.63 172.24.152.0 0.0.0.255 // надання доступу на проходження пакетів з основної на віддалену мережу

permit ip 172.24.154.0 0.0.0.63 172.24.153.0 0.0.0.127

permit ip 172.24.154.0 0.0.0.63 172.24.153.128 0.0.0.127

permit ip 172.24.154.0 0.0.0.63 172.24.154.64 0.0.0.63

permit ip 172.24.154.0 0.0.0.63 172.14.152.0 0.0.0.255

crypto isakmp policy 10 // створення криптографічної політики

encr 3des // вибір алгоритму шифрування

hash md5 // вибір алгоритму створення геш-суми

authentication pre-share // вибір методу аутентифікації пірів

group 2

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

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

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

set peer 209.165.202.1 // створення піра

set transform-set TS // вибір набору перетворень

match address VPN12 // прив’язка до списку VPN12

int GigabitEthernet0/1 // вибір інтерфейсу

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

3.7 Перевірка комп’ютерної Системи підприємства

Для аналізу стандартних конфігурацій мережевих пристроїв, ми використовуємо маршрутизатор Rydenko_R3 як зразок. Застосовуючи команду show running-config, ми оглядаємо основні параметри налаштувань, включно з іменем пристрою, конфігурацією паролів та налаштуваннями безпеки.

Першочергово, ми звертаємо увагу на ім'я пристрою, яке допомагає у розпізнаванні маршрутизатора у мережі. Це критично важливо для забезпечення консистенції в номенклатурі пристроїв, спрощуючи таким чином управління мережею.

Далі ми аналізуємо налаштування пароля для доступу через консольний порт, критичний аспект безпеки, що забороняє несанкціонований фізичний доступ до маршрутизатора. Також ми розглядаємо налаштування паролів для віддаленого доступу через vty лінії та використання протоколу SSH для забезпечення шифрованого з'єднання, що покращує безпеку при дистанційному адмініструванні.

Крім того, ми перевіряємо налаштування пароля для доступу до привілейованого режиму, що становить додатковий захист від

несанкціонованих дій та потенційного зловживання. Огляд також включає перевірку банера MOTD (Message of the Day), який використовується для відображення важливих повідомлень користувачам при спробі входу в систему, нагадуючи про правила безпеки.

Нарешті, ми переглядаємо користувацькі імена та паролі, а також ім'я домену, що має значення для інтеграції маршрутизатора в загальну структуру домену мережі. Такий всеохоплюючий огляд налаштувань не тільки підтверджує правильність конфігурацій, але й гарантує високий рівень безпеки та ефективності в управлінні мережею.

```
!
hostname Rydenko_R3
!
```

Рисунок 3.2 – Назва пристрою

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

Рисунок 3.3 – Пароль до консолі

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

Рисунок 3.4 – Пароль до ліній vty та використання на них протоколу ssh

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

Рисунок 3.5 – Пароль до привілейованого режиму

```
!
banner motd ^CRydenko_R3^C
!
```

Рисунок 3.6 – Банер MOTD

```
username 12321ck_Rydenko password 7 0820484300170 61E010803
username Rydenko password 7 082048430017544541
!
```

Рисунок 3.7 – Ім’я користувача та пароль

```
!
ip domain-name Rydenko_R3
!
```

Рисунок 3.8 – Ім’я домена

Як бачимо, усі паролі зашифровані. Наступним етапом перевіряємо технологію EtherChannel у віддаленій мережі LAN_1 (рис. 3.9).

```
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 3.9 – Технологія EtherChannel

Для аналізу конфігурації маршрутизаторів у нашій мережі ми використовуємо маршрутизатор Rydenko_R3 як приклад. Ми зосереджуємося на перевірці налаштувань протоколу OSPF, який є важливим для розподілу трафіку в складних мережах. Використовуючи команду show ip protocols, ми

отримуємо інформацію про активні протоколи маршрутизації, стан OSPF-сусідств, параметри таймерів та мережі, задіяні в маршрутизації. Це дозволяє нам не тільки перевіряти налаштування на точність, але й виявляти помилки, що можуть впливати на роботу мережі

```
Rydenko_R3#show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 209.165.202.2
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.14.152.0 0.0.0.3 area 0
    172.14.152.4 0.0.0.3 area 0
    172.14.152.8 0.0.0.3 area 0
    209.165.202.0 0.0.0.3 area 0
    172.24.153.192 0.0.0.31 area 0
    172.24.153.160 0.0.0.15 area 0
    172.24.153.144 0.0.0.15 area 0
    172.24.153.128 0.0.0.15 area 0
  Passive Interface(s):
    Vlan1
    GigabitEthernet0/2.10
    GigabitEthernet0/2.20
    GigabitEthernet0/2.30
    GigabitEthernet0/2.99
  Routing Information Sources:
    Gateway         Distance      Last Update
    172.24.152.1         110      00:09:57
    172.24.153.1         110      00:10:06
    172.24.154.1         110      00:06:51
    172.24.154.65        110      00:09:20
    209.165.202.1        110      00:17:26
    209.165.202.2        110      00:22:20
  Distance: (default is 110)
```

Рисунок 3.10 – Налаштований OSPF

На рис. 3.11, наведено зв’язок між різними підмережами на прикладі підмереж LAN_4 та LAN_2 є успішним.

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Failed	PC15	PC0	ICMP		0.000	N	0	(edit)	
	Successful	PC15	PC0	ICMP		0.000	N	1	(edit)	
	Successful	PC0	PC15	ICMP		0.000	N	2	(edit)	

Рисунок 3.11 – Зв’язок між LAN_4 та LAN_2

Використовуючи команду show ip route static, ми проводимо аналіз налаштувань статичного маршруту, зокрема маршруту за замовчуванням, на маршрутизаторі, який має безпосереднє підключення до інтернет-провайдера.

```
      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 3.12 – Налаштований маршрут за замовчуванням на маршрутизаторі

Перевіряємо налаштування всіх маршрутизаторів на підтримку служби AAA на прикладі Rydenko_R3. Як бачимо, при вході система запитує логін та пароль (рис. 3.13).

```
Rydenko_R3

User Access Verification

Username: Rydenko
Password:
Rydenko_R3>
```

Рисунок 3.13 – Налаштований маршрутизатор на підтримку служби AAA

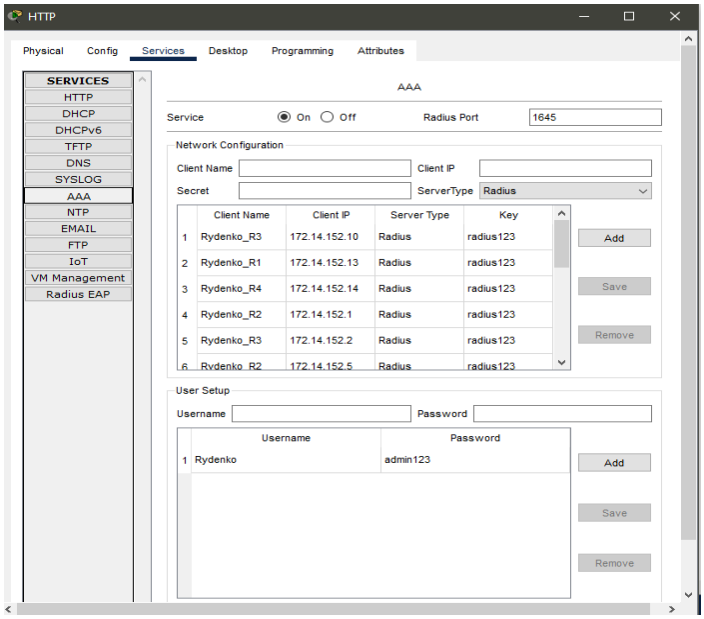

Рисунок 3.14 – Налаштування RADIUS-сервера

Налаштування DHCP перевіряємо на прикладі комп'ютера, який знаходиться в LAN_1 (рис. 3.15).

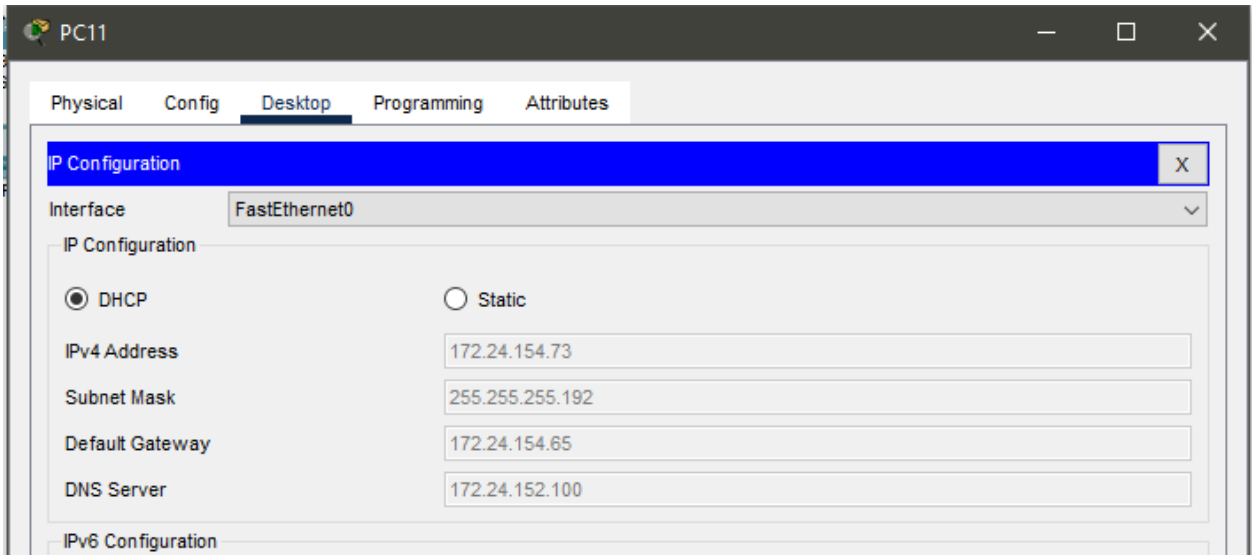

Рисунок 3.15 – Ip-адреса PC11

Перевіряємо транкові порти (рис. 3.16)

```
Port        Mode         Encapsulation  Status        Native
vlan
Fa0/1       on           802.1q         trunking      100

Port        Vlans allowed on trunk
Fa0/1       22,32,42,99-100

Port        Vlans allowed and active in management domain
Fa0/1       22,32,42,99,100

Port        Vlans in spanning tree forwarding state and not
pruned
Fa0/1       22,32,42,99,100
```

Рисунок 3.16 – Транкові порти

Перевіряємо налаштування DHCP для VLAN на прикладі PC15, який знаходиться в VLAN10

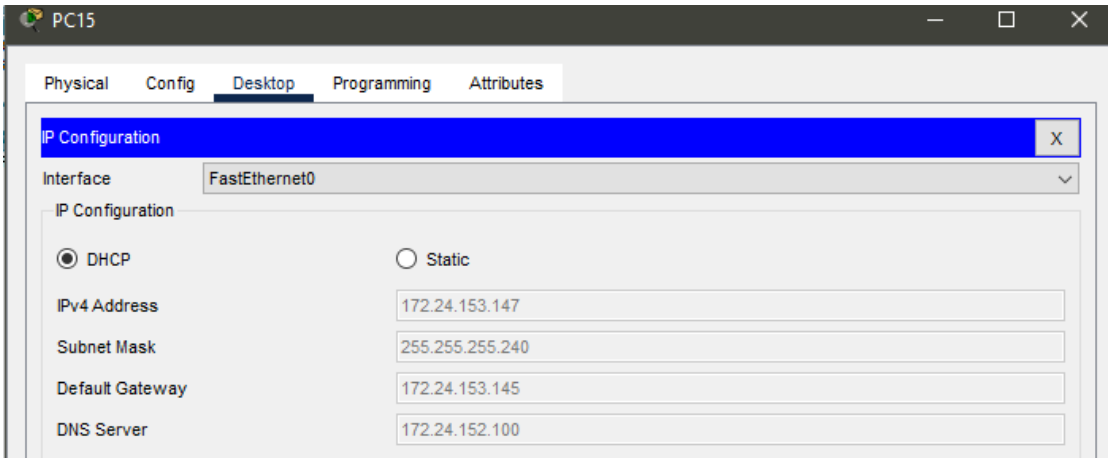

Рисунок 3.17 – IP-адреса PC15

Як бачимо на рисунку нижчу, зв'язок між PC13 та PC14, які знаходять в VLAN20 та VLAN30 відповідно, є успішним.

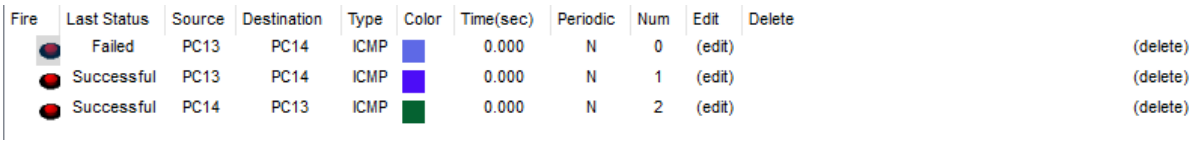

Рисунок 3.18 – Зв'язок між VLAN

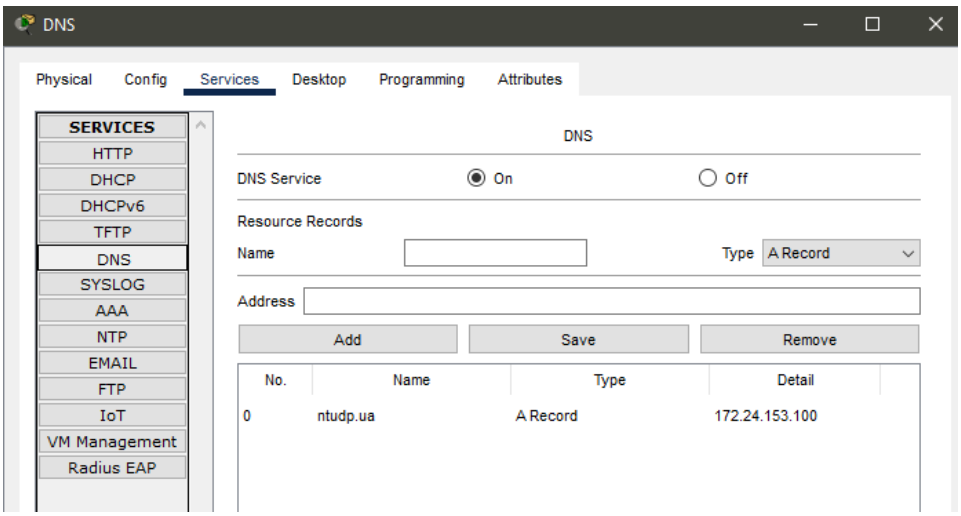

Рисунок 3.19 – DNS сервер

Перевіряємо відкриття веб-сайту з відомостями про тему та завдання на кваліфікаційну роботу студента на прикладі PC3 (рис. 3.10)

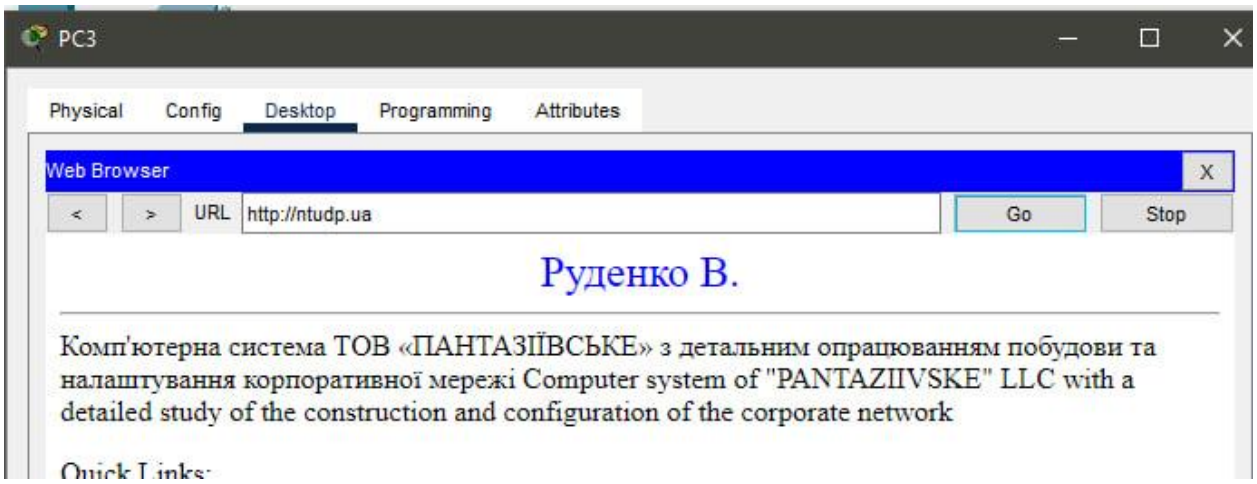

Рисунок 3.20 – Відкритий веб-сайт з відомостями про тему та завдання на кваліфікаційну роботу студента

4 РОЗРОБКА КОМПОНЕНТА СИСТЕМИ

4.1 Інженерне рішення по розробці компонента Системи

За завданням розробника створено систему безпеки головного офісу компанії, окремо від віддаленої мережі. Система являю собою компонент контролю доступу до приміщень за допомогою RFID зчитувачів та міток які керують дверями, нічну систему відеоспостереження(за замовленням компанії), систему сповіщення у локальній мережі де є спрацювання Trip сенсора та у мережі охорони, створеної спеціально для потреб компанії. Розробка компонента задіяє концепцію IoT.

IoT, або Інтернет речей, це концепція підключення будь-яких пристроїв до Інтернету або інших пристроїв. Це включає в себе все, від звичайних побутових приладів, таких як холодильники та мікрохвильові печі, до складніших систем, таких як машини, що взаємодіють між собою в промислових установках. IoT дозволяє об'єктам збирати та обмінюватися даними через мережу, ефективно

інтегруючи фізичний світ з комп'ютерними системами, що збільшує ефективність, точність і економічну вигоду.

4.2 Налаштування обладнання та сервісів системи IoT

Для розгортання IoT-системи в мережі спочатку додаємо та налаштовуємо підмережу для охорони з адресом 172.24.155.0/25 та на кордонному з мережою маршрутизаторі налаштовуємо пул адрес для DHCP та додаємо мережу до OSPF протоколу маршрутизації(рис. 4.1–4.3). Далі встановлюємо IoT-пристрої та датчики, підключаючи їх до Home Gateway. На цих Home Gateway в мережі налаштовуємо бездротову точку доступу, використовуючи як приклад мережу LAN1 з SSID "Rydneko_LAN1" та паролем "Rydneko_LAN112321ck1", вдаючись до протоколу безпеки WPA2-PSK та методу шифрування AES.

```
ip dhcp pool security
 network 172.24.155.0 255.255.255.128
 default-router 172.24.155.1
 dns-server 172.24.152.100
!
```

Рисунок 4.1 – Налаштування пулу адрес

```
router ospf 1
 log-adjacency-changes
 passive-interface default
 no passive-interface GigabitEthernet0/0
 no passive-interface GigabitEthernet0/1
 no passive-interface Serial0/0/0
 network 172.14.152.12 0.0.0.3 area 0
 network 172.14.152.8 0.0.0.3 area 0
 network 172.24.152.0 0.0.0.255 area 0
 network 172.24.155.0 0.0.0.127 area 0
```

Рисунок 4.2 – Налаштування OSPF

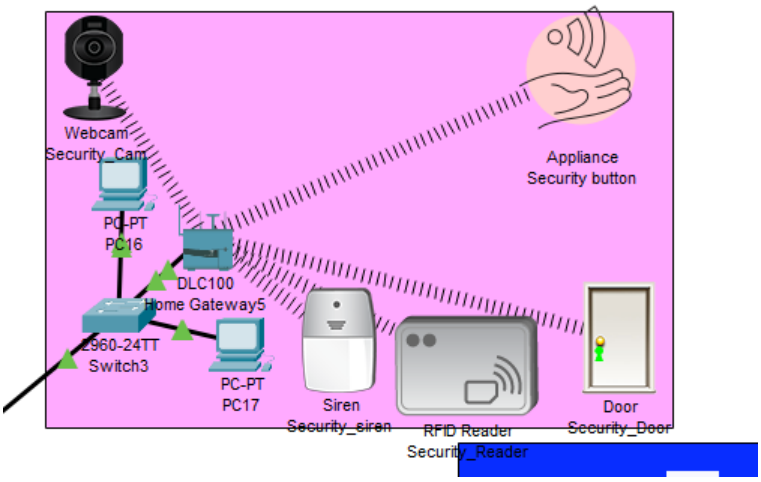

Рисунок 4.3 – Топологі підмережі охорони

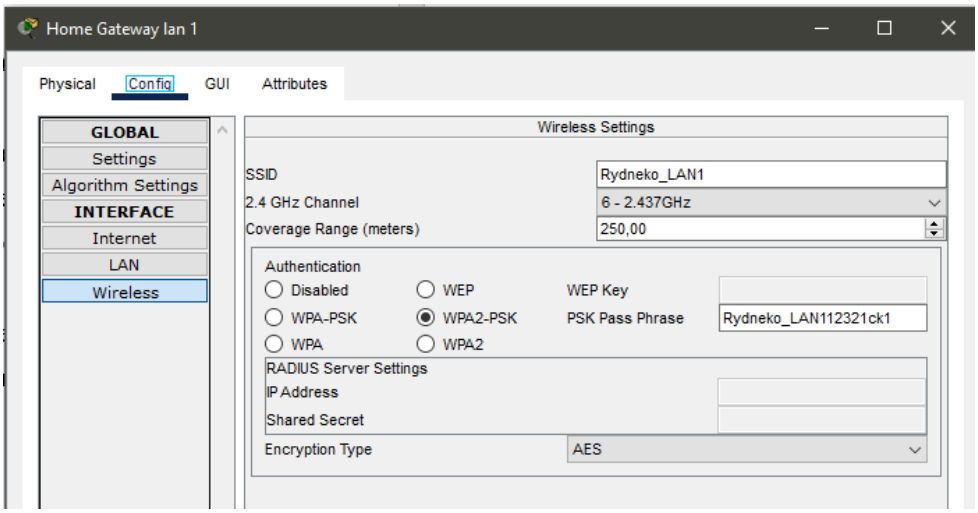

Рисунок 4.4 – Налаштування бездротової мережі

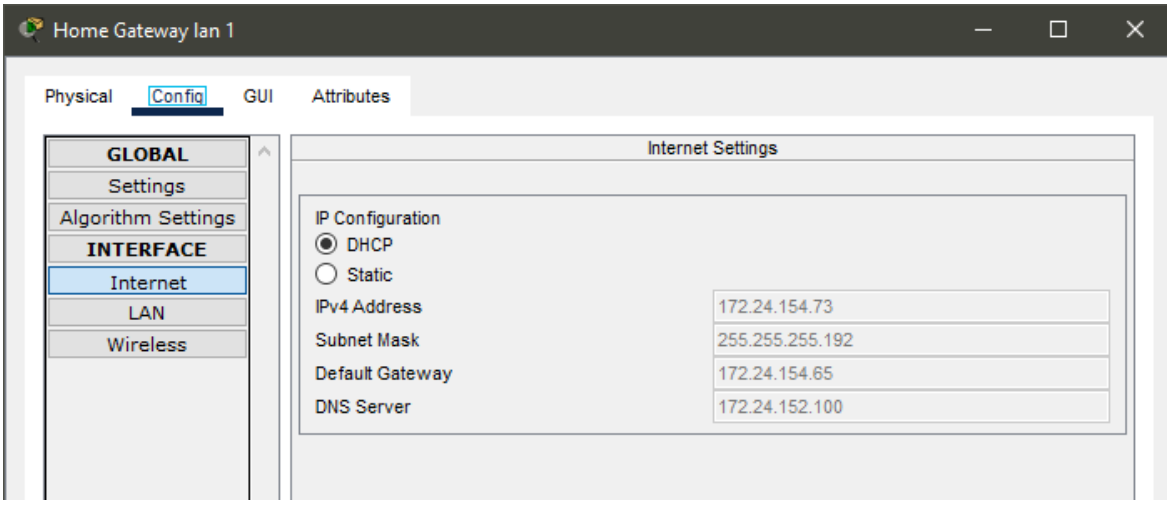

Рисунок 4.5 – Налаштування підключення до LAN1

Для інтеграції кожного IoT-пристрою в корпоративну мережу необхідно налаштувати з'єднання з Home Gateway. Це здійснюється шляхом конфігурації кожного пристрою з використанням унікальних ідентифікаторів мережі (SSID) та відповідних паролів для доступу. Завдяки цьому забезпечується безпечне та надійне підключення до мережі.

Для обробки та управління даними, які надсилають IoT-пристрої, в мережі LAN2 використовується спеціалізований HTTP сервер. Цей сервер має IP-адресу 172.24.153.100 і є центральним вузлом для збору та аналізу інформації від різноманітних пристроїв, підключених до мережі.

На рисунку 4.8 представлена топологічна схема, що ілюструє розташування всіх IoT-пристроїв у корпоративній мережі. Ця схема дає змогу легко ідентифікувати та аналізувати розміщення та з'єднання різних компонентів мережі, спрощуючи управління мережею та пошук та усунення можливих неполадок.

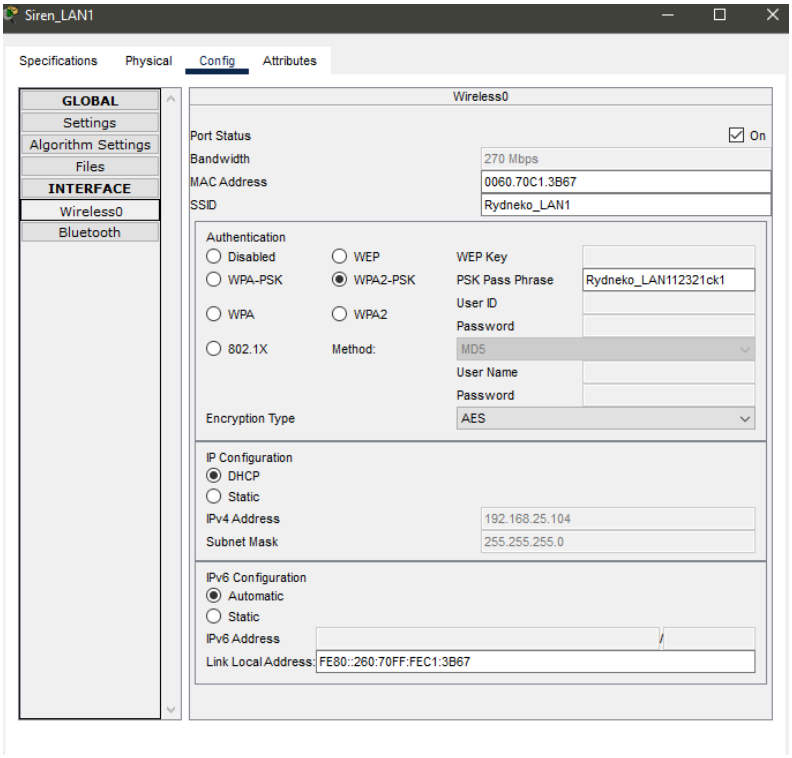

Рисунок 4.6 – Налаштування бездротової мережі на пристроях

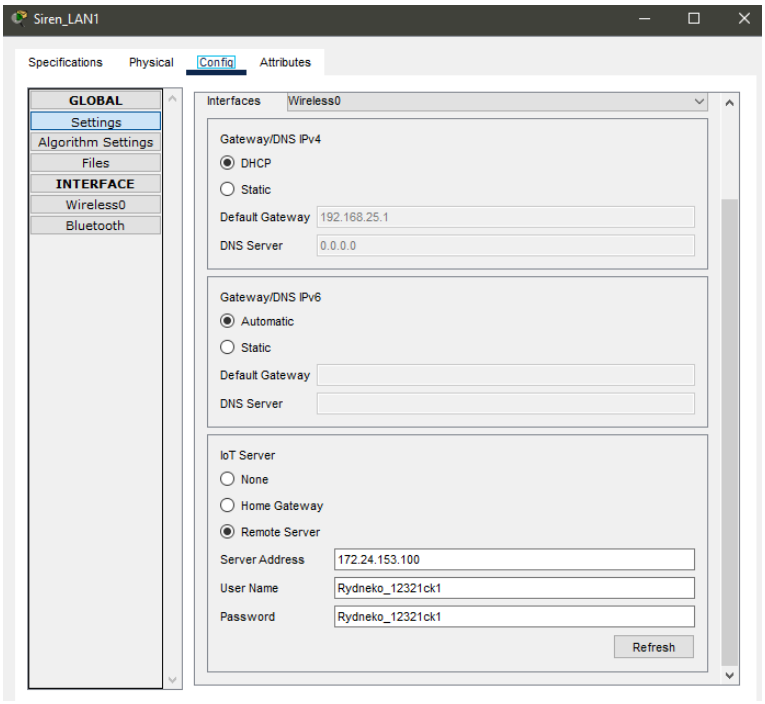

Рисунок 4.7 – Налаштування підключення до віддаленого серверу

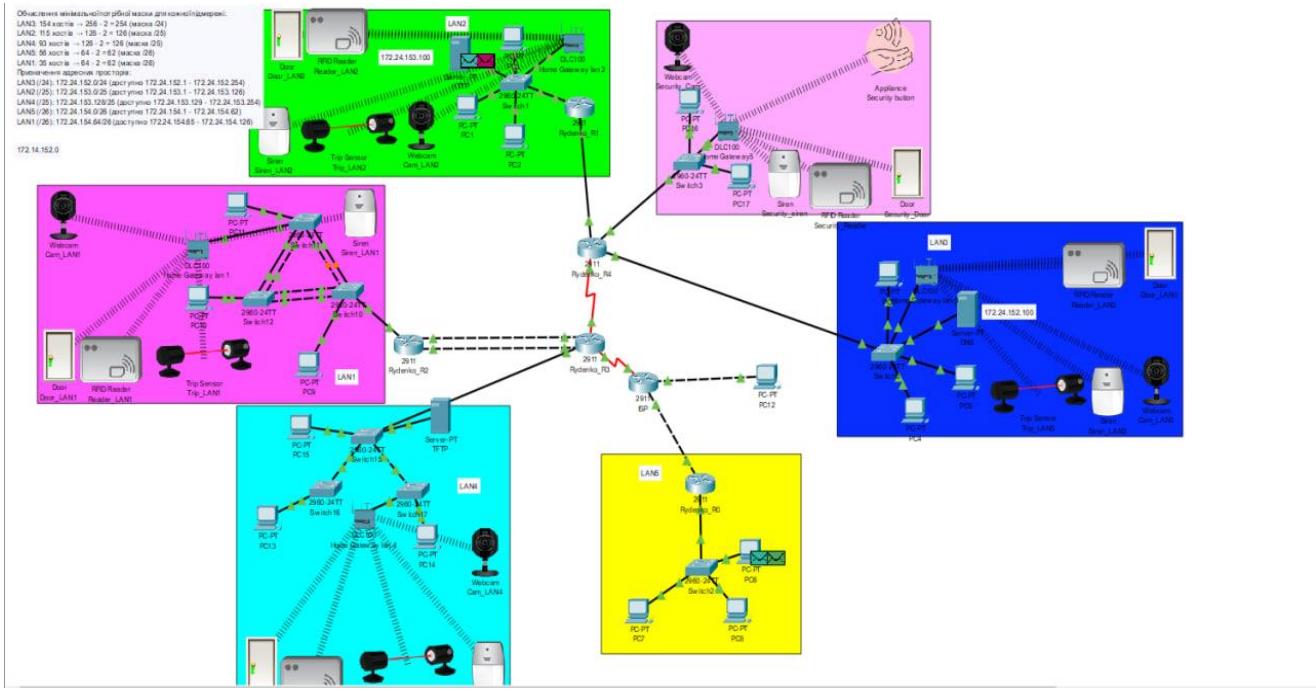

Рисунок 4.8 – Топологічна схема корпоративної мережі компанії з розміщенням IoT пристроїв

Щоб налаштувати роботу IoT-системи на комп'ютері всередині мережі, необхідно використати програму IoT Monitor. Цей інструмент дозволяє централізовано управляти IoT-пристроями. У інтерфейсі програми потрібно ввести адресу шлюзу та облікові дані для підключення до мережі. Після авторизації доступ до управління IoT-пристроями здійснюється через головну сторінку програми, де ви можете переглянути список підключених пристроїв, їх статус та основні характеристики. Інтерфейс зазвичай відображає цю інформацію у формі таблиці або сітки. На рисунку 4.6 можна побачити веб-інтерфейс IoT Monitor з прикладом візуалізації підключених пристроїв.

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

Для системи, створено такі сценарії:

– для системи доступу створено по 3 сценарії на кожну підмережу, при виконанні першого, це при валідному значені зчитувача відкриваються двері, при інших сигналах з зчитувача двері зачиняються. Та сценарій для валідного значення зчитувача, при зчитуванні картки з унікальним номером надсилається валідне значення;

– для нічного керування камерами створено сценарій де при ввімкнені особливого вимикача у підмережі охорони вмикаються всі камери;

– та при вмиканні того ж security вимикача починають робити Trip сенсори та сирени при їх спрацюванні.

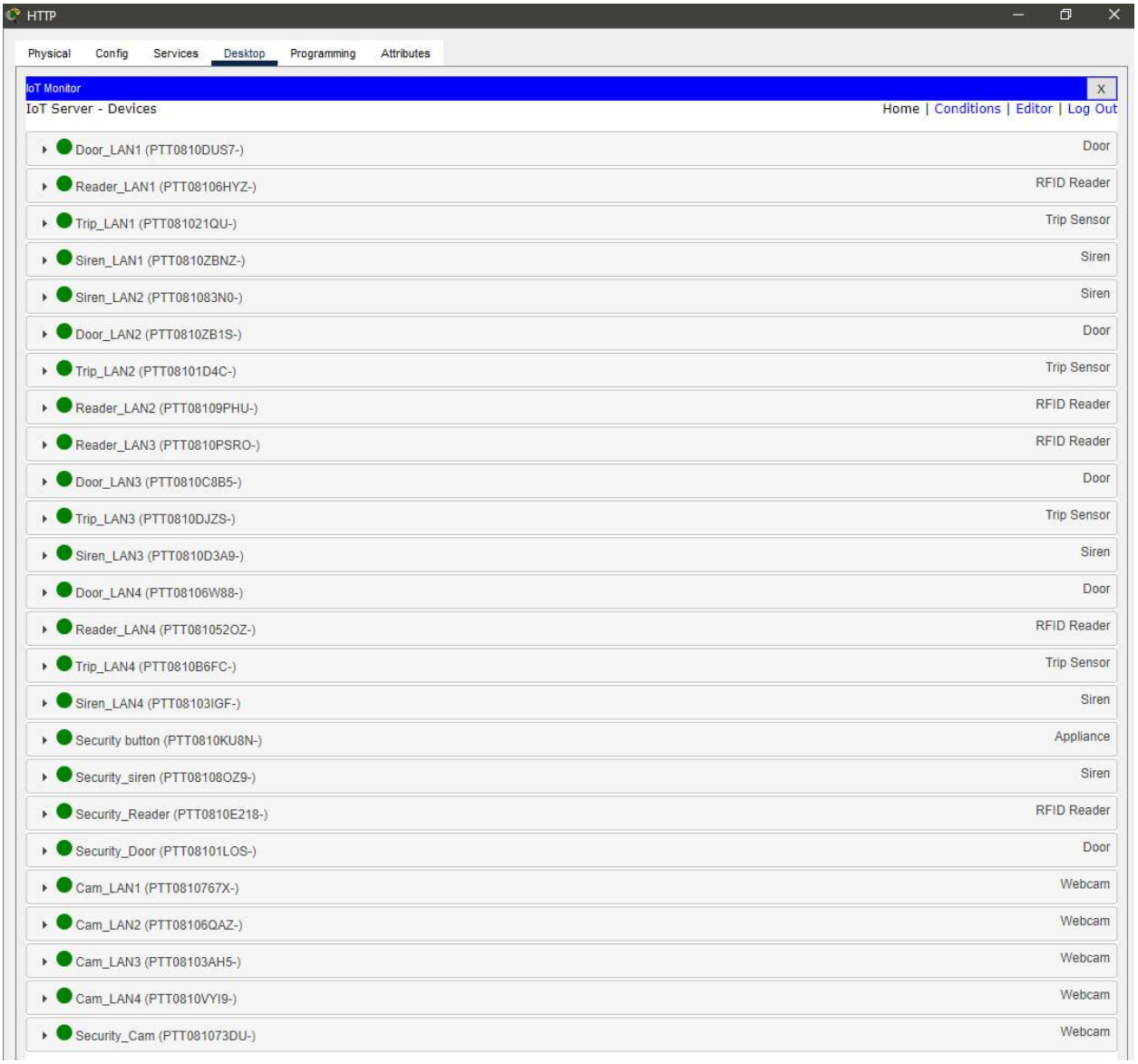

Рисунок 4.9 – Під’єднані IoT-пристрої основної мережі

HTTP

Physical Config Services Desktop Programming Attributes

IoT Monitor

IoT Server - Device Conditions

Home | Conditions | Editor | Log Out

Actions	Enabled	Name	Condition	Actions
Edit Remove	Yes	LAN1_Door_open	Match all: • Security button On is false • Reader_LAN1 Status is Valid	Set Door_LAN1 Lock to Unlock
Edit Remove	Yes	LAN2_Door_open	Match all: • Security button On is false • Reader_LAN2 Status is Valid	Set Door_LAN2 Lock to Unlock
Edit Remove	Yes	LAN3_Door_open	Match all: • Security button On is false • Reader_LAN3 Status is Valid	Set Door_LAN3 Lock to Unlock
Edit Remove	Yes	LAN4_Door_open	Match all: • Reader_LAN4 Status is Valid • Security button On is false	Set Door_LAN4 Lock to Unlock
Edit Remove	Yes	Security_Door_open	Security_Reader Status is Valid	Set Security_Door Lock to Unlock
Edit Remove	Yes	LAN1_Door_close	Reader_LAN1 Status is Waiting	Set Door_LAN1 Lock to Lock
Edit Remove	Yes	LAN2_Door_close	Reader_LAN2 Status is Waiting	Set Door_LAN2 Lock to Lock
Edit Remove	Yes	LAN3_Door_close	Reader_LAN3 Status is Waiting	Set Door_LAN3 Lock to Lock
Edit Remove	Yes	LAN4_Door_close	Reader_LAN4 Status is Waiting	Set Door_LAN4 Lock to Lock
Edit Remove	Yes	Sesurity_Door_close	Security_Reader Status is Waiting	Set Security_Door Lock to Lock
Edit Remove	Yes	LAN1_Reader_Valid	Reader_LAN1 Card ID = 1	Set Reader_LAN1 Status to Valid
Edit Remove	Yes	LAN2_Reader_Valid	Reader_LAN2 Card ID = 2	Set Reader_LAN2 Status to Valid
Edit Remove	Yes	LAN3_Reader_Valid	Reader_LAN3 Card ID = 3	Set Reader_LAN3 Status to Valid
Edit Remove	Yes	LAN4_Reader_Valid	Reader_LAN4 Card ID = 4	Set Reader_LAN4 Status to Valid
Edit Remove	Yes	Security_Reader_Valid	Security_Reader Card ID = 1000	Set Security_Reader Status to Valid
Edit Remove	Yes	Security_Siren_LAN1	Match all: • Security button On is true • Trip_LAN1 On is true	Set Security_siren On to true Set Siren_LAN1 On to true
Edit Remove	Yes	Security_Siren_LAN2	Match all: • Security button On is true • Trip_LAN2 On is true	Set Siren_LAN2 On to true Set Security_siren On to true
Edit Remove	Yes	Security_Siren_LAN3	Match all: • Trip_LAN3 On is true • Security button On is true	Set Security_siren On to true Set Siren_LAN3 On to true
Edit Remove	Yes	Security_Siren_LAN4	Match all: • Security button On is true • Trip_LAN4 On is true	Set Security_siren On to true Set Siren_LAN4 On to true
Edit Remove	Yes	Security_Siren_OFF	Match all: • Trip_LAN1 On is false • Trip_LAN2 On is false • Trip_LAN3 On is false • Trip_LAN4 On is false	Set Siren_LAN2 On to false Set Siren_LAN1 On to false Set Siren_LAN3 On to false Set Siren_LAN4 On to false Set Security_siren On to false
Edit Remove	Yes	Cam_ON	Security button On is true	Set Security_Cam On to true Set Cam_LAN2 On to true Set Cam_LAN1 On to true Set Cam_LAN3 On to true Set Cam_LAN4 On to true
Edit Remove	Yes	Cam_OFF	Security button On is false	Set Cam_LAN4 On to false Set Cam_LAN1 On to false Set Cam_LAN2 On to false Set Cam_LAN3 On to false Set Security_Cam On to false

Add

Рисунок 4.10 – Сценарії мережі

4.3 Перевірка роботи компонента Системи

Перевірка системи при наявності валідної ключ картки на прикладі LAN3(рис. 4.11)

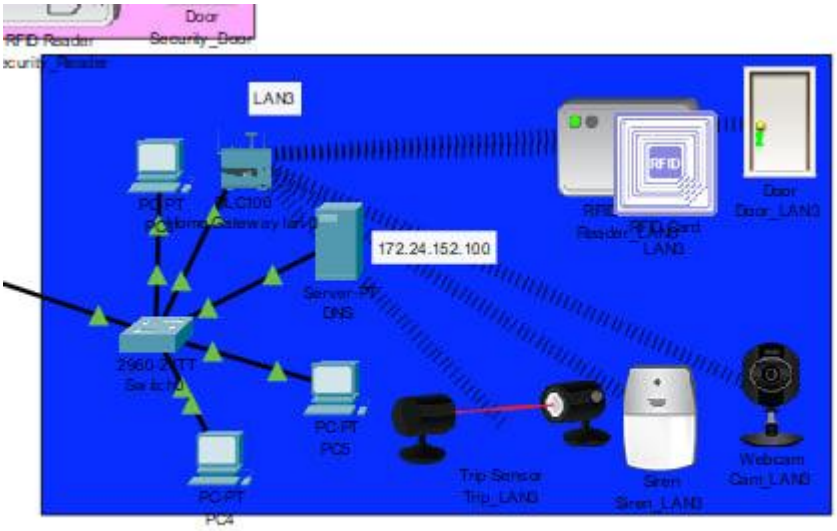

Рисунок 4.11 – Наявність валідної ключ карти

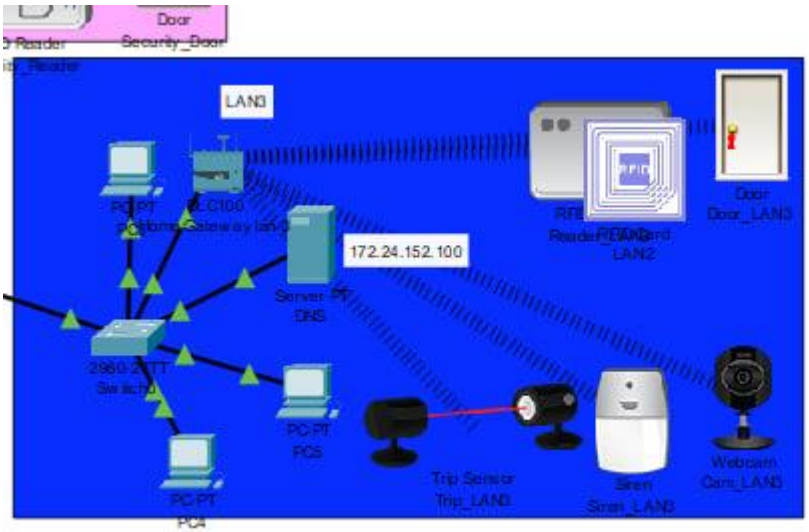

Рисунок 4.12 – Поведінка при іншій картці

Перевірка системи при спрацюванні Trip сенсора у LAN1 (рис. 4.13-14)

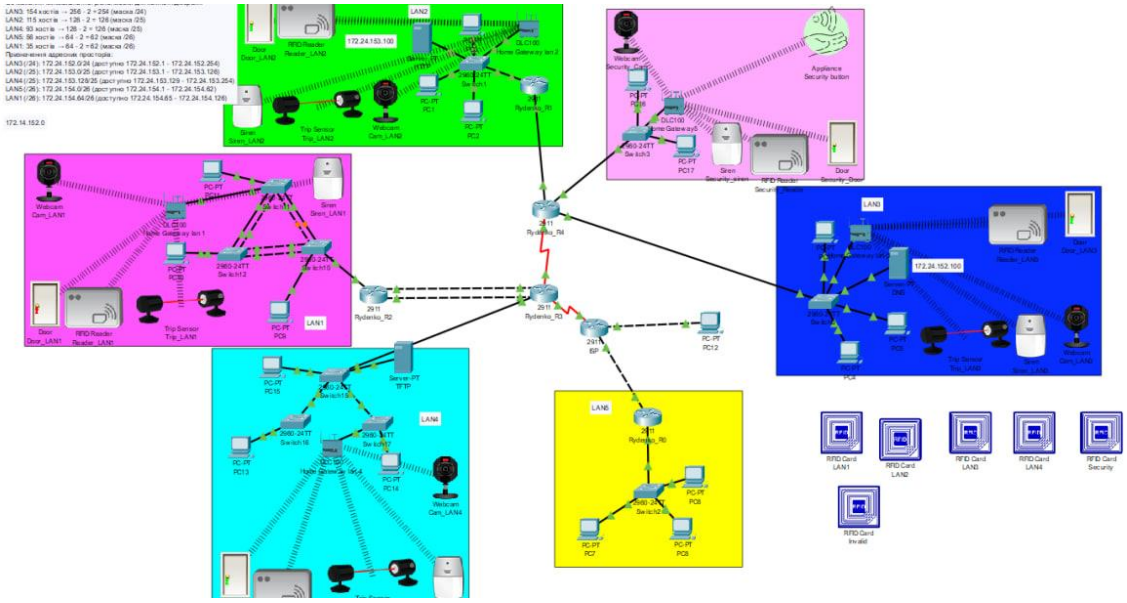

Рисунок 4.13 – Ввімкнена система безпеки

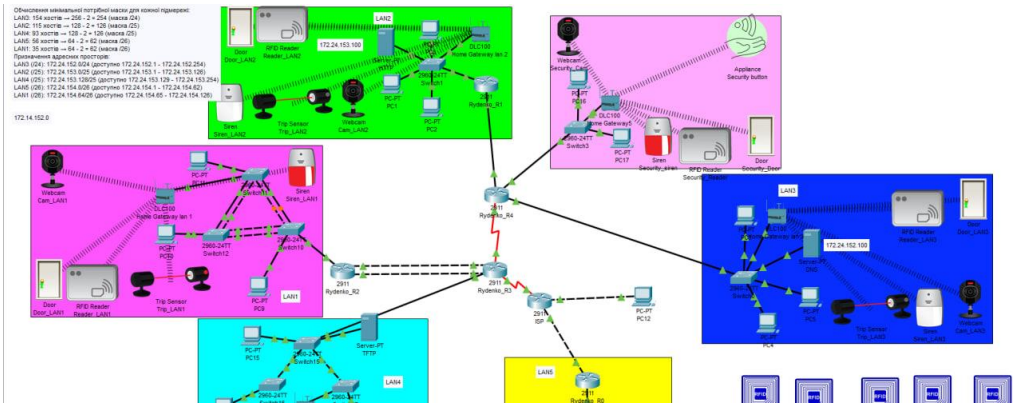

Рисунок 4.14 – Спрацювання сирени у LAN 1

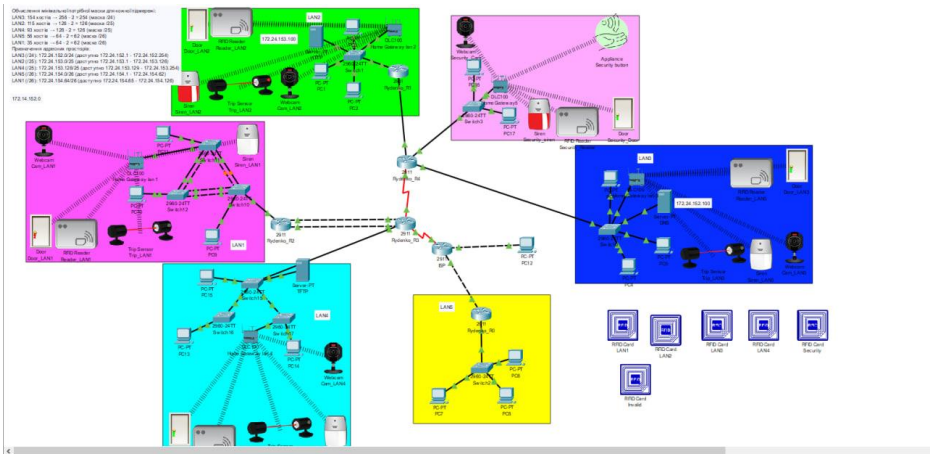

Рисунок 4.15 – Спрацювання сирени у LAN 2

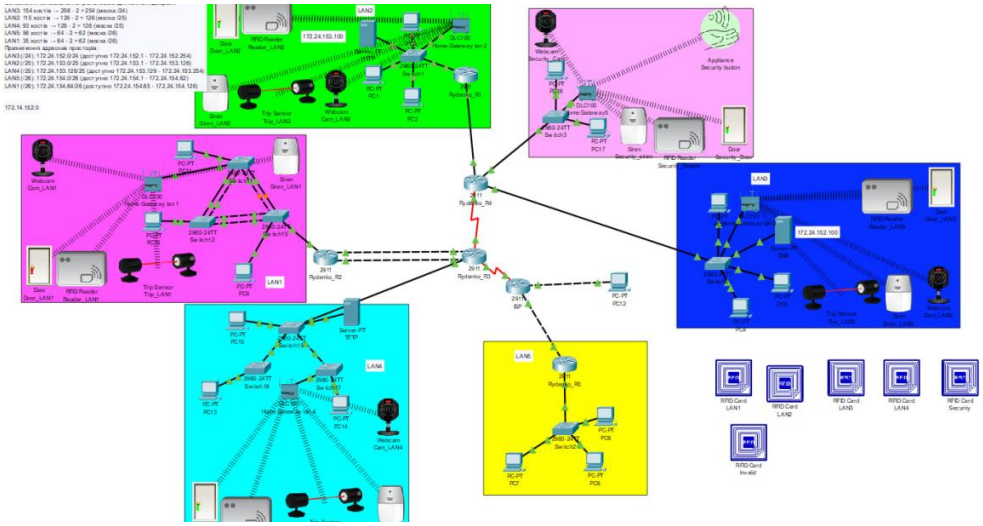

Рисунок 4.16 – Робота камер

ВИСНОВКИ

В даній роботі було проаналізовано ТОВ "ПАНТАЗІЇВСЬКЕ". Детально опрацьована побудова та налаштування корпоративної мережі дозволить компанії забезпечити надійність, безпеку та ефективність у виробничих процесах, обліку, зберіганні та обміні даними.

В результаті аналізу потреб і вимог компанії, розробимо імплементуєму мережеву інфраструктуру, яка враховує специфіку сільського господарства, забезпечуючи необхідну надійність та ефективність. Впровадження запропонованих рішень дозволить підвищити продуктивність праці, зменшити час та витрати на обробку та обмін інформацією, а також забезпечить безпеку та надійність даних.

Також було реалізовано компонент Системи у вигляді IoT-системи безпеки.

Був проведений ретельний огляд об’єкту та прописано вимоги до комп’ютерної Системи. Згідно цих вимог було підібрано необхідно обладнання та побудовано комп’ютерну мережу у середовищі Cisco Packet Tracer.

Згідно завдання була розрахована адресація підмереж та було призначено IP-адресу кожному пристрою.

Соціально-економічна важливість роботи полягає в покращенні бізнес-процесів шляхом підвищення ефективності обробки та обміну даними, скорочення часу на розв'язання інформаційних запитів і підвищення рівня захисту корпоративної інформації.

Отже, вироблені у цій роботі рекомендації і рішення щодо побудови та налаштування корпоративної мережі відповідають потребам і вимогам ТОВ "ПАНТАЗІЇВСЬКЕ", допомагаючи підвищити його конкурентоспроможність та успішність у сучасному бізнес-середовищі.

ПЕРЕЛІК ПОСИЛАНЬ

1. Методичні рекомендації до виконання кваліфікаційної роботи бакалавра студентами галузі знань 12 Інформаційні технології спеціальності 123 Комп'ютерна інженерія / Л.І. Цвіркун, С.М. Ткаченко, Я.В. Панферова, Д.О. Бешта, Л.В. Бешта. – Д.: НТУ «ДП», 2023. – 62 с.

2. Мережа cisco – [Електронний ресурс] – Режим доступу до ресурсу: https://www.cisco.com/site/us/en/products/networking/access-networking/index.html

3. Трой Макміллан « Cisco Networking Essentials » 2011. – 458 с

4. Андрій Ковальов «Безпека корпоративних мереж» / https://ua.kursoviks.com.ua/

5. Iot for all (рекомендації) – [Електронний ресурс] – Режим доступу до ресурсу:https://www.iotforall.com/

6. Налаштування NAT – Education [Електронний ресурс] – Режим доступу до ресурсу: http://surl.li/hsyzr (дата звернення 20.05.2023р.)

7. Налаштування VLAN – Education [Електронний ресурс] – Режим доступу до ресурсу: http://surl.li/hrjwk (дата звернення 23.05.2023р.)

8. ACL списки – Education [Електронний ресурс] – Режим доступу до ресурсу: http://surl.li/hszbq (дата звернення 26.05.2023р.)

9. Налаштування VPN – Education [Електронний ресурс] – Режим доступу до ресурсу: http://surl.li/hrjwr (дата звернення 26.05.2023р.)

10. Інтернет речей – Education [Електронний ресурс] – Режим доступу до ресурсу: http://surl.li/dcsqu (дата звернення 31.05.2023р.)

Додатки

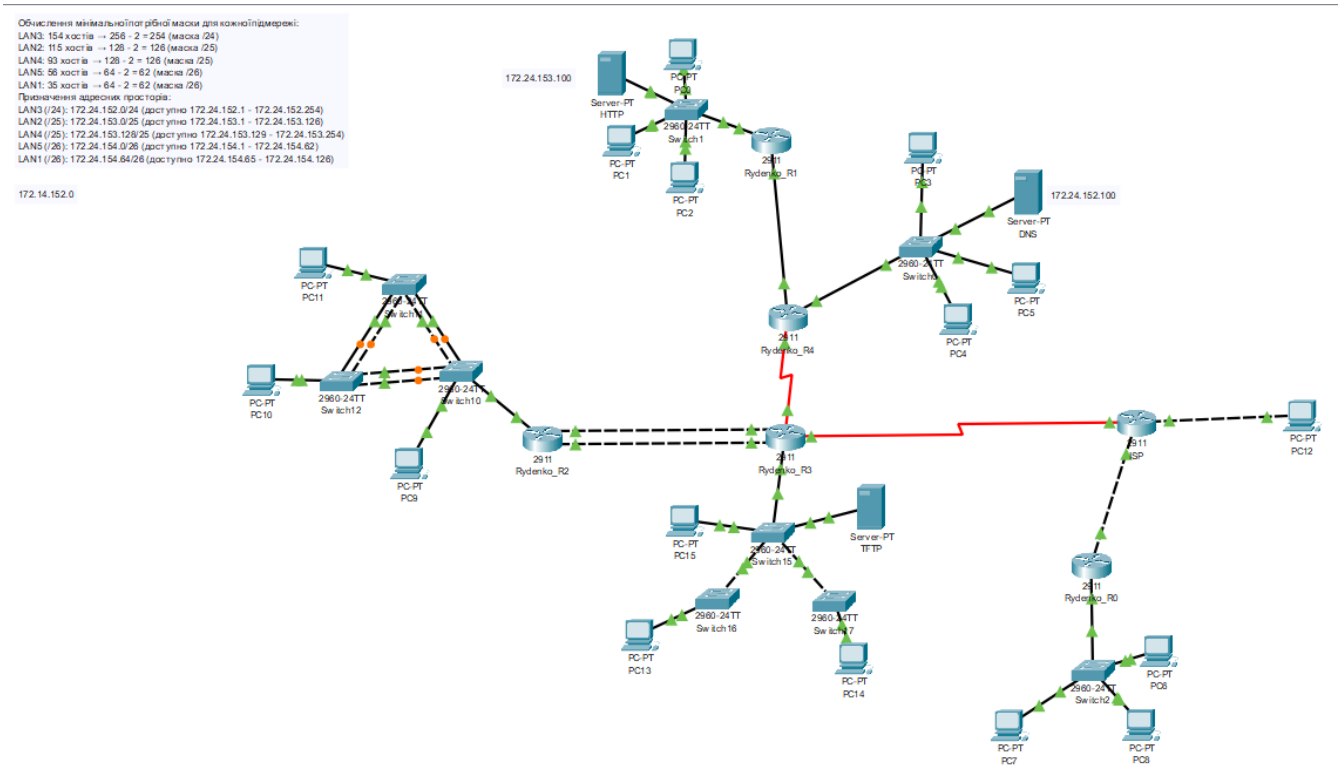

Рисунок ДА.1 – Загальна архітектура мережі ТОВ "ПАНТАЗІЇВСЬКЕ"

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

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ НАЛАШТУВАННЯ МЕРЕЖІ КОМП’ЮТЕРНОЇ СИСТЕМИ

Текст програми

804.02070743.23004-01 12 01

Листів 16

2024

АНОТАЦІЯ

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

ЗМІСТ

1. Rydenko_R2

```
Rydenko_R2#show run
Current configuration : 1918 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Rydenko_R2
!
!
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
!
ip dhcp excluded-address 172.24.154.65 172.24.154.70
!
ip dhcp pool LAN-1
network 172.24.154.64 255.255.255.192
default-router 172.24.154.65
dns-server 172.24.152.100
!
!
aaa new-model
!
aaa authentication login console group radius local
aaa authentication login default local
!
ip cef
no ipv6 cef
```

```
!
!
!
username 12321ck_Rydenko password 7 082048430017061E010803
username Rydenko password 7 082048430017544541
!
!
license udi pid CISCO2911/K9 sn FTX15246PEH-
!
ip domain-name Rydenko_R2
!
!
spanning-tree mode pvst
!
interface GigabitEthernet0/0
ip address 172.14.152.1 255.255.255.252
duplex auto
speed auto
!
interface GigabitEthernet0/1
ip address 172.14.152.5 255.255.255.252
duplex auto
speed auto
!
interface GigabitEthernet0/2
ip address 172.24.154.65 255.255.255.192
duplex auto
speed auto
!
interface Vlan1
no ip address
```

```
shutdown
!
router ospf 1
log-adjacency-changes
passive-interface default
no passive-interface GigabitEthernet0/0
no passive-interface GigabitEthernet0/1
no passive-interface GigabitEthernet0/2
network 172.14.152.0 0.0.0.3 area 0
network 172.14.152.4 0.0.0.3 area 0
network 172.24.154.64 0.0.0.63 area 0
!
ip classless
!
ip flow-export version 9
!
!
!
banner motd ^CRydenko_R2^C
!
radius server host
address ipv4 172.24.153.100 auth-port 1645
key radius123
radius server 172.24.153.100
address ipv4 172.24.153.100 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. Rydenko_R3

```
Rydenko_R3#show run
Current configuration : 4019 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Rydenko_R3
!
!
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
```

```
!
ip dhcp excluded-address 172.24.153.145 172.24.153.146
ip dhcp excluded-address 172.24.153.161 172.24.153.162
ip dhcp excluded-address 172.24.153.177 172.24.153.180
ip dhcp excluded-address 172.24.153.209 172.24.153.210
!
ip dhcp pool LAN3-VLAN10
network 172.24.153.144 255.255.255.240
default-router 172.24.153.145
dns-server 172.24.152.100
ip dhcp pool LAN3-VLAN20
network 172.24.153.160 255.255.255.240
default-router 172.24.153.161
dns-server 172.24.152.100
ip dhcp pool LAN3-VLAN30
network 172.24.153.192 255.255.255.224
default-router 172.24.153.209
dns-server 172.24.152.100
!
!
aaa new-model
!
aaa authentication login console group radius local
aaa authentication login default local
!
no ip cef
no ipv6 cef
!
!
!
username 12321ck_Rydenko password 7 082048430017061E010803
```

```
username Rydenko password 7 082048430017544541
!
!
license udi pid CISCO2911/K9 sn FTX15246LMN-
!
ip domain-name Rydenko_R3
!
!
spanning-tree mode pvst
!
interface GigabitEthernet0/0
ip address 172.14.152.2 255.255.255.252
ip nat inside
duplex auto
speed auto
!
interface GigabitEthernet0/1
ip address 172.14.152.6 255.255.255.252
ip nat inside
duplex auto
speed auto
!
interface GigabitEthernet0/2
no ip address
ip nat inside
duplex auto
speed auto
!
interface GigabitEthernet0/2.10
encapsulation dot1Q 10
ip address 172.24.153.145 255.255.255.240
```

```
!
interface GigabitEthernet0/2.20
encapsulation dot1Q 20
ip address 172.24.153.161 255.255.255.240
!
interface GigabitEthernet0/2.30
encapsulation dot1Q 30
ip address 172.24.153.209 255.255.255.224
!
interface GigabitEthernet0/2.99
encapsulation dot1Q 99
no ip address
!
interface Serial0/0/0
ip address 172.14.152.10 255.255.255.252
ip nat inside
clock rate 148000
!
interface Serial0/0/1
ip address 209.165.202.2 255.255.255.252
ip nat outside
!
interface Vlan1
no ip address
shutdown
!
router ospf 1
log-adjacency-changes
passive-interface default
no passive-interface GigabitEthernet0/0
no passive-interface GigabitEthernet0/1
```

```
no passive-interface GigabitEthernet0/2
no passive-interface Serial0/0/0
no passive-interface Serial0/0/1
auto-cost reference-bandwidth 1000
network 172.14.152.0 0.0.0.3 area 0
network 172.14.152.4 0.0.0.3 area 0
network 172.14.152.8 0.0.0.3 area 0
network 209.165.202.0 0.0.0.3 area 0
network 172.24.153.192 0.0.0.31 area 0
network 172.24.153.160 0.0.0.15 area 0
network 172.24.153.144 0.0.0.15 area 0
network 172.24.153.128 0.0.0.15 area 0
!
router rip
!
ip nat pool Internet 209.165.200.6 209.165.200.30 netmask 255.255.255.224
ip nat inside source list NAT14 pool Internet
ip nat inside source static 172.24.152.100 209.165.200.3
ip nat inside source static 172.24.153.100 209.165.200.4
ip nat inside source static 172.24.153.210 209.165.200.5
ip classless
!
ip flow-export version 9
!
!
ip access-list extended NAT14
deny ip 172.24.152.0 0.0.0.255 172.24.154.0 0.0.0.63
deny ip 172.24.153.128 0.0.0.127 172.24.154.0 0.0.0.63
deny ip 172.24.154.64 0.0.0.63 172.24.154.0 0.0.0.63
deny ip 172.14.152.0 0.0.0.255 172.24.154.0 0.0.0.63
permit ip 172.24.152.0 0.0.0.255 any
```

```
permit ip 172.24.153.0 0.0.0.127 any
permit ip 172.24.153.128 0.0.0.127 any
permit ip 172.24.154.64 0.0.0.63 any
permit ip 172.14.152.0 0.0.0.255 any
deny ip 172.24.153.0 0.0.0.127 172.24.154.0 0.0.0.63
!
banner motd ^CRydenko_R3^C
!
radius server host
address ipv4 172.24.153.100 auth-port 1645
key radius123
radius server 172.24.153.100
address ipv4 172.24.153.100 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. Rydenko_R0

```
Current configuration : 1829 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Rydenko_R0
!
!
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
!
ip dhcp excluded-address 172.24.154.1 172.24.154.5
!
ip dhcp pool LAN-5
network 172.24.154.0 255.255.255.192
default-router 172.24.154.1
dns-server 172.24.152.100
!
!
aaa new-model
!
aaa authentication login console group radius local
aaa authentication login default local
```

```
!
ip cef
no ipv6 cef
!
!
username 12321ck_Rydenko password 7 082048430017061E010803
username Rydenko password 7 082048430017544541
!
!
license udi pid CISCO2911/K9 sn FTX1524FW47-
!
ip domain-name Rydenko_R0
!
!
spanning-tree mode pvst
!
!
interface GigabitEthernet0/0
ip address 64.100.13.1 255.255.255.252
duplex auto
speed auto
!
interface GigabitEthernet0/1
ip address 172.24.154.1 255.255.255.192
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
network 64.100.13.0 0.0.0.3 area 0
network 172.24.154.0 0.0.0.63 area 0
!
router rip
!
ip classless
!
ip flow-export version 9
!
!
!
banner motd ^CRydenko_R0^C
!
radius server host
address ipv4 172.24.153.100 auth-port 1645
key radius123
radius server 172.24.153.100
address ipv4 172.24.153.100 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 : 1386 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
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

5.switch0

Current configuration : 1080 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
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
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
```