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 Лакізи Н.Г.
(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 ВКФ «Інватех» з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі»
(назва за наказом ректора)

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	Шедловський І.А			
спеціальної частини	Шедловський І.А			
розділів:				
розробка апаратної частини	Бешта Д.О			
розробка корпоративної мережі	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 Лакізи Н.Г **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 ВКФ «Інватех» з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі»

затверджену наказом ректора НТУ «Дніпровська політехніка» 11.04.2024 № 256-с
від

Розділ	**Зміст**	**Термін виконання**
Стан питання та постановка завдання	На основі матеріалів виробничих практик, інших науково-технічних джерел розглянути призначення та завдання комп'ютерної системи ТОВ ВКФ «Інватех»	11.04.2024
Розробка апаратної частини	Розробити вимоги до функцій, виконуваними комп'ютерною системою ТОВ ВКФ «Інватех»	1.05.2024
Розробка корпоративної мереж	Побудувати в Packet Tracer модель корпоративної мережі компанії, виконати налаштування та перевірку роботи системи	20.05.2024
Розробка компонента системи	Розробити систему санкціонованого доступу та мікроклімату	4.06.2024

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

Дата видачі 11.04.24

Дата подання до екзаменаційної комісії

Прийнято до виконання Лакіза Н.Г.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 87 с., 35 рис., 4 табл., 1 додаток, 10 джерел. БЕЗПЕКА, ВІРТУАЛЬНІ МЕРЕЖІ, КОРПОРАТИВНА МЕРЕЖА, МЕРЕЖЕВА АРХІТЕКТУРА, МЕРЕЖЕВА БЕЗПЕКА, МІКРОКОНТРОЛЕРИ, МОНІТОРИНГ СИСТЕМ, УПРАВЛІННЯ ДОСТУПОМ, МІКРОКЛІМАТ.

Об’єкт розробки: комп'ютерна система ТОВ ВКФ «Інватех».

Мета роботи: розробка та оптимізація корпоративної мережевої системи з особливим акцентом на підвищення ефективності управління ресурсами та забезпечення безпеки.

Здійснено: детальне проєктування, налаштування та впровадження комплексної мережевої інфраструктури, включно з системами безпеки та автоматизації на основі IoT технологій.

Методи дослідження та апаратура: Використання сучасних методологій проектування мережі, програмного забезпечення для моделювання мережевих систем, а також мікроконтролерів для розробки системи управління кліматом і доступом.

Результати та їх новизна: Створення інтегрованої системи, яка включає в себе механізми розумного управління доступом на базі IoT та ефективне управління кліматом приміщень з використанням даних сенсорів у реальному часі.

Основні конструктивні, технологічні й техніко-експлуатаційні характеристики та показники: Система забезпечує високий рівень безпеки за допомогою технологій шифрування та двофакторної автентифікації, а також автоматизоване управління енергоспоживанням та клімат-контролем.

Інформація щодо впровадження: Система успішно впроваджена у всіх офісах та виробничих цехах компанії, демонструючи значне покращення в роботі мережевої інфраструктури.

Взаємозв’язок з іншими роботами: Робота корелює з глобальними тенденціями у сфері мережевих технологій та безпеки, використовуючи передові практики і стандарти.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

DHCP - Протокол динамічної конфігурації хостів

DNS - Система доменних імен

HTTP - Протокол передачі гіпертексту

HTTPS - Безпечний протокол передачі гіпертексту

IP - Інтернет-протокол

ISP - Провайдер інтернет-послуг

КМ - Комп'ютерна мережа

NAT - Трансляція мережевих адрес

OSPF - Протокол визначення найкоротшого шляху спершу

ПК - Персональний комп'ютер

TCP - Протокол керування передачею

VLAN - Віртуальна локальна мережа

VLSM - Маскування змінної довжини

ВСТУП

У сучасному світі медичних технологій, де швидкість інновацій і стрімке впровадження новітніх рішень визначають лідерів ринку, роль ефективної інформаційної інфраструктури набуває ключового значення. ТОВ ВКФ «Інватех», як провідний виробник медичного обладнання, стикається з необхідністю постійного оновлення своїх технологічних процесів і систем безпеки для підтримки високих стандартів якості та ефективності своєї продукції. Ця робота присвячена розробці та оптимізації корпоративної мережі «Інватех», з акцентом на інтеграції сучасних інженерних рішень, які допоможуть забезпечити не тільки надійність, але й гнучкість управління даними і ресурсами компанії.

Завдання, поставлені перед «Інватех», вимагають комплексного підходу до розробки мережевої архітектури, що включає захист конфіденційної інформації, вдосконалення виробничих ліній та оптимізацію внутрішніх та зовнішніх комунікацій. В контексті цих викликів, робота зосереджується на впровадженні передових технологій таких як IoT (Інтернет речей) для моніторингу стану обладнання, використанні хмарних рішень для збільшення масштабованості та гнучкості, та застосуванні розширених систем безпеки для захисту від кіберзагроз.

Метою цієї роботи є не тільки підвищення оперативної ефективності «Інватех» через технологічні інновації, але й створення умов для сталого розвитку компанії в умовах постійної конкуренції та технологічних змін. Основний акцент зроблено на модернізації та безпеці, як основах для досягнення стратегічних бізнес-цілей та підтримки високого рівня задоволеності клієнтів.

1 СТАН ПИТАННЯ І ПОСТАНОВКА ЗАВДАННЯ

1.1 Стисла характеристика галузі та умов застосування корпоративної мережі

ТОВ ВКФ «Інватех» спеціалізується на виробництві медичного обладнання, ключова галузь, яка відіграє життєво важливу роль у системі охорони здоров'я. Галузь медичних технологій зосереджена на розробці, виробництві та продажу обладнання, яке використовується для діагностики, лікування та моніторингу стану пацієнтів. Оскільки сектор неперервно розвивається завдяки технологічним інноваціям та зростаючим інвестиціям у дослідження та розробки, компанії, як «Інватех», повинні постійно адаптуватися до нових вимог ринку та вдосконалювати свої виробничі процеси.

У контексті виробництва медичного обладнання, корпоративна мережа «Інватех» відіграє критичну роль у забезпеченні ефективності всіх аспектів бізнесу:

1) Інтеграція виробничих процесів: цифровізація виробничих ліній з використанням IoT (Інтернет речей) для моніторингу та управління обладнанням у реальному часі, що дозволяє оптимізувати роботу та скоротити простої.

2) Обмін даними: надійне з'єднання між різними відділами (виробництво, наукові лабораторії, логістика, адміністрація) для швидкого та безпечного обміну даними та інформацією, критичною для оперативного рішення питань.

3) Безпека даних: оскільки компанія обробляє конфіденційні дані, пов'язані з медичними дослідженнями , високий рівень інформаційної безпеки є обов'язковим. Використання шифрування, брандмауерів, антивірусного захисту та інших технологій захисту є необхідними для захисту важливої інформації.

4) Підтримка ділових комунікацій: ефективні комунікації через корпоративну мережу, включаючи електронну пошту, відеоконференції, та внутрішній портал, сприяють підтримці високих стандартів співпраці та обслуговування клієнтів.

Таким чином, корпоративна мережа є фундаментом для сталого розвитку «Інватех», забезпечуючи надійний зв'язок внутрішніх і зовнішніх процесів, підвищення продуктивності та впровадження інновацій.

1.2 Характеристика підприємства та умов застосування КС

ТОВ ВКФ «Інватех» спеціалізується на розробці та виробництві медичного обладнання, зокрема, високотехнологічних медичних приладів для діагностики та лікування. Завдяки своїй інноваційній продукції, компанія займає одне з провідних місць на ринку медичних технологій в Україні. Основні напрями діяльності компанії включають дослідження та розробку новітніх медичних технологій, виробництво медичного обладнання, а також його сервісне обслуговування та ремонт.

Умови застосування комп'ютерної системи

Комп'ютерна система «Інватех» відіграє ключову роль у всіх аспектах діяльності компанії, від дослідження та розробки до виробництва та обслуговування продукції. Система забезпечує централізоване управління ресурсами, оптимізацію процесів та високий рівень захисту корпоративної інформації.

Основні вимоги до комп'ютерної системи включають:

Підтримка досліджень та розробок: необхідність великої обчислювальної потужності для моделювання та аналізу даних. Зберігання та обробка великих обсягів даних з високим рівнем безпеки.

Управління виробничими процесами: автоматизація виробничих ліній і моніторинг стану обладнання через IoT. Централізація управління даними про виробництво, логістику та запаси.

Сервісне обслуговування та підтримка клієнтів: ведення бази даних клієнтів та обладнання. Онлайн підтримка та діагностика через веб-інтерфейси та мобільні додатки.

Безпека та конфіденційність: захист персональних та інтелектуальної власності. Впровадження передових методів шифрування та багаторівневих систем аутентифікації.

Комп'ютерна система «Інватех» повинна бути високонадійною, масштабованою, та легко адаптованою до змінюваних умов ринку та технологій. Інтеграція сучасних ІТ-рішень дозволяє компанії підтримувати високий рівень інновацій та оперативно реагувати на потреби ринку, забезпечуючи високу конкурентоспроможність та якість обслуговування клієнтів.

1.3 Принципи, технічні способи та математичні методи інформаційного забезпечення підприємства

Принципи інформаційного забезпечення:

1) Цілісність даних: забезпечення точності та незмінності даних протягом всього життєвого циклу.

2) Конфіденційність: захист інформації від несанкціонованого доступу або розголошення.

3) Доступність: гарантія доступу до інформаційних ресурсів для уповноважених осіб і систем коли це потрібно.

4) Надійність: Забезпечення безперебійної роботи інформаційних систем та засобів.

5) Масштабованість: спроможність системи адаптуватися до зростаючих обсягів даних або змін в оперативних потребах.

Технічні способи інформаційного забезпечення:

1) Шифрування: використання передових алгоритмів шифрування для захисту даних при зберіганні та передачі.

2) Мережеві брандмауери та IPS (Intrusion Prevention Systems): захист мережі від несанкціонованих доступів і атак.

3) Системи виявлення і запобігання вторгненням (IDS/IPS): моніторинг мережі на предмет підозрілої активності та автоматичне вживання заходів.

4) Багаторівнева аутентифікація: впровадження процедур, які вимагають двофакторної або багатофакторної аутентифікації для доступу до критичних систем.

5) Віртуалізація: ізоляція систем та додатків від фізичного обладнання для забезпечення гнучкості та безпеки.

Математичні методи інформаційного забезпечення:

1) Криптографічні алгоритми: використання симетричного та асиметричного шифрування для захисту конфіденційності даних.

2) Статистичний аналіз: аналіз великих обсягів даних для виявлення аномалій, підозрілих патернів поведінки та потенційних загроз.

3) Оптимізаційні алгоритми: використання лінійного та не лінійного програмування для оптимізації ресурсів і процесів.

4) Методи штучного інтелекту: застосування машинного навчання та нейронних мереж для підвищення ефективності обробки даних і прийняття рішень.

5) Теорія інформації та кодування: застосування методів кодування для забезпечення цілісності даних та ефективної передачі інформації.

Ці методи та техніки є фундаментом для створення інформаційної системи «Інватех», здатної ефективно відповідати на виклики сучасної медичної галузі, забезпечуючи високий рівень безпеки, ефективності обробки даних та гнучкості у відповіді на змінні умови роботи.

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

1) Cisco Systems:

Опис: Cisco є світовим лідером у галузі мережевих технологій для Інтернету. Компанія пропонує широкий спектр рішень для мережевої інфраструктури, включаючи маршрутизатори, комутатори, бездротові системи та безпеку.

Застосування: їх рішення ідеально підходять для забезпечення надійності та масштабованості корпоративних мереж в медичній галузі, з особливим фокусом на безпеку даних.

2) Hewlett Packard Enterprise (HPE):

Опис: HPE пропонує розширені мережеві рішення, які включають мережеве обладнання та управління, забезпечуючи високу ефективність та простоту управління мережами.

Застосування: їхні технології дозволяють інтегрувати новітні рішення у мережеву інфраструктуру без перерв у роботі, що є ключовим для медичних виробничих потужностей.

3) Juniper Networks:

Опис: Juniper Networks спеціалізується на розробці та імплементації інноваційних рішень для мереж, що забезпечують безпеку, продуктивність та масштабованість.

Застосування: їх продукти ідеально підходять для створення високозахищених мережевих середовищ, що є критично важливим для забезпечення конфіденційності медичної інформації.

4) Dell Technologies:

Опис: Dell пропонує комплексні рішення для побудови корпоративних мереж, які включають сервери, зберігання даних, мережеве обладнання та безпеку.

Застосування: Dell забезпечує надійність і гнучкість управління даними, що дозволяє медичним компаніям впроваджувати рішення, адаптовані до їх специфічних потреб.

Використання передових мережевих рішень від світових лідерів дозволить «Інватех» значно підвищити ефективність своїх виробничих і дослідницьких процесів. Зокрема, можна розглянути наступні напрямки:

Оптимізація мережевої інфраструктури: Вибір і впровадження інтегрованих рішень для підвищення продуктивності мережі та зменшення часу простоїв.

Забезпечення високого рівня безпеки: Впровадження комплексних рішень з захисту даних для забезпечення конфіденційності та захисту від кіберзагроз.

Скальованість та гнучкість: Розробка мережевої архітектури, здатної адаптуватися до майбутнього росту та змін у технологічному ландшафті без значних капіталовкладень.

1.5 Розробка схеми організаційної структури підприємства

Структура організації

Верхній менеджмент:

– генеральний директор (CEO): Відповідає за стратегічне планування та загальне управління компанією;

– фінансовий директор (CFO): Керує фінансовими операціями, включаючи бухгалтерський облік, бюджетування та фінансове планування;

– технічний директор (CTO): Відповідає за управління технологіями, виробництвом та дослідженнями та розробками.

Операційний сектор:

– виробничий відділ: Керує всіма аспектами виробничого процесу, від планування до випуску готової продукції;

– відділ контролю якості: Забезпечує відповідність продукції стандартам якості та безпеки;

– логістичний відділ: Відповідає за управління постачаннями, розподіл та доставку продукції.

Відділ досліджень та розробок:

– розробка нових продуктів та удосконалення існуючих моделей медичного обладнання. Цей відділ є ключовим для інноваційної діяльності компанії.

Маркетинговий та продажний відділ:

– маркетинг: Розробка стратегій продвиження продуктів та аналіз ринку;

– продажі: Відповідає за взаємодію з клієнтами та збут продукції.

IT-відділ:

– забезпечення підтримки всіх комп'ютерних систем та мереж, розробка та впровадження інформаційних систем, що підтримують виробничі та адміністративні процеси.

Відділ кадрів (HR):

– управління персоналом, включаючи найм, навчання, розвиток та оцінка працівників.

Рисунок 1.1 – Схема архітектури компанії

1.6 Завдання і мета роботи

Основна мета даної роботи полягає у розробці та вдосконаленні корпоративної мережі для ТОВ ВКФ «Інватех», що спеціалізується на виробництві медичного обладнання. Мережа має забезпечувати високу ефективність комунікацій, безпеку обробки та зберігання даних, а також підтримувати інтеграцію різноманітних відділів компанії. Робота має на меті оптимізувати існуючі мережеві ресурси, впровадити передові технології для підвищення продуктивності та розробити стратегії захисту важливої інформації.

Завдання роботи

1) Аналіз поточного стану мережевої інфраструктури: оцінка існуючих мережевих рішень в «Інватех», ідентифікація слабких місць та потенційних ризиків.

2) Розробка вимог до нової мережевої архітектури: визначення технічних та функціональних вимог до мережі з урахуванням специфіки виробництва медичного обладнання.

3) Проектування мережевої структури: розробка детальної схеми мережі, включаючи вибір обладнання, топологію мережі та стратегії забезпечення безпеки.

4) Впровадження мережевих рішень: реалізація проекту корпоративної мережі, включаючи інсталяцію обладнання та програмного забезпечення.

5) Тестування та оптимізація мережі: проведення комплексного тестування новоствореної мережевої інфраструктури для перевірки її продуктивності та надійності.

1.7 Визначення можливих напрямків рішення поставлених завдань

Покращення мережевої архітектури:

– упровадження розподілених систем зберігання даних: Розгортання технологій, які дозволяють ефективне зберігання та швидкий доступ до медичних даних;

– використання облачних рішень: Застосування хмарних технологій для забезпечення масштабованості, гнучкості та зниження вартості IT-інфраструктури.

Впровадження передових мережевих технологій:

– розгортання SDN (Software-Defined Networking): Упровадження програмно-конфігурованої мережі для покращення управління трафіком та забезпечення гнучкості мережевих налаштувань;

– інтеграція IoT рішень: Застосування інтернету речей для моніторингу стану медичного обладнання та оптимізації процесів обслуговування.

Розробка комплексних стратегій кібербезпеки:

– зміцнення захисту периметру мережі: Встановлення багаторівневих брандмауерів та систем виявлення та запобігання вторгнень (IDS/IPS);

– використання шифрування даних: Запровадження сучасних алгоритмів шифрування для захисту чутливих даних, які передаються та зберігаються в мережі.

Розробка політик доступу та автентифікації:

– впровадження багатофакторної автентифікації: Забезпечення доступу до корпоративних ресурсів лише для авторизованих осіб;

– сегментація мережі: Імплементація VLAN і ACL для ізоляції критично важливих систем та даних.

Автоматизація та роботизація:

– упровадження автоматизованих робочих станцій: Впровадження роботизованих систем для автоматизації складних і повторюваних процесів на виробництві;

– цифровізація документообігу: Перехід на електронний документообіг для підвищення продуктивності та зниження помилок.

Вдосконалення системи управління якістю:

– впровадження систем ERP: Розгортання корпоративних ресурсних планувальних систем для оптимізації логістики, управління запасами, фінансами та людськими ресурсами.

Ці напрямки дозволять ТОВ ВКФ «Інватех» не тільки оптимізувати свої поточні процеси, але й покласти міцний фундамент для майбутнього розвитку та адаптації до змінюваних ринкових умов.

1.8 Обґрунтування вибраного напрямку інженерного рішення

Для компанії ТОВ ВКФ «Інватех», що спеціалізується на виробництві медичного обладнання, ключовим напрямком інженерного рішення є інтеграція авангардних технологій кібербезпеки та автоматизації виробничих процесів. Цей напрямок вибрано з огляду на потребу захисту чутливих медичних даних та забезпечення високої ефективності виробництва.

1) Забезпечення безпеки даних:

Важливість: медична індустрія вимагає надзвичайно високого рівня захисту даних через обробку великої кількості конфіденційної інформації, включаючи персональні дані і деталі медичних досліджень.

Реалізація: впровадження комплексних рішень кібербезпеки, включаючи шифрування, багаторівневі брандмауери, інтрузивні детекційні системи (IDS/IPS) та сучасні методи аутентифікації, дозволяє забезпечити необхідний рівень безпеки.

2) Автоматизація виробничих процесів:

Важливість: автоматизація необхідна для підвищення продуктивності, зниження виробничих витрат і забезпечення високої якості продукції.

Реалізація: впровадження автоматизованих роботизованих ліній і систем управління ресурсами підприємства (ERP) сприяє оптимізації всіх аспектів виробництва, від запланування до виконання.

3) Інтеграція IoT та Big Data:

Важливість: використання інтернету речей (IoT) та технологій обробки великих даних (Big Data) дозволяє реалізувати передові аналітичні засоби для моніторингу стану обладнання та оптимізації логістики.

Реалізація: застосування IoT датчиків для збору даних у реальному часі та аналітики Big Data для їх обробки і виявлення патернів сприяє підвищенню ефективності виробничих процесів.

Вибраний напрямок забезпечує комплексний підхід до вирішення ключових завдань «Інватех» у сферах безпеки, виробничої ефективності та інновацій. Він дозволяє не тільки реагувати на сучасні виклики, а й адаптуватися до майбутніх змін у технологічному ландшафті, забезпечуючи сталий розвиток та конкурентоспроможність компанії на міжнародному ринку.

2 РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ КОМП'ЮТЕРНОЇ СИСТЕМИ

2.1 Технічні вимоги до КС компанії

2.1.1 Вимоги до системи в цілому

2.1.1.1 Вимоги до структури і функціонуванню системи

ТОВ ВКФ «Інватех» потребує комплексної комп'ютерної системи, яка охоплює кілька ключових підсистем для забезпечення ефективності своєї діяльності:

Мережева інфраструктура: основа для всіх IT-операцій, забезпечує з'єднання між усіма пристроями в мережі, включаючи сервери, робочі станції, мобільні пристрої тощо.

Серверні ресурси: включають файлові сервери, сервери баз даних, веб-сервери та інші критичні системи, що підтримують основні бізнес-процеси.

Системи зберігання даних: централізовані сховища даних, які забезпечують високу доступність та цілісність корпоративної інформації.

Безпека мережі: системи, що включають файрволи, системи виявлення та запобігання вторгнень, антивірусне програмне забезпечення та інші інструменти безпеки для захисту від зовнішніх та внутрішніх загроз.

Системи резервного копіювання та відновлення: забезпечують здатність швидко відновлювати операції після будь-яких технічних або природних збоїв.

Основні характеристики:

Масштабованість: система має бути здатною адаптуватися до змін у розмірі та потребах бізнесу без значних переробок.

Надійність: мінімізація часу простою та забезпечення стабільності роботи системи в критичні періоди.

Безпека: високий рівень захисту даних і мережевих ресурсів від несанкціонованого доступу та інших загроз.

Інтегрованість: легке зв'язування з іншими системами та програмним забезпеченням для спрощення процесів управління та аналізу.

Вимоги до числа рівнів ієрархії та ступені централізації:

Ієрархічна структура: система має мати чітку ієрархічну структуру з визначеними рівнями управління та доступу для різних типів користувачів.

Централізація: певний ступінь централізації управління необхідний для координації загальносистемних процесів та політик безпеки. Водночас, локальні підрозділи мають мати можливість самостійно управляти ресурсами, що їх стосуються.

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

1) Надійність з'єднань: засоби зв'язку між компонентами системи повинні забезпечувати стабільність і надійність без перебоїв. Використання високоякісного обладнання та сучасних технологій, таких як оптоволоконні кабелі та надійні бездротові рішення.

2) Швидкість передачі даних: система повинна підтримувати високу швидкість передачі даних для ефективної взаємодії між відділами та швидкого доступу до медичних даних і ресурсів, особливо для великих обсягів медичних зображень та відеоданих.

3) Безпека зв'язку: всі канали зв'язку мають бути захищені від несанкціонованого доступу та зовнішніх атак. Це включає використання VPN, шифрування з'єднань, та імплементацію сучасних протоколів безпеки.

4) Скальованість та гнучкість: засоби зв'язку мають бути гнучкими і скальованими, щоб підтримувати розширення компанії та впровадження нових технологій без потреби повної заміни існуючої інфраструктури.

5) Інтегрованість: системи зв'язку мають бути інтегрованими з усіма внутрішніми системами управління, ERP-системами та іншими інструментами, що використовуються в «Інватех», для забезпечення єдиного інформаційного простору.

6) Резервування та відновлення: наявність резервних каналів зв'язку та стратегій швидкого відновлення зв'язку у разі аварійних ситуацій для забезпечення безперервності виробничих та дослідницьких процесів.

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

Для ТОВ ВКФ «Інватех», ефективна інтеграція новоствореної системи з існуючими та суміжними системами є критичною. Система повинна підтримувати безшовну інтеграцію з такими системами, як ERP для управління ресурсами, системи керування відносинами з клієнтами (CRM), а також з іншими медичними та адміністративними системами. Взаємодія має включати обмін даними в реальному часі, забезпечення сумісності протоколів і форматів даних, а також використання API для автоматизації процесів.

2.1.1.4 Вимоги до режимів функціонування системи

Система має підтримувати декілька режимів роботи, включаючи стандартний (денний), нічний та аварійний режими. Кожен режим повинен мати свої параметри енергоспоживання, доступності ресурсів та рівнів безпеки. Важливою є підтримка автоматичного переходу між режимами в залежності від внутрішніх або зовнішніх подій.

2.1.1.5 Вимоги до діагностування системи

Система повинна включати комплексні інструменти для моніторингу та діагностики, які дозволяють виявляти і виправляти помилки та несправності у роботі обладнання і програмного забезпечення. Вимоги включають логування подій, систему сповіщень про помилки і засоби для дистанційного та автоматичного втручання.

2.1.1.6 Перспективи розвитку, модернізації системи

Система повинна бути розроблена з можливістю легкої модернізації та розширення функціоналу без значних витрат чи перерв у роботі. Перспективи

розвитку включають інтеграцію з новітніми технологіями, як штучний інтелект і машинне навчання, для підвищення ефективності обробки даних і автоматизації процесів.

2.1.1.7 Вимоги до показників призначення

Система повинна відповідати показникам, які оцінюють її ефективність, надійність, швидкість обробки даних, а також здатність підтримувати необхідний рівень безпеки. Ці показники включають час відгуку системи, частоту помилок, пропускну здатність мережі та індекси доступності критичних додатків.

2.1.1.8 Вимоги до патентної чистоти

Необхідно забезпечити, що всі компоненти системи, як програмне так і апаратне забезпечення, мають патентну чистоту у ключових країнах оперування, зокрема у США, ЄС, Канаді та Японії. Це включає аналіз існуючих патентів та забезпечення, що нові розробки не порушують існуючих патентних прав.

2.1.1.9 Додаткові вимоги

Особливі умови експлуатації: Система повинна бути стійкою до високих навантажень і здатною працювати в умовах великої кількості одночасних запитів.

Активне обладнання: має включати високопродуктивні сервери з резервними блоками живлення, а також комутатори та маршрутизатори з підтримкою необхідної кількості портів.

Кабель-канали та розетки: виконання з урахуванням необхідних стандартів та специфікацій для забезпечення надійного з'єднання.

Розміщення обладнання: розробка специфікацій для оптимального розміщення у шафах, включаючи вентиляцію та доступ до обслуговування.

Резервування та однорідність: Забезпечення наявності резервних систем та використання уніфікованих компонентів для легкого заміщення та ремонту.

2.1.1.10 Вимоги функцій, виконуваним системою

1) Мережева інфраструктура:

– Функції:

Підтримка стабільного зв'язку між всіма вузлами мережі.

Автоматичне виявлення та виправлення помилок у мережі.

Моніторинг та аналіз трафіку для оптимізації продуктивності.

– Вимоги:

Час відновлення зв'язку після збою не повинен перевищувати 30 секунд.

99.9% надійності зв'язку.

Вихідні дані повинні включати звіти про стан мережі, доступні у форматах CSV та PDF.

2) Серверні ресурси:

– Функції:

Хостинг баз даних та веб-аплікацій.

Забезпечення резервного копіювання та відновлення даних.

Управління доступом користувачів до серверних ресурсів.

– Вимоги:

Резервне копіювання даних має відбуватися щоночі з можливістю відновлення протягом однієї години.

Відповідність політикам безпеки із застосуванням шифрування для захисту даних.

Логінг всіх доступів до серверів з точністю до секунди.

3) Системи зберігання даних:

– Функції:

Централізоване зберігання корпоративних даних.

Синхронізація даних між різними локаціями.

Захист даних від несанкціонованого доступу.

– Вимоги:

Доступність даних не менше 99.8%.

Регулярна перевірка цілісності даних.

Звіти про активність системи зберігання, представлені в графічних дашбордах.

4) Безпека мережі:

– Функції:

Фільтрація трафіку для виявлення та блокування зловмисних дій.

Ведення аудиту безпеки для виявлення потенційних вразливостей.

Реагування на інциденти безпеки.

– Вимоги:

Швидке реагування на інциденти безпеки — не пізніше 5 хвилин з моменту їх виявлення.

Докладні звіти про інциденти, включаючи аналіз причин та рекомендації для запобігання майбутніх інцидентів.

5) Системи резервного копіювання та відновлення:

– Функції:

Автоматичне резервне копіювання критично важливих даних.

Швидке відновлення операцій після збоїв.

Тестування планів відновлення для гарантії їх ефективності.

– Вимоги:

Відновлення основних бізнес-сервісів протягом 2 годин після катастрофічного збою.

Планові перевірки систем відновлення не рідше одного разу на квартал.

Ведення детальної документації про процеси резервного копіювання та відновлення.

2.1.2 Вимоги до видів забезпечення комп’ютерної системи

2.1.2.1 Вимоги до математичного забезпечення

Склад і застосування математичних методів: Використання статистичних методів для аналізу даних, оптимізаційних алгоритмів для планування ресурсів, а також алгоритмів штучного інтелекту для обробки медичних зображень.

Обмеження: Забезпечення точності та надійності використаних алгоритмів, відповідність вимогам конфіденційності.

Способи використання: Інтеграція математичних модулів безпосередньо у системи діагностики, логістичні та управлінські платформи.

2.1.2.2 Вимоги до інформаційного забезпечення

Склад та структура даних: централізоване зберігання даних з використанням реляційних баз даних для гарантії цілісності та безпеки.

Інформаційний обмін: використання захищених протоколів передачі даних між системами.

Сумісність: інтеграція з іншими медичними та адміністративними системами через стандартні API.

Бази даних: впровадження систем керування базами даних з високим рівнем доступності та відмовостійкості.

Обробка та передача даних: автоматизація процесів збору та аналізу даних.

Контроль, збереження та відновлення даних: Реалізація політик регулярного бекапу та швидкого відновлення.

2.1.2.3 Вимоги до лінгвистичного забезпечення

Мови програмування: Використання мов високого рівня, таких як Python для обробки даних, Java для бекенду, та JavaScript для фронтенду.

Кодування та декодування даних: Впровадження стандартів кодування, як UTF-8 для текстових даних та AES для шифрування файлів.

Мови маніпулювання даними: SQL для реляційних баз даних та спеціалізовані мови для NoSQL систем.

2.1.2.4 Вимоги до технічного забезпечення

Технічні засоби: Використання серверів, мережевих пристроїв та систем зберігання даних, що підтримують високу пропускну здатність і надійність.

Функціональні вимоги: Сервери мають включати резервні джерела живлення, а мережеві пристрої — підтримку різних протоколів безпеки.

2.1.2.5 Вимоги до організаційного забезпечення

Структура підрозділів: Чітке визначення функцій і відповідальностей між підрозділами, що забезпечують технічну підтримку та експлуатацію системи.

Організація роботи: Розробка процедур для ефективної взаємодії персоналу в рамках системи.

2.1.2.6 Вимоги до методичного забезпечення

Нормативно-технічна документація: Підготовка комплекту документів, що включають інструкції, стандарти та методики, які регулюють експлуатацію та обслуговування системи.

Дотримання стандартів: Використання міжнародних та національних стандартів для забезпечення якості та безпеки роботи системи.

2.2 Розробка апаратної частини комп’ютерної системи

2.2.1 Розробка загальної архітектури мережі підприємства

Ключові елементи архітектури:

Маршрутизатори (Router1, Router2, Router3, Router4, Router0): Забезпечують маршрутизацію та ізоляцію трафіку між різними сегментами мережі.

Мережеві комутатори (Switch2, Switch3, CopySwitch4, CopySwitch5): Керують локальним трафіком в межах визначених VLANs, що підвищує ефективність розподілу даних.

Серверне обладнання (Server HTTP, Server DNS, Server TFTP): Відповідають за веб-сервіси, розв'язання імен та передачу файлів відповідно.

Системи безпеки (IPS): Відіграють ключову роль у захисті мережі від несанкціонованих спроб доступу та інших загроз.

Мережеві зони:

LAN-1, LAN-2, LAN-3, LAN-4, LAN-5: Це окремі зони, кожна з яких має свої власні вимоги до безпеки і пропускної спроможності, а також спеціалізоване обладнання.

Безпека:

Основним компонентом безпеки в архітектурі є IPS, розташований для моніторингу та аналізу мережевого трафіку, що дозволяє своєчасно виявляти та реагувати на загрози.

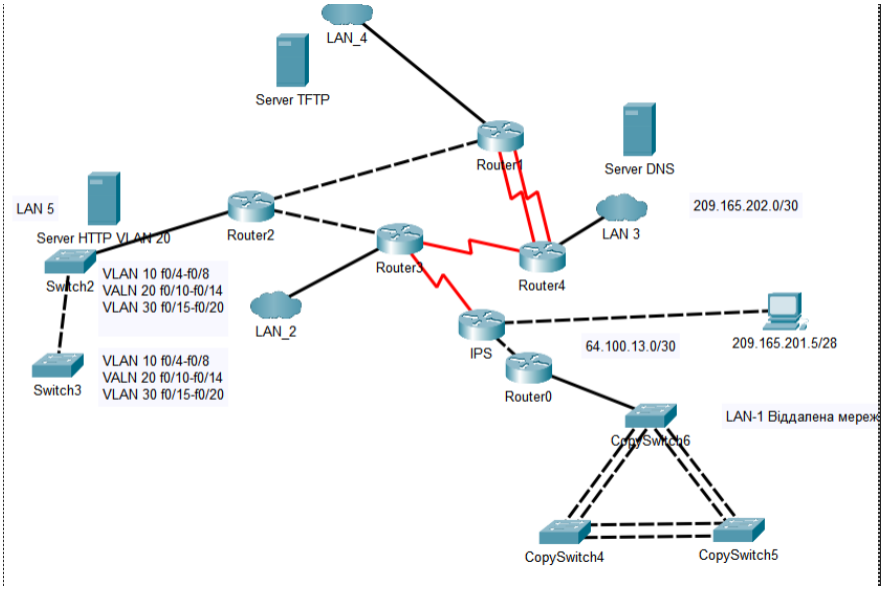


Рисунок 2.1 – Схема архітектури мережі

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

За допомогою аналізу поточної архітектури та вимог бізнесу, було обрано структурну схему, яка оптимально відповідає потребам «Інватех». Схема включає інтеграцію високопродуктивного серверного обладнання, сучасних комутаторів та маршрутизаторів, а також систем безпеки як невід'ємну частину мережевої інфраструктури.

Технічне обґрунтування:

Надійність і масштабованість: Використання надійних серверів і мережевих пристроїв від відомих виробників гарантує високу доступність ресурсів і легкість у масштабуванні системи.

Висока пропускна спроможність і мінімізація затримок: Застосування сучасних мережевих технологій, таких як Gigabit Ethernet і оптоволоконні з'єднання, забезпечує швидкий обмін даними.

Безпека: Інтеграція IPS і розширених брандмауерів допомагає забезпечити захист від внутрішніх та зовнішніх загроз.

Ця структурна схема не лише відповідає поточним потребам «Інватех», але й забезпечує основу для подальшої модернізації та розвитку, дозволяючи компанії адаптуватися до майбутніх технологічних змін і ринкових вимог.

2.2.3 Розробка специфікації апаратних засобів комп'ютерної системи

Таблиця 2.1 – Специфікація обладнання

Позиція	Найменування і технічна характеристика	Тип, марка, позначення документа	Одиниці виміру	Кількість
1	**2**	**3**	**4**	**5**
1	Маршрутизатор: Crypto, 4 built-in GE, Dual P/S, 20Gbit, 6x1000Base-X (SFP), 2x10G SFP+ інтегровані RP, SIP та ESP, 1xNIM, 1xSPA, RAM 8Gb, 2xAC	Cisco 2911	Од.	5
2	Комутатор: 24 x Ethernet 10/100/1000 Мбіт/сек, RIP v1, RIP v2, OSPF, USB-порт, LAN Base, 4 SFP слоти	Cisco Catalyst 2960-24TT	Од.	22
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
5	Комп'ютер: AMD Ryzen 3 3600G (3.9 — 4.4 ГГц), 16 ГБ DDR4, 250gb SSD, Windows 11 Pro	ARTLINE Business B38v08Win	Од.	329

2.2.4 Розрахунок інтенсивності трафіку вихідного трафіку найбільшої локальної мережі підприємства

В підмережі встановлений комутатори Cisco2960, що об’єднує 113 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=216 (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:

$$P_{р.р.} = \mu * L_{пов} * N * 8 = 216 * 1150 * 113 * 8 = 22.4 \text{ Мбіт/с} \quad (2.1)$$

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

N – кількість вузлів в мережі.

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

Комутатор SW1_DLS 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:

$$N = \mu_{вих} / \mu = 108\,696/113 \approx 962 \text{ джерела} \quad (2.3)$$

Ця кількість задовольняє кількості вузлів у найбільшій нашій локальній мережі, до якої входить 113 ПК.

Кожен з 113 ПК посилає потік заявок з інтенсивністю у 216 кадрів/с. Звідси, можем розрахувати інтенсивність вихідного трафіку:

$$\lambda = N * \mu = 113*216 = 24408 \text{ пакетів/с.} \quad (2.4)$$

Коефіцієнт затримки:

$$\rho = \frac{\lambda}{\mu вих} = \frac{24408}{108696} = 0{,}22 \quad (2.5)$$

Коефіцієнт зайнятості маршрутизатора:

$$\frac{\rho}{1-\rho} = \frac{0{,}22}{1-0{,}22} = 0{,}28 \quad (2.6)$$

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

$$T = \frac{1}{(\mu-\lambda)} = \frac{1}{(108696 - 24408)} = 11{,}86 \text{ мкс} \quad (2.7)$$

Середня довжина черги:

$$L_{чер} = \frac{\rho^2}{1-\rho} = \frac{0{,}22^2}{1-0.22} = 0.062 \quad (2.8)$$

Середній час перебування пакета у черзі:

$$T_{оч} = \frac{Lчер}{\lambda} = \frac{0{,}062}{24048} = 0{,}25 \text{ мкс} \quad (2.9)$$

Це значення задовольняє вимогам до затримки в ЛМ.

3 РОЗРОБКА КОРПОРАТИВНОЇ МЕРЕЖІ

3.1 Проектування логічної топології мережі

Проектування логічної топології мережі є важливим етапом у створенні комп'ютерної інфраструктури компанії, мета роботи побудувати корпоративну мережу з сегментованої структурую та можливістю масштабованості та надійного захисту. У мережі є 5-ть підмереж 4 з яких локальні в одному з офісів та інша це віддалений офіс у якому треба забезпечити роботу Etherchannel для безперервної роботи при виході з ладу комутаторів та 329 хостів у всій мережі. Забезпечено роботу таких сервісів як DNS та TFTP, захист доступу за моделі AAA та маршрутизація мережі з протоколом OSPF.

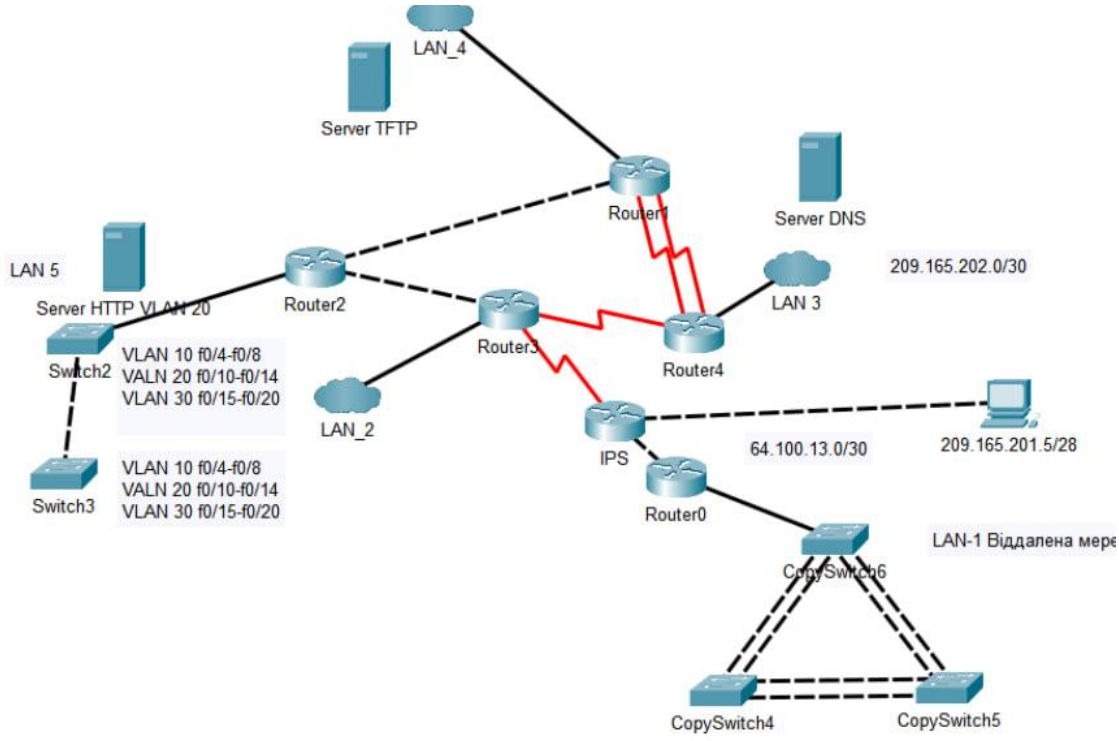


Рисунок 3.1 – Топологія мережі

3.2 Вибір та опис мережного обладнання

У сучасному світі інформаційних технологій, вибір надійного та ефективного мережного обладнання є ключовим для забезпечення стійкості та продуктивності

корпоративних мереж. Інтегровані сервісні маршрутизатори Cisco 2911, комутатори Cisco 2960 та сервери Cisco забезпечують комплексне рішення, яке відповідає потребам сучасних підприємств у швидкісній передачі даних, безпеці та надійності.

Маршрутизатор Cisco 2911 входить у серію ISR G2 і призначений для підтримки широкого спектру модулів для голосових, відео, безпеки, бездротових з'єднань та зберігання даних. Завдяки архітектурі Integrated Services, Cisco 2911 забезпечує гнучку настройку і масштабування, що дозволяє підприємствам оптимізувати свої мережеві ресурси відповідно до змінних вимог бізнесу.

Технічні характеристики:

Пропускна здатність: Cisco 2911 забезпечує до 35 Mbps пропускної спроможності при шифруванні, що робить його ідеальним для застосувань, які вимагають високого рівня безпеки передачі даних.

Порти: Обладнаний трема інтегрованими 10/100/1000 Ethernet портами, а також новими слотами, що дозволяють інтеграцію широкого спектру інтерфейсів.

Розширені можливості: Підтримка модулів голосу, безпеки, VPN та зовнішніх сервісів.

Комутатори Cisco 2960 є основою для створення корпоративних мережевих рішень, призначених для середовищ з інтенсивними мережевими взаємодіями, включаючи передачу голосу, відео та даних.

Технічні характеристики:

Порти: Варіюються від 8 до 48 Ethernet портів з підтримкою PoE, що забезпечує живлення через Ethernet для IP-телефонів та інших пристроїв.

Продуктивність: Висока пропускна спроможність з низьким часом відгуку, підтримка автоматичної настройки QoS для оптимізації голосових і відео з'єднань.

Безпека: Розширені функції безпеки, такі як ACL, гостьовий VLAN, MAC-адресна фільтрація.

Сервери Cisco UCS створені для інтеграції в центри обробки даних і підтримки обчислювальних операцій великого масштабу. Вони забезпечують високу гнучкість, масштабування та управління.

Технічні характеристики:

Процесори: Підтримка багатоядерних процесорів Intel Xeon для високої обчислювальної потужності.

Пам'ять: Великий обсяг оперативної пам'яті для обробки великих об'ємів даних і складних додатків.

Інтеграція: Єдина система управління для всіх компонентів сервера, що значно спрощує управління ресурсами і знижує загальні 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.

– Підмережа для 113 хостів - мінімально потрібно 128 адрес (2^7 = 128, де 128 - 2 = 126 доступних адрес), отже маска буде /25.

– Підмережа для 75 хостів - мінімально потрібно 128 адрес, отже маска буде /25.

– Підмережа для 50 хостів - мінімально потрібно 64 адреси (2^6 = 64, де 64 - 2 = 62 доступних адрес), отже маска буде /26.

– Підмережа для 46 хостів - мінімально потрібно 64 адреси, отже маска буде /26.

– Підмережа для 45 хостів - мінімально потрібно 64 адреси, отже маска буде /26.

1) Підмережа для 113 хостів (/25):

– Мережева адреса: 172.24.120.0

– Широкомовний адрес (Broadcast): 172.24.120.127

– Діапазон використання адрес: 172.24.120.1 - 172.24.120.126

– Маска підмережі: 255.255.255.128

2) Підмережа для 75 хостів (/25):

– Мережева адреса: 172.24.120.128

– Широкомовний адрес: 172.24.120.255

– Діапазон використання адрес: 172.24.120.129 - 172.24.120.254

– Маска підмережі: 255.255.255.128

3) Підмережа для 50 хостів (/26):

– Мережева адреса: 172.24.121.0

– Широкомовний адрес: 172.24.121.63

– Діапазон використання адрес: 172.24.121.1 - 172.24.121.62

– Маска підмережі: 255.255.255.192

4) Підмережа для 46 хостів (/26):

– Мережева адреса: 172.24.121.64

– Широкомовний адрес: 172.24.121.127

– Діапазон використання адрес: 172.24.121.65 - 172.24.121.126

– Маска підмережі: 255.255.255.192

5) Підмережа для 45 хостів (/26):

– Мережева адреса: 172.24.121.128

– Широкомовний адрес: 172.24.121.191

– Діапазон використання адрес: 172.24.121.129 - 172.24.121.190

– Маска підмережі: 255.255.255.192

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	113	172.24.120.0	/25	172.24.120.1 - 172.24.120.126
LAN 2	75	172.24.120.128	/25	172.24.120.129-172.24.120.254
LAN 3	50	172.24.121.0	/26	172.24.121.1 - 172.24.121.62
LAN 4	46	172.24.121.64	/26	172.24.121.65 - 172.24.121.126
LAN 5	45	172.24.121.128	/26	172.24.121.129-172.24.121.190

У таблиці 3.2 наведено схему адресації маршрутизаторів мережі.

Таблиця 3.2 – Схема адресації пристроїв

Пристрій	Інтерфейс	IP-адреса мережі	Маска
Lakiza_R3	Se0/0/0	209.165.202.0/30	255.255.255.252
	Gig0/0	172.10.120.4/30	255.255.255.252
	Gig0/1	172.24.120.128/25	255.255.255.128
	Se0/0/1	172.10.120.8/30	255.255.255.252
Lakiza_R1	Gig0/0	172.24.121.64/26	255.255.255.192
	Se0/0/0	172.10.120.12/30	255.255.255.252
	Se0/0/1	172.10.120.16/30	255.255.255.252
	Gig0/1	172.10.120.0/30	255.255.255.252
Lakiza_R2	Gig0/0	172.10.120.0/30	255.255.255.252
	Gig0/1	172.10.120.4/30	255.255.255.252
	Gig0/2	172.24.121.128/26	255.255.255.192
Lakiza_R4	Se0/0/0	172.10.120.12/30	255.255.255.252
	Se0/0/1	172.10.120.16/30	255.255.255.252
	Se0/1/0	172.10.120.8/30	255.255.255.252
	Gig0/1	172.24.121.0/26	255.255.255.192
Lakiza_R0	Gig0/0	64.100.13.0/30	255.255.255. 252
	Gig0/1	172.24.120.0/25	255.255.255.128

3.4 Базове налаштування конфігурації пристроїв

Ініціальне конфігурування маршрутизатора та комутатора включає встановлення відповідних назв пристроїв, впровадження методів захисту паролів, налаштування доступу в режимі з підвищеними правами, а також застосування захищених протоколів для управління мережевим обладнанням. Особливу увагу слід приділити використанню технології Etherchannel для підвищення ефективності і безпеки мережі.

Базове налаштування конфігурації пристроїв на прикладі Lakiza_R3:

hostname Lakiza_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 # Lakiza_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_ Lakiza password admincisco // призначення імені користувача та паролю

ip domain-name Lakiza_R3 // налаштування імені домена

crypto key generate rsa // створення ключа шфируваня

1024 // вибір довжини ключа шифрування

Технологія Etherchannel, яка використовується в мережі LAN_1, є важливим інструментом для підвищення ефективності та надійності мережевої інфраструктури. Etherchannel дозволяє об'єднувати кілька фізичних портів у один логічний канал, що забезпечує декілька ключових переваг для мережевих операцій.

Сама основна перевага використання Etherchannel полягає в збільшенні загальної пропускної спроможності мережі. Наприклад, якщо один порт може передавати дані зі швидкістю 1 Гбіт/с, то об'єднання чотирьох таких портів у рамках Etherchannel може теоретично збільшити пропускну здатність до 4 Гбіт/с. Це

особливо корисно в середовищах з високими вимогами до обміну даними, таких як центри обробки даних, масштабні веб-сервери або платформи стрімінгових сервісів.

Etherchannel також збільшує надійність мережі. Шляхом агрегування декількох з'єднань в одне, знижується ризик повного переривання зв'язку через відмову одного з портів. Якщо один порт вийде з ладу, інші продовжуватимуть функціонувати, забезпечуючи неперервність мережевих послуг. Це критично важливо для підтримки безперервної доступності до критично важливих систем і додатків.

Крім збільшення пропускної здатності та надійності, Etherchannel також дозволяє більш рівномірно розподіляти трафік між агрегованими портами. Це досягається шляхом різних алгоритмів балансування навантаження, які можуть розподіляти вхідний і вихідний трафік залежно від адреси джерела або призначення, типу протоколу та інших параметрів. Таке балансування оптимізує використання мережевих ресурсів і зменшує ймовірність перевантаження окремих мережевих інтерфейсів.

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
```

3.5 Вибір та налаштування способу маршрутизації

Під час проектування мережевої інфраструктури критично важливим є вибір ефективного та надійного методу маршрутизації. Протокол OSPF (Open Shortest Path

First) було обрано завдяки його здатності швидко адаптуватися до змін у мережі та динамічно вибирати найкоротші і найефективніші маршрути для передачі даних. Завдяки своїй ієрархічній структурі та масштабованості, OSPF ідеально підходить для складних корпоративних мереж. Налаштування OSPF дозволяє оптимізувати розподіл даних між вузлами мережі, забезпечуючи мінімізацію затримок та втрат. Окрім цього, мережевий протокол DHCP автоматизує призначення IP-адрес, спрощуючи адміністрування мережі. У мережах можна використовувати статичну або динамічну маршрутизацію: статична потребує ручного введення маршрутів, тоді як динамічна автоматично оновлює маршрути, надаючи більш гнучке налаштування.

Налаштування DHCP на прикладі маршрутизатора Lakiza_R3:

```
ip dhcp excluded-address 172.24.120.129 172.24.120.135
!
ip dhcp pool LAN-2
network 172.24.120.128 255.255.255.128
default-router 172.24.120.129
dns-server 172.24.121.10
```

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

Налаштування протоколу OSPF на прикладі маршрутизатора Lakiza_R3:

```
router ospf 1
log-adjacency-changes
passive-interface default
no passive-interface GigabitEthernet0/0
no passive-interface GigabitEthernet0/1
no passive-interface Serial0/0/0
no passive-interface Serial0/0/1
auto-cost reference-bandwidth 1000
network 172.10.120.4 0.0.0.3 area 0
network 172.10.120.8 0.0.0.3 area 0
```

network 209.165.202.0 0.0.0.3 area 0

network 172.24.120.128 0.0.0.127 area 0

network 172.10.120.24 0.0.0.3 area 0

На граничному маршрутизаторі Lakiza_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

3.6 Налаштування роботи Інтернет

Для забезпечення ефективного доступу внутрішніх систем до Інтернету важливо використовувати технологію Network Address Translation (NAT). NAT дозволяє транслювати приватні IP-адреси, які використовуються всередині організації, у публічні IP-адреси, необхідні для зв'язку з зовнішнім світом. Це дозволяє множині пристроїв в мережі організації взаємодіяти з Інтернетом через одну чи кілька публічних адрес, що значно підвищує безпеку та ефективність використання мережевих ресурсів.

NAT також допомагає в управлінні портами, що важливо при організації численних з'єднань через обмежену кількість доступних публічних IP-адрес. В процесі NAT кожне з'єднання може бути ідентифіковане за допомогою унікальної комбінації порту та адреси, що дозволяє зберегти індивідуальність сесій між великою кількістю внутрішніх користувачів та зовнішніми сервісами.

Конкретно, визначений пул адрес для NAT, який використовується у цій мережі, варіюється від 209.165.202.5 до 209.165.202.30. Ці публічні IP-адреси

використовуються для агрегації зовнішніх з'єднань, розподіляючи їх серед багатьох внутрішніх користувачів, що дозволяє забезпечити стабільний та безперебійний доступ до Інтернету.

Запровадження NAT в організації включає налаштування маршрутизаторів або вогнезахисних систем для перекладу адрес та управління трафіком. Це не тільки сприяє захисту внутрішньої мережі від несанкціонованого доступу ззовні, але й забезпечує оптимальне використання мережевих ресурсів.

Давайте розглянемо налаштування NAT, використовуючи як приклад прикордонний маршрутизатор Lakiza_R3:

```
ip nat pool Internet 209.165.200.6 209.165.200.30 netmask 255.255.255.224
ip nat inside source list NAT10 pool Internet
ip nat inside source static 172.24.121.70 209.165.200.3
ip nat inside source static 172.24.121.10 209.165.200.4
ip nat inside source static 172.24.121.150 209.165.200.5
ip classless
ip access-list extended NAT10
deny ip 172.24.121.0 0.0.0.63 172.24.120.0 0.0.0.127
deny ip 172.24.120.128 0.0.0.127 172.24.120.0 0.0.0.127
deny ip 172.24.121.64 0.0.0.63 172.24.120.0 0.0.0.127
deny ip 172.24.121.128 0.0.0.63 172.24.120.0 0.0.0.127
deny ip 172.10.120.0 0.0.0.255 172.24.120.0 0.0.0.127
permit ip 172.24.121.0 0.0.0.63 any
permit ip 172.24.120.128 0.0.0.127 any
permit ip 172.24.121.64 0.0.0.63 any
permit ip 172.24.121.128 0.0.0.63 any
permit ip 172.10.120.0 0.0.0.255 any
```

3.7 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. Щоб розділити підмережу 172.24.121.128/26 на три VLAN та один керуючий VLAN (№ 99) з 5 хостами, спочатку потрібно переконатися, що в цій підмережі достатньо адресного простору. Підмережа 172.24.121.128/26 містить 64 адреси (від 172.24.121.128 до 172.24.121.191).

Для розміщення керуючого VLAN з 5 хостами нам знадобиться підмережа, яка може вмістити щонайменше 7 адрес (5 хостів + 1 мережева адреса + 1 броадкаст адреса). Найменша підмережа, яка може це забезпечити, буде /29, оскільки 2^3 = 8 адрес.

1) Підмережа для керуючого VLAN 99 (/29):

– Мережева адреса (Network Address): 172.24.121.128

– Броадкаст адреса (Broadcast Address): 172.24.121.135

– Діапазон адрес: 172.24.121.129 - 172.24.121.134

– Маска підмережі: 255.255.255.248 або /29

Залишковий адресний простір у підмережі 172.24.121.128/26 після виділення підмережі /29 буде від 172.24.121.136 до 172.24.121.191. Цей простір можна розділити на три рівні частини, використовуючи підмережі /28 (кожна містить 16 адрес).

1) VLAN 10 (/28):

– Мережева адреса (Network Address): 172.24.121.136

– Броадкаст адреса (Broadcast Address): 172.24.121.151

– Діапазон адрес: 172.24.121.137 - 172.24.121.150

– Маска підмережі: 255.255.255.240 або /28

2) VLAN 20 (/28):

– Мережева адреса (Network Address): 172.24.121.152

– Броадкаст адреса (Broadcast Address): 172.24.121.167

– Діапазон адрес: 172.24.121.153 - 172.24.121.166

– Маска підмережі: 255.255.255.240 або /28

3) VLAN 30 (/28):

– Мережева адреса (Network Address): 172.24.121.168

– Броадкаст адреса (Broadcast Address): 172.24.121.183

– Діапазон адрес: 172.24.121.169 - 172.24.121.182

– Маска підмережі: 255.255.255.240 або /28

У таблиці 3.3 наведена адресація під інтерфейсів мережі.

Таблиця 3.3 – Адресація мереж VLAN

Назва	Мережева адреса	/маска	Маска мережі	Діапазон адрес
VLAN10	172.24.121.136	/28	255.255.255.240	172.24.121.137 - 172.24.121.150
VLAN20	172.24.121.152	/28	255.255.255.240	172.24.121.153 - 172.24.121.166
VLAN30	172.24.121.168	/28	255.255.255.240	172.24.121.169 - 172.24.121.182
VLAN99	172.24.121.128	/29	255.255.255.248	172.24.121.129 - 172.24.121.134

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 172.24.121.137 255.255.255.240

interface GigabitEthernet0/2.20

encapsulation dot1Q 20

ip address 172.24.121.153 255.255.255.240

interface GigabitEthernet0/2.30

encapsulation dot1Q 30

ip address 172.24.121.167 255.255.255.240

interface GigabitEthernet0/2.99

encapsulation dot1Q 99

ip address 172.24.121.193 255.255.255.248

Для автоматичного призначення IP-адрес вузлам в різних VLAN буде використовуватись протокол DHCP. Налаштування DHCP на маршрутизаторі:

ip dhcp pool LAN5-VLAN10

network 172.24.121.128 255.255.255.240

default-router 172.24.121.137

dns-server 172.24.121.10

ip dhcp pool LAN5-VLAN30

network 172.24.121.160 255.255.255.240

default-router 172.24.121.167

dns-server 172.24.121.10

ip dhcp pool LAN5-VLAN20

network 172.24.121.144 255.255.255.240

default-router 172.24.121.153

3.8 Захист інформації в комп'ютерній системі від несанкціонованого доступу

Для забезпечення надійного захисту нашої мережі від несанкціонованого доступу ми впроваджуємо технологію AAA (Аутентифікація, Авторизація, та Облік). AAA є комплексним фреймворком, що дозволяє ефективно управляти доступом до мережевих ресурсів, перевіряти права користувачів та відстежувати їх діяльність у мережі. Система AAA використовує протоколи, такі як RADIUS або TACACS+, для централізованої аутентифікації та авторизації користувачів, які намагаються отримати доступ до мережі через різні мережеві пристрої, включаючи комутатори та маршрутизатори.

Основною перевагою сервера RADIUS в системі AAA є його здатність централізовано обробляти запити на вхід у систему, забезпечуючи єдиний точок доступу для аутентифікації та авторизації. Це значно спрощує управління безпекою мережі, оскільки адміністраторам не потрібно налаштовувати політики безпеки на кожному пристрої окремо. Такий підхід також підвищує загальну безпеку, оскільки всі політики та облікові дані централізовано керуються і контролюються.

У нашій мережевій інфраструктурі ми впровадили підтримку AAA на всіх маршрутизаторах для забезпечення єдиної та безпечної схеми доступу. Наприклад, на маршрутизаторі Lakiza_R3, ми налаштували AAA для забезпечення не тільки аутентифікації та авторизації, але й для ведення детального обліку дій користувачів. Це дозволяє нам точно відслідковувати використання мережевих ресурсів, виявляти можливі зловживання та швидко реагувати на будь-які інциденти безпеки.

```
aaa new-model
radius server host
address ipv4 172.24.9.120 auth-port 1645
key radius123
aaa authentication login console group radius local
line console 0
login authentication console
```

aaa authentication login default local

username Akimow password admin123

line vty 0 15

login authentication default

3.9 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 Lakiza_R0:

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

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

permit ip 172.24.120.00.0.0.127 172.24.120.128 0.0.0.127 // надання доступу на проходження пакетів з основної на віддалену мережу

permit ip 172.24.120.0 0.0.0.127 172.24.121.128 0.0.0.63

permit ip 172.24.120.0 0.0.0.127 172.24.121.64 0.0.0.63

permit ip 172.24.120.0 0.0.0.127 172.24.121.0 0.0.0.63

permit ip 172.24.120.0 0.0.0.127 172.10.120.0 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

3.10 Перевірка комп’ютерної Системи підприємства

Для аналізу базових налаштувань мережевих пристроїв, ми використовуємо маршрутизатор Lakiza_R2 як приклад. З використанням команди show running-config, ми проводимо перевірку ключових конфігураційних параметрів, які включають назву пристрою, налаштування паролів та параметри безпеки.

Перш за все, перевіряємо назву пристрою, що дозволяє ідентифікувати маршрутизатор в мережі. Це особливо важливо для забезпечення єдності в номенклатурі пристроїв, що спрощує управління мережею.

Далі, ми перевіряємо налаштування пароля для доступу до консолі. Це критично важливий елемент безпеки, який запобігає несанкціонованому доступу до маршрутизатора через фізичний консольний порт.

Також перевіряємо налаштування паролів для віддаленого доступу через лінії vty, а також використання протоколу ssh для цих з'єднань. SSH забезпечує зашифроване з'єднання, що значно підвищує безпеку при адмініструванні пристроїв віддалено.

Додатково ми контролюємо налаштування пароля для доступу до привілейованого режиму, що є ще одним захистом від неавторизованого втручання та можливих зловживань.

Перевірка також охоплює банер MOTD (Message of the Day), який використовується для відображення повідомлень користувачам при спробі входу до системи, що може містити важливі правила та інформацію про безпеку.

Нарешті, ми аналізуємо імена та паролі користувачів, а також назву домену, що важливо для інтеграції маршрутизатора в загальну доменну структуру мережі.

Такий комплексний перегляд налаштувань дозволяє не тільки підтвердити коректність конфігурації маршрутизатора, але й забезпечує високий рівень безпеки та ефективності в управлінні мережею.

```
hostname Lakiza_R2
```

Рисунок 3.2 – hostname

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

Рисунок 3.3 – Зашифрований пароль до консольного режиму

```
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 –Зашифровані пароль ліній vty

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

Рисунок 3.5 – Пароль до привілейованого режиму

```
!
banner motd ^CLakiza_R2^C
```

Рисунок 3.6 – Повідомлення при підключенні до CLI режиму

```
!
ip domain-name Lakiza_R2
!
```

Рисунок 3.8 – Доменне ім’я

```
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

```
 Routing Protocol is "ospf 1"
   Outgoing update filter list for all interfaces is
   Incoming update filter list for all interfaces is
   Router ID 172.24.121.193
   Number of areas in this router is 1. 1 normal 0 s
   Maximum path: 4
   Routing for Networks:
     172.24.121.128 0.0.0.63 area 0
     172.10.120.4 0.0.0.3 area 0
     172.10.120.0 0.0.0.3 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
     172.24.120.1         110      00:05:27
     172.24.121.1         110      00:06:02
     172.24.121.65        110      00:05:28
     172.24.121.193       110      00:05:28
     209.165.202.1        110      00:05:29
     209.165.202.2        110      00:05:28
   Distance: (default is 110)
```

Рисунок 3.10 – Налаштована маршутизація

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC2	PC7	ICMP		0.000	N	0	(edit)	(delete)
	Successful	PC7	PC2	ICMP		0.000	N	1	(edit)	(delete)

```
Lakiza_R4

User Access Verification

Username: lakiza2321ck1
Password:
Lakiza_R4>S
```

Рисунок 3.13 – Налаштований маршрутизатор на підтримку служби AAA

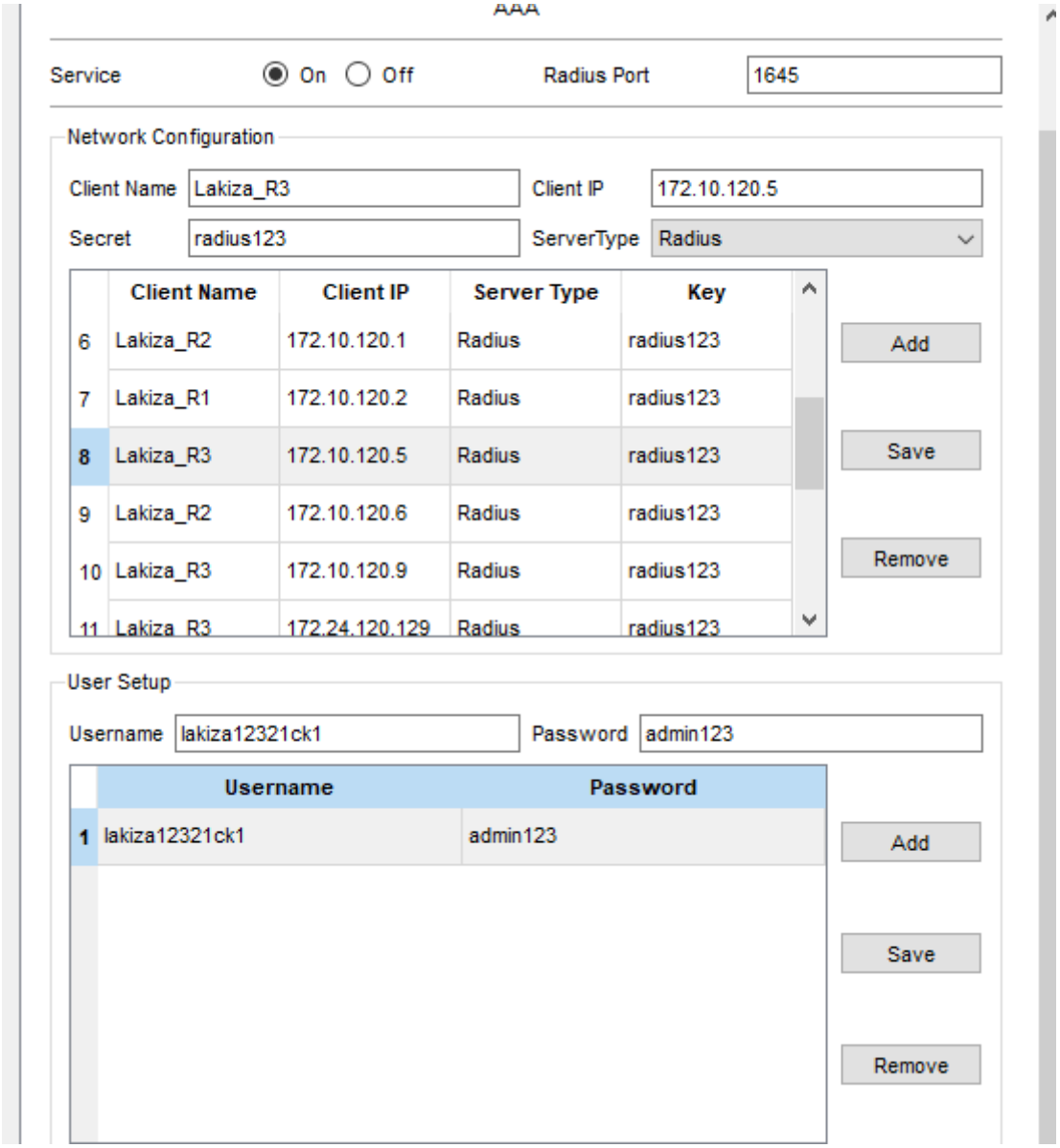


Рисунок 3.14 – Налаштування RADIUS-сервера

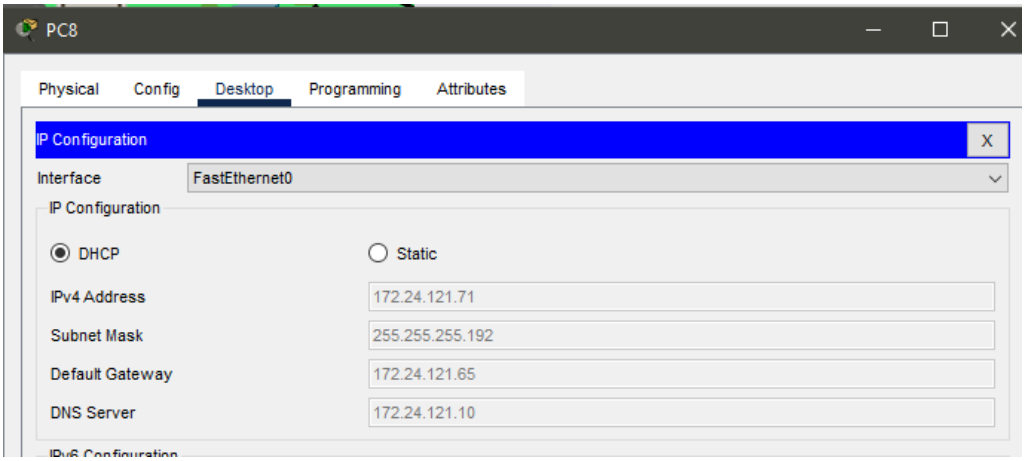


Рисунок 3.15 – Перевірка DHCP

```
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

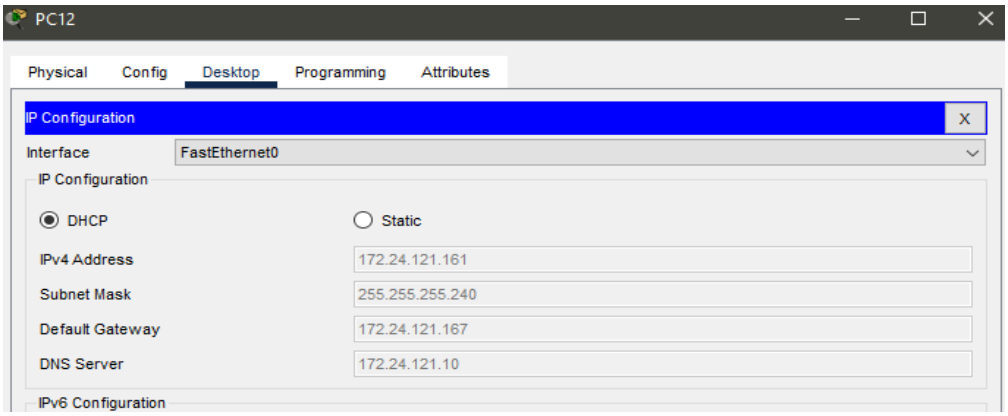


Рисунок 3.17 – Перевірка DHCP для VLAN

Successful	PC10	PC11	ICMP		0.000	N	0	(edit)	(delete)
Successful	PC10	PC11	ICMP		0.000	N	1	(edit)	(delete)
Successful	PC11	PC10	ICMP		0.000	N	2	(edit)	(delete)

Рисунок 3.18 – Зв’язок між VLAN

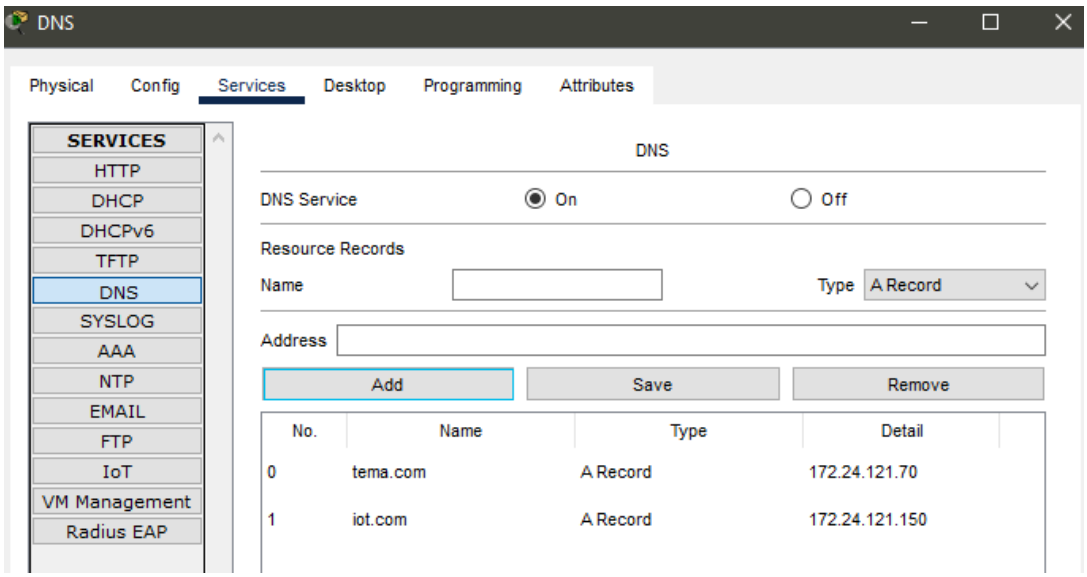


Рисунок 3.19 – DNS сервер

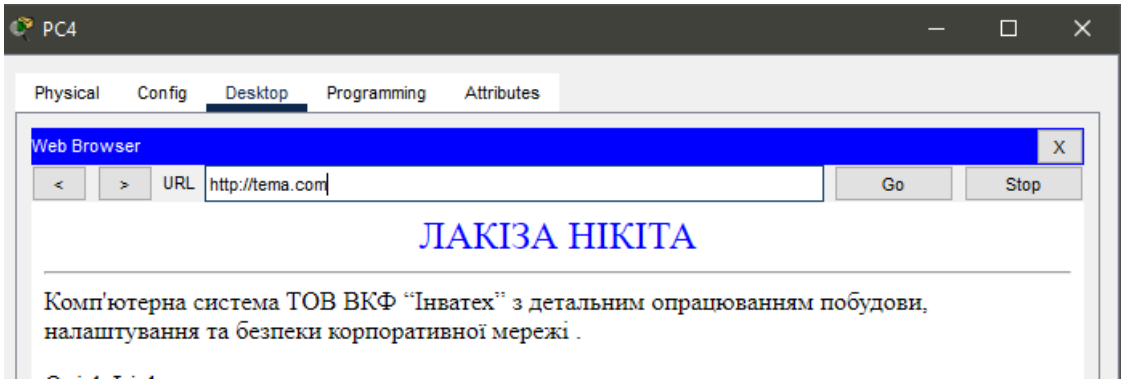


Рисунок 3.20 – Веб-сайт, який містить інформацію про тему і завдання для кваліфікаційної роботи студента

4 РОЗРОБКА КОМПОНЕНТА СИСТЕМИ

Після налаштування корпоративної мережі за заявою замовника розроблено IoT структуру захисту всіх локальних приміщень крім віддаленої мережі від несанкціонованого доступу за допомогою card reader`ов та розумних механізмів на дверях. Та також розробити клімат систему за допомогою мікроконтролерів при умові вмикання підігріву від 16 до 21 та за разом вмикання зволожувача повітря, при умові температури у діапазоні від 26 до 37 вмикати охолодження та вимикати зволожувач. Данні температури відправляти на сервер.

Internet of Things (IoT) описує мережу фізичних об'єктів—«речей»—які вбудовуються з сенсорами, програмним забезпеченням та іншими технологіями з метою з'єднання та обміну даними з іншими пристроями та системами через інтернет. Ці пристрої зібрані з широкого спектру областей, включаючи звичайні побутові предмети, як холодильники та світильники, до складніших інструментів, таких як монітори здоров'я, які забезпечують важливі медичні дані в реальному часі, або вузли промислового обладнання, що можуть прогнозувати та попереджати про потенційні збої у виробництві.

Розвиток IoT став можливим завдяки злиттю кількох технологій, включаючи безперервний доступ до інтернету, дешевші вартості з'єднань, збільшення мобільних пристроїв, а також великі досягнення в області нанотехнологій та обробки великих масивів даних. Це дало змогу IoT проникнути в різні сфери життя, покращуючи управління та ефективність операцій, зменшуючи витрати енергії та ресурсів та підвищуючи загальну якість життя через інтелектуальніше взаємодію між людьми та машинами.

Першим етапом монтуємо всі контролери датчики та пристрої на свої місця(рис. 4.1).

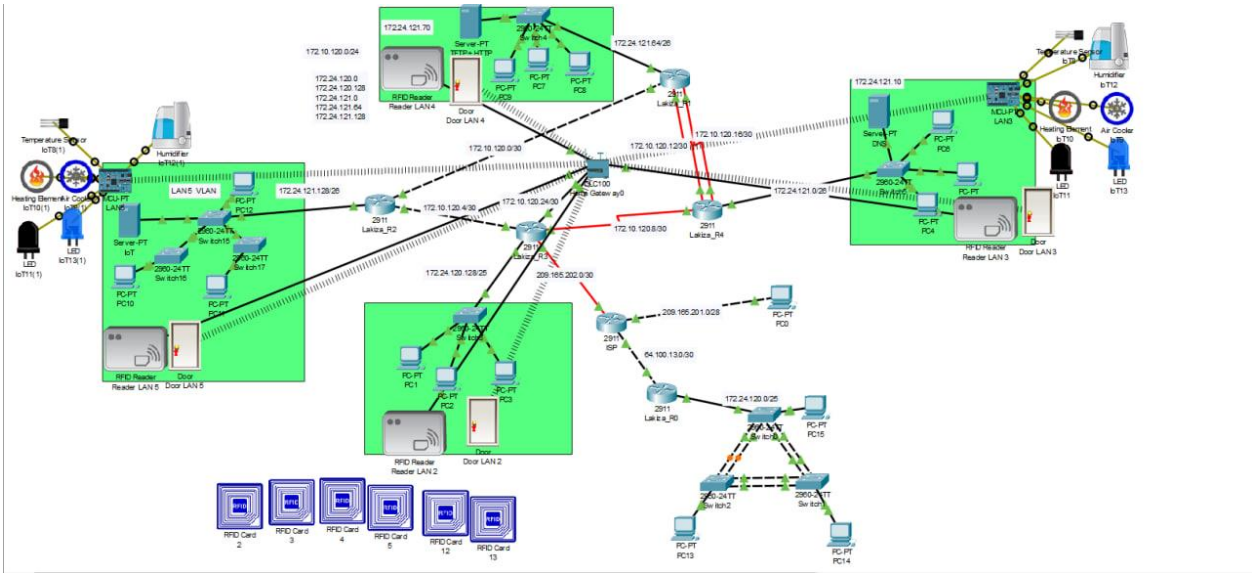


Рисунок 4.1 – Топологія мережі з пристроями

Далі підключаємо пристрої до home gateway раніше встановлений у мережі та задаємо йому налаштування бездротової мережі та підключення до віддаленого серверу на прикладі «DoorLAN3»(рис. 4.2-4.4).

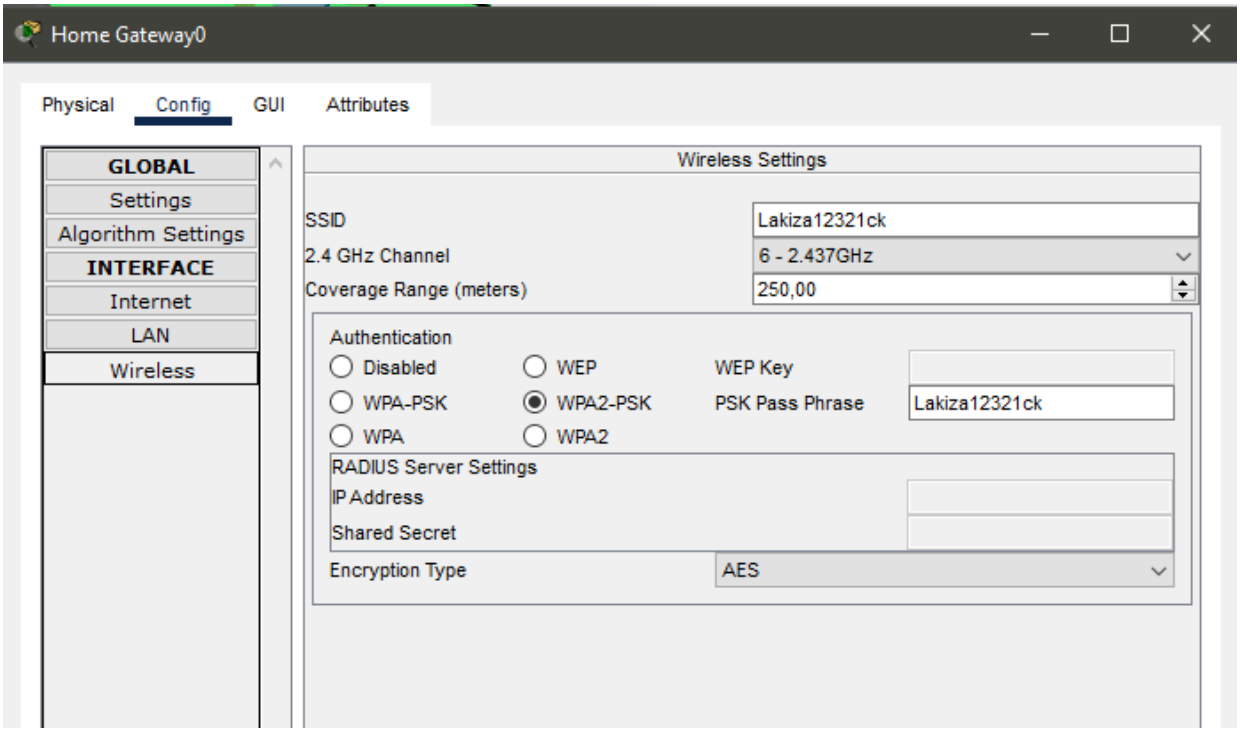


Рисунок 4.2 – Налаштування Home Gateway

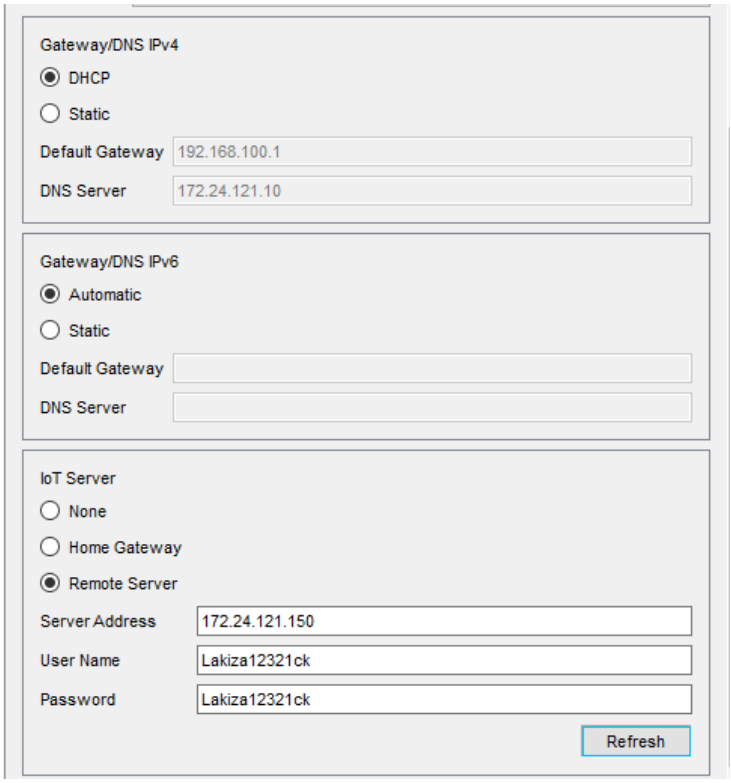


Рисунок 4.3 – Підключення пристрою до віддаленого серверу

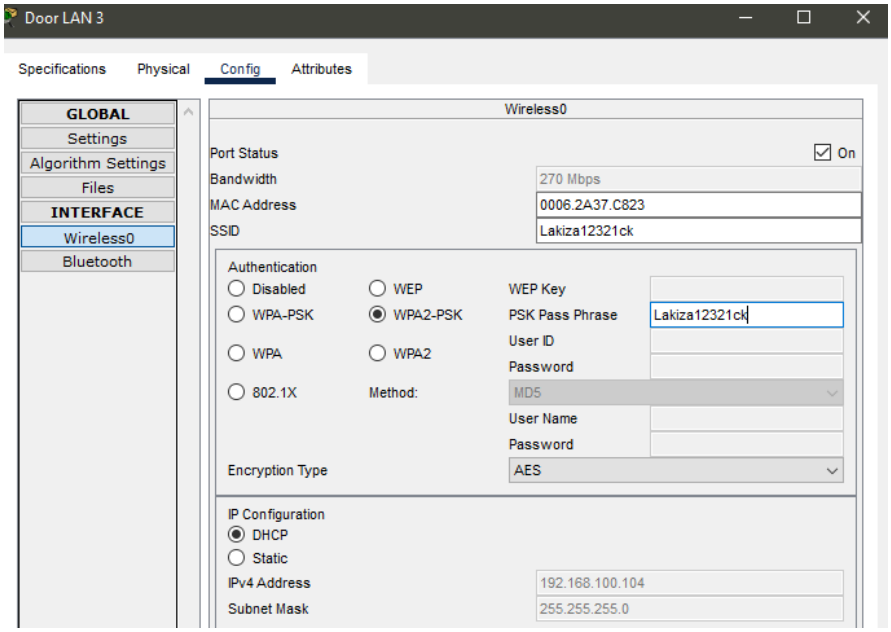


Рисунок 4.4 – Підключення до бездротової мережі та отримення адреси за допомогою DHCP

Підключаємось до серверу за допомогою веб браузеру, вводимо логін та пароль який раніше був створений та бачимо підключені пристрої(рис. 4.5-4.6).

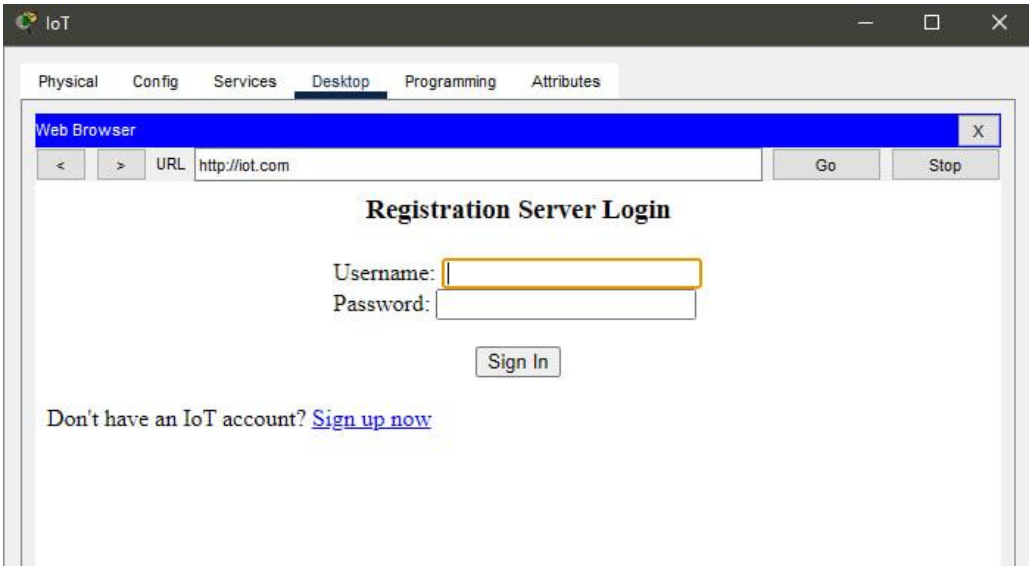


Рисунок 4.5 – Підключення до серверу

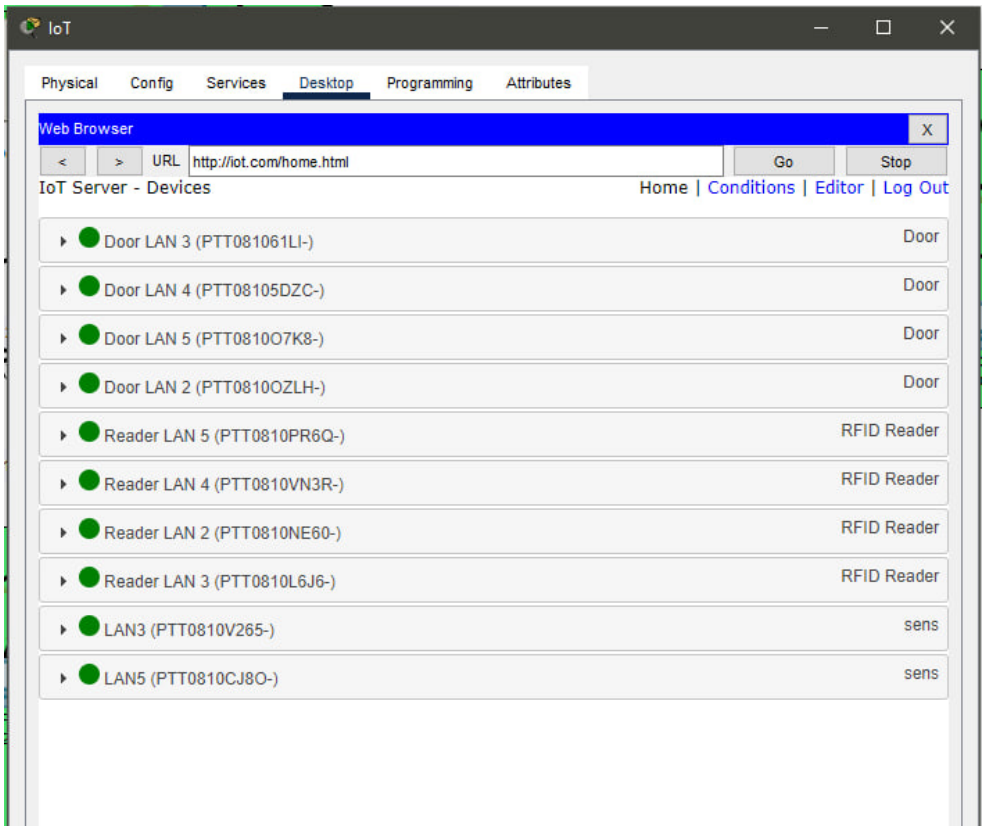
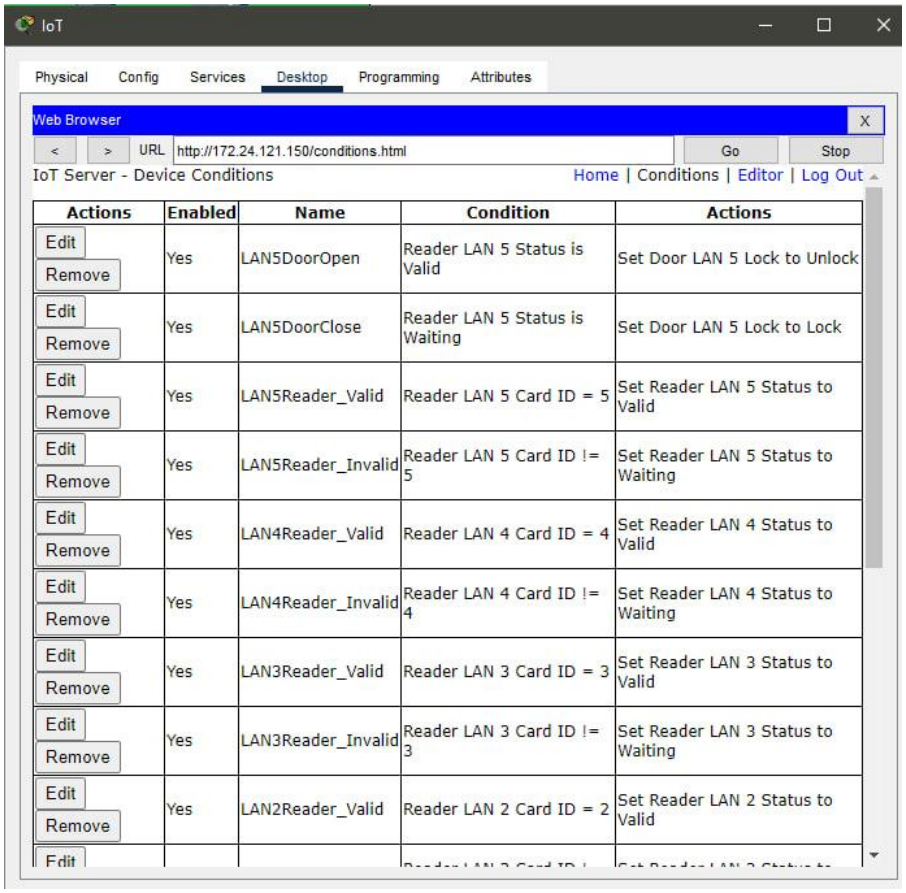


Рисунок 4.6 – Підключені пристрої

Наступним етапом на вкладці Conditions створюємо сценарії для доступу за RFID мітками та тестуємо роботу доступу на прикладі пристроїв з LAN2(рис. 4.7-4.10).



Actions	Enabled	Name	Condition	Actions
Edit Remove	Yes	LAN5DoorOpen	Reader LAN 5 Status is Valid	Set Door LAN 5 Lock to Unlock
Edit Remove	Yes	LAN5DoorClose	Reader LAN 5 Status is Waiting	Set Door LAN 5 Lock to Lock
Edit Remove	Yes	LAN5Reader_Valid	Reader LAN 5 Card ID = 5	Set Reader LAN 5 Status to Valid
Edit Remove	Yes	LAN5Reader_Invalid	Reader LAN 5 Card ID != 5	Set Reader LAN 5 Status to Waiting
Edit Remove	Yes	LAN4Reader_Valid	Reader LAN 4 Card ID = 4	Set Reader LAN 4 Status to Valid
Edit Remove	Yes	LAN4Reader_Invalid	Reader LAN 4 Card ID != 4	Set Reader LAN 4 Status to Waiting
Edit Remove	Yes	LAN3Reader_Valid	Reader LAN 3 Card ID = 3	Set Reader LAN 3 Status to Valid
Edit Remove	Yes	LAN3Reader_Invalid	Reader LAN 3 Card ID != 3	Set Reader LAN 3 Status to Waiting
Edit Remove	Yes	LAN2Reader_Valid	Reader LAN 2 Card ID = 2	Set Reader LAN 2 Status to Valid
Edit				

Рисунок 4.7 – Створені сценарії для доступу за RFID мітками

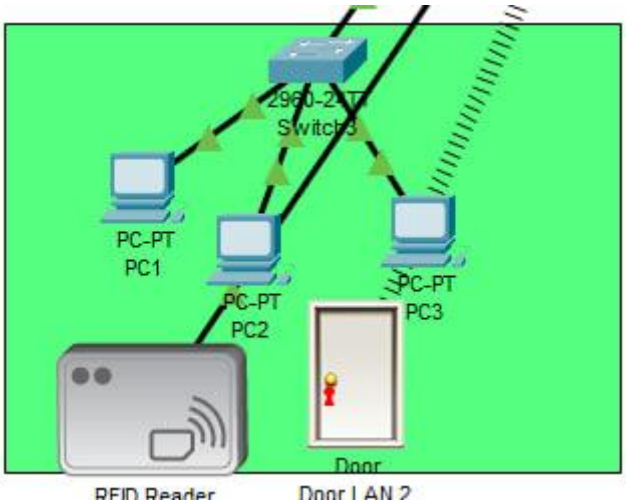


Рисунок 4.8 – Двері у зачиненому стані

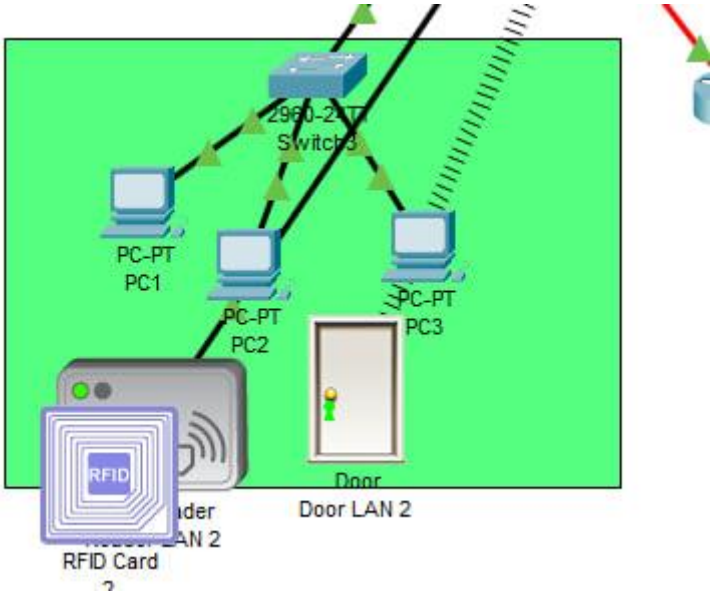


Рисунок 4.9 – Двері при зчитанні валідної картки

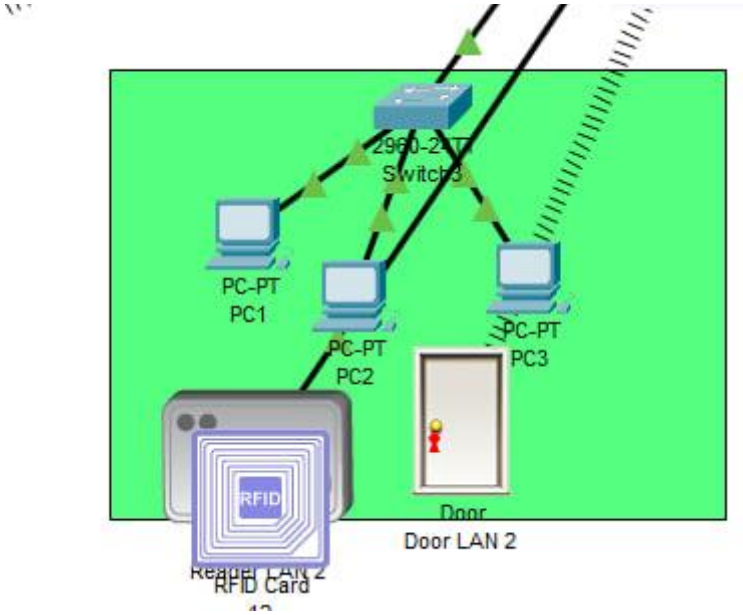


Рисунок 4.10 – Двері при зчитанні невалідної картки

Далі за допомогою мікроконтролера, елементів температури, діодів, температурного сенсору та зволожувача повітря пишемо код взаємодії та тестуємо кліматичну систему на прикладі LAN3

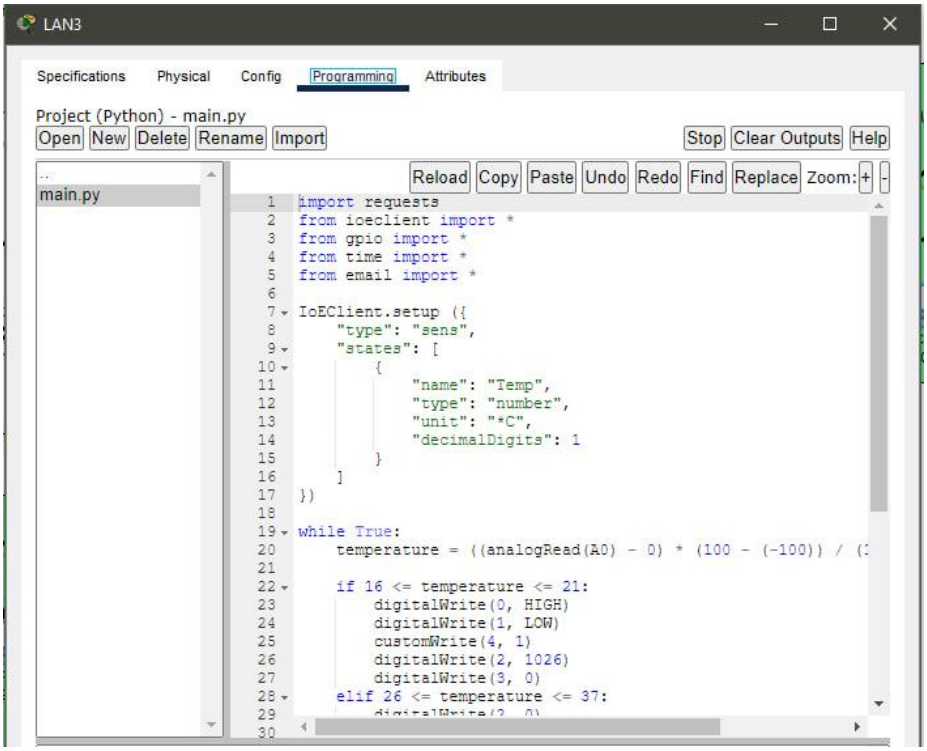


Рисунок 4.11 – Програмування на мікроконтроллері

Код програми наведено нижче:

```
from ioeclient import *
from gpio import *
from time import *
from email import *
IoEClient.setup ({
    "type": "sens",
    "states": [
        {
            "name": "Temp",
            "type": "number",
            "unit": "*C",
            "decimalDigits": 1
        }
    ]
})
while True:
    temperature = ((analogRead(A0) - 0) * (100 - (-100)) / (1023 - 0)) + (-100)

    if 16 <= temperature <= 21:
        digitalWrite(0, HIGH)
```

```
            digitalWrite(1, LOW)
            customWrite(4, 1)
            digitalWrite(2, 1026)
            digitalWrite(3, 0)
        elif 26 <= temperature <= 37:
            digitalWrite(2, 0)
            digitalWrite(3, 1026)
            digitalWrite(0, LOW)
            digitalWrite(1, HIGH)
            customWrite(4, 0)
        elif 21 <= temperature <= 26:
            digitalWrite(2, 0)
            customWrite(4, 0)
            digitalWrite(0, LOW)
            digitalWrite(1, LOW)
            digitalWrite(3, 0)

        IoEClient.reportStates([temperature])
        delay(500)

if name == "main":
    main()
```

Тестування роботи підсистеми відбувалося при різних температурах наведено на рисунках 4.12-4.13.

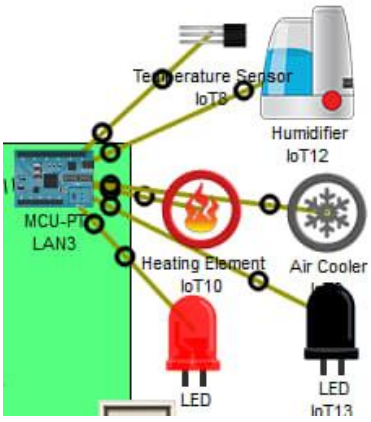


Рисунок 4.12 – Сценарів обігріву

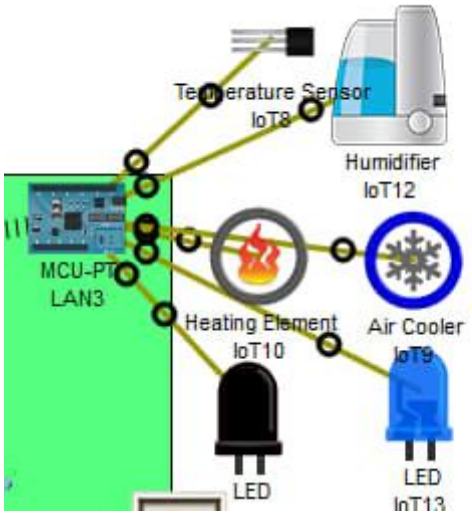


Рисунок 4.13 – Сценарій охолодження зони

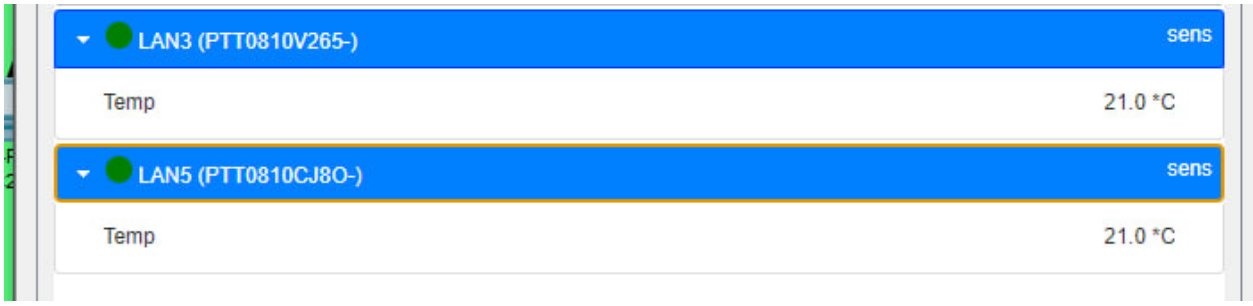


Рисунок 4.14 – Значеня температури у реальному часі на сервері

ВИСНОВКИ

У рамках кваліфікаційної роботи було розроблено та налаштовано комплексну корпоративну мережу для ТОВ ВКФ "Інватех". Робота зосереджувалася на побудові, налаштуванні, та забезпеченні безпеки мережевої інфраструктури. Було створено високоефективну систему, що відповідає сучасним вимогам до швидкодії, надійності та безпеки інформаційних потоків. Важливою частиною проєкту стала інтеграція IoT технологій для забезпечення захисту всіх локальних приміщень з допомогою card reader'ів та розумних механізмів на дверях, а також розробка кліматичної системи, керованої мікроконтролерами.

Результати проєкту демонструють високий рівень технічної досконалості та відповідність сучасним технологічним стандартам. Система не тільки ефективно вирішує поставлені задачі автоматизації контролю доступу та управління кліматом, але й відкриває нові можливості для розширення та інтеграції з іншими інтелектуальними системами у майбутньому.

Наукова та науково-технічна значущість роботи полягає в адаптації новітніх IoT технологій для потреб корпоративної безпеки та комфорту, що може бути застосоване в різних галузях, зокрема в промисловості, офісному управлінні, готельному бізнесі тощо. Соціально-економічна значущість роботи визначається підвищенням рівня безпеки працівників та оптимізацією витрат на утримання приміщень за рахунок ефективного управління ресурсами.

Доцільність продовження досліджень очевидна, адже додаткові розробки можуть включати впровадження розширених аналітичних інструментів для моніторингу і аналізу даних з IoT сенсорів, що дасть можливість ще більше оптимізувати процеси управління внутрішнім середовищем і збільшити загальну ефективність системи.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Методичні рекомендації до виконання кваліфікаційної роботи бакалавра студентами галузі знань 12 Інформаційні технології спеціальності 123 Комп’ютерна інженерія / Л.І. Цвіркун, С.М. Ткаченко, Я.В. Панферова, Д.О. Бешта, Л.В. Бешта. – Д.: НТУ «ДП», 2023-2024. – 62 с.

2. Автоматизація домашніх систем – Education [Електронний ресурс] – Режим доступу до ресурсу: https://itea.ua/aaa (дата звернення 25.05.2024р.)

3. Комп'ютерні мережі та безпека – Education [Електронний ресурс] – Режим доступу до ресурсу: https://itea.ua/network(дата звернення 27.05.2024р.)

4. Бази даних та їх оптимізація – Education [Електронний ресурс] – Режим доступу до ресурсу: https://itea.ua/sql/sqllite/bd(дата звернення 27.05.2024р.)

5. Розробка мобільних додатків – Education [Електронний ресурс] – Режим доступу до ресурсу: https://itea.ua/mobileapp/appwork(дата звернення 10.06.2024р.)

6. Системи штучного інтелекту – Education [Електронний ресурс] – Режим доступу до ресурсу: https://itea.ua/ai (дата звернення 11.06.2024р.)

7. Мікроконтролери – Education [Електронний ресурс] – Режим доступу до ресурсу: https://itea.ua/micro/python (дата звернення 31.05.2024р.)

8. Робота з IoT простоями – Education [Електронний ресурс] – Режим доступу до ресурсу: https://itea.ua/iot/read/manual (дата звернення 13.06.2024р.)

9. Температура та аналогове читання – Education [Електронний ресурс] – Режим доступу до ресурсу: https://itea.ua/tempread (дата звернення 14.06.2024р.)

10. RFID– Education [Електронний ресурс] – Режим доступу до ресурсу: https://itea.ua/rfidtech (дата звернення 14.06.2024р.)

Додаток А

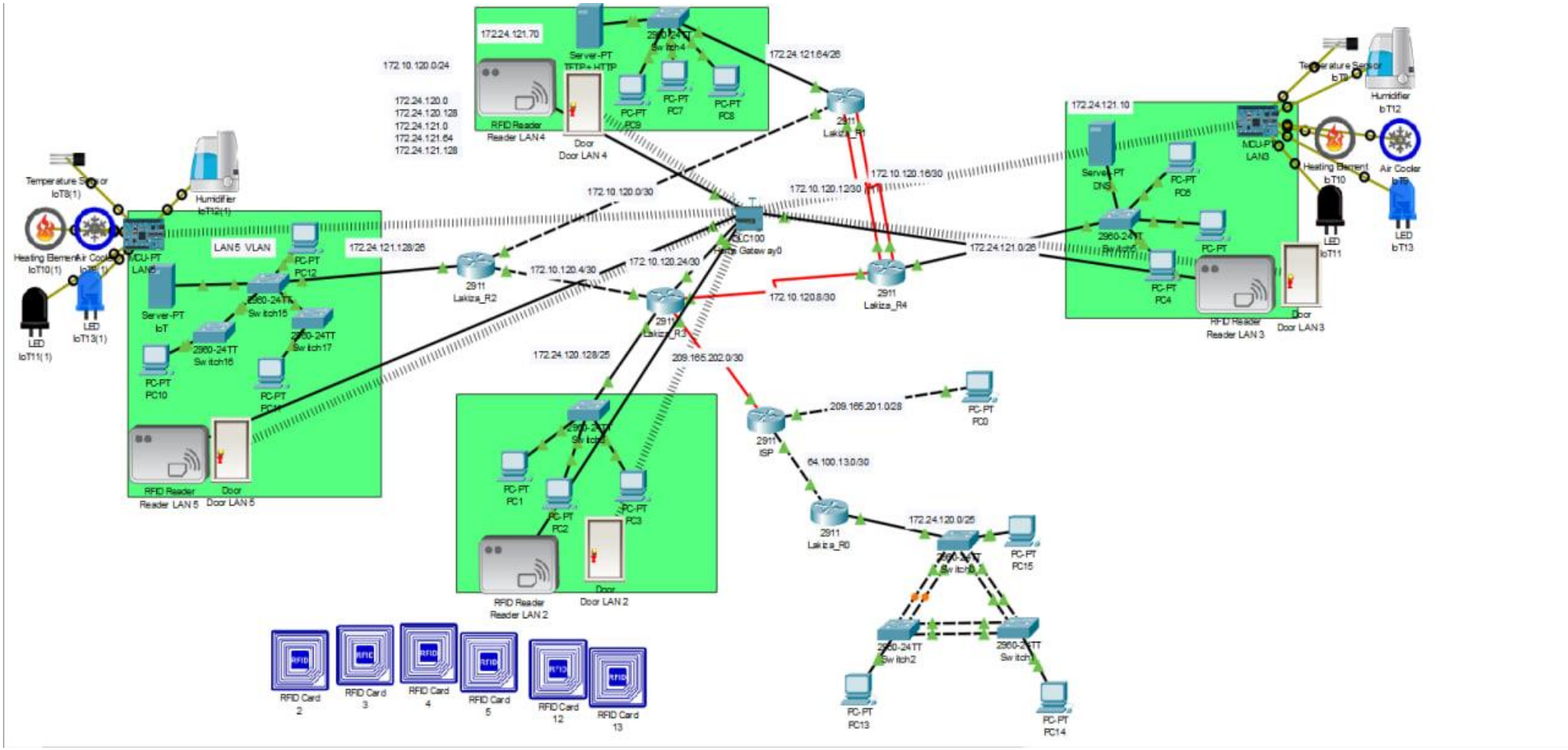


Рисунок ДА.1 – Загальна архітектура мережі

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

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ НАЛАШТУВАННЯ МЕРЕЖІ КОМП’ЮТЕРНОЇ СИСТЕМИ

Текст програми

804.02070743.24009-01 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. Lakiza_R3

```
Current configuration : 3073 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Lakiza_R3
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
ip dhcp excluded-address 172.24.120.129 172.24.120.135
ip dhcp pool LAN-2
network 172.24.120.128 255.255.255.128
default-router 172.24.120.129
dns-server 172.24.121.10
aaa new-model
!
aaa authentication login console group radius local
aaa authentication login default local
no ip cef
username 12321ck_Lakiza password 7 082048430017061E010803
username lakiza12321ck1 password 7 082048430017544541
license udi pid CISCO2911/K9 sn FTX1524L2XB-
ip domain-name Lakiza_R3
spanning-tree mode pvst
interface GigabitEthernet0/0
ip address 172.10.120.5 255.255.255.252
ip nat inside
duplex auto
```

```
speed auto
!
interface GigabitEthernet0/1
ip address 172.24.120.129 255.255.255.128
ip nat inside
duplex auto
speed auto
!
interface GigabitEthernet0/2
ip address 172.10.120.25 255.255.255.252
duplex auto
speed auto
!
interface Serial0/0/0
ip address 172.10.120.9 255.255.255.252
ip nat inside
clock rate 2000000
!
interface Serial0/0/1
ip address 209.165.202.1 255.255.255.252
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 Serial0/0/0
no passive-interface Serial0/0/1
auto-cost reference-bandwidth 1000
network 172.10.120.4 0.0.0.3 area 0
network 172.10.120.8 0.0.0.3 area 0
network 209.165.202.0 0.0.0.3 area 0
network 172.24.120.128 0.0.0.127 area 0
network 172.10.120.24 0.0.0.3 area 0
!
ip nat pool Internet 209.165.200.6 209.165.200.30 netmask 255.255.255.224
ip nat inside source list NAT10 pool Internet
ip nat inside source static 172.24.121.70 209.165.200.3
ip nat inside source static 172.24.121.10 209.165.200.4
ip nat inside source static 172.24.121.150 209.165.200.5
ip classless
!
ip flow-export version 9
!
!
ip access-list extended NAT10
deny ip 172.24.121.0 0.0.0.63 172.24.120.0 0.0.0.127
deny ip 172.24.120.128 0.0.0.127 172.24.120.0 0.0.0.127
deny ip 172.24.121.64 0.0.0.63 172.24.120.0 0.0.0.127
deny ip 172.24.121.128 0.0.0.63 172.24.120.0 0.0.0.127
deny ip 172.10.120.0 0.0.0.255 172.24.120.0 0.0.0.127
permit ip 172.24.121.0 0.0.0.63 any
permit ip 172.24.120.128 0.0.0.127 any
```

```
permit ip 172.24.121.64 0.0.0.63 any
permit ip 172.24.121.128 0.0.0.63 any
permit ip 172.10.120.0 0.0.0.255 any
!
banner motd ^CLakiza_R3^C
!
radius server host
address ipv4 172.24.121.150 auth-port 1645
key radius123
radius server 172.24.121.150
address ipv4 172.24.121.150 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. Lakiza_R1

```
Current configuration : 2653 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Lakiza_R2
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
ip dhcp excluded-address 172.24.121.137
ip dhcp excluded-address 172.24.121.153
ip dhcp excluded-address 172.24.121.167
ip dhcp pool LAN5-VLAN10
network 172.24.121.128 255.255.255.240
default-router 172.24.121.137
dns-server 172.24.121.10
ip dhcp pool LAN5-VLAN30
network 172.24.121.160 255.255.255.240
default-router 172.24.121.167
dns-server 172.24.121.10
ip dhcp pool LAN5-VLAN20
network 172.24.121.144 255.255.255.240
default-router 172.24.121.153
dns-server 172.24.121.10
aaa new-model
!
```

```
aaa authentication login console group radius local
aaa authentication login default local
ip cef
no ipv6 cef
username 12321ck_Lakiza password 7 082048430017061E010803
username lakiza12321ck1 password 7 082048430017544541
license udi pid CISCO2911/K9 sn FTX1524NBFQ-
ip domain-name Lakiza_R2
spanning-tree mode pvst
interface GigabitEthernet0/0
ip address 172.10.120.6 255.255.255.252
duplex auto
speed auto
!
interface GigabitEthernet0/1
ip address 172.10.120.1 255.255.255.252
duplex auto
speed auto
!
interface GigabitEthernet0/2
no ip address
duplex auto
speed auto
!
interface GigabitEthernet0/2.10
encapsulation dot1Q 10
ip address 172.24.121.137 255.255.255.240
!
interface GigabitEthernet0/2.20
```

```
encapsulation dot1Q 20
ip address 172.24.121.153 255.255.255.240
!
interface GigabitEthernet0/2.30
encapsulation dot1Q 30
ip address 172.24.121.167 255.255.255.240
!
interface GigabitEthernet0/2.99
encapsulation dot1Q 99
ip address 172.24.121.193 255.255.255.248
!
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
auto-cost reference-bandwidth 1000
network 172.24.121.128 0.0.0.63 area 0
network 172.10.120.4 0.0.0.3 area 0
network 172.10.120.0 0.0.0.3 area 0
!
ip classless
!
ip flow-export version 9
```

```
banner motd ^CLakiza_R2^C
!
radius server host
address ipv4 172.24.121.150 auth-port 1645
key radius123
radius server 172.24.121.150
address ipv4 172.24.121.150 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. Lakiza_R0

```
Current configuration : 1856 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Lakiza_R0
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
ip dhcp excluded-address 172.24.120.1 172.24.120.10
ip dhcp pool LAN-1
network 172.24.120.0 255.255.255.128
default-router 172.24.120.1
dns-server 172.24.121.10
aaa new-model
aaa authentication login console group radius local
aaa authentication login default local
ip cef
no ipv6 cef
username 12321ck_Lakiza password 7 082048430017061E010803
username lakiza12321ck1 password 7 082048430017544541
license udi pid CISCO2911/K9 sn FTX1524O914-
ip domain-name Lakiza_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 172.24.120.1 255.255.255.128
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 64.100.13.0 0.0.0.3 area 0
network 172.24.120.0 0.0.0.127 area 0
!
ip classless
!
ip flow-export version 9
!
banner motd ^CLakiza_R0^C
!
```

```
radius server host
address ipv4 172.24.121.150 auth-port 1645
key radius123
radius server 172.24.121.150
address ipv4 172.24.121.150 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.switch15

```
Current configuration : 1828 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
```

```
!
hostname Switch
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
switchport mode trunk
!
interface FastEthernet0/2
switchport mode trunk
!
interface FastEthernet0/3
switchport mode trunk
!
interface FastEthernet0/4
switchport mode trunk
!
interface FastEthernet0/5
switchport mode trunk
!
interface FastEthernet0/6
switchport access vlan 10
switchport mode access
!
interface FastEthernet0/7
switchport access vlan 10
switchport mode access
!
interface FastEthernet0/8
```

```
switchport access vlan 10
switchport mode access
!
interface FastEthernet0/9
switchport access vlan 10
switchport mode access
!
interface FastEthernet0/10
switchport access vlan 10
switchport mode access
!
interface FastEthernet0/11
switchport access vlan 20
!
interface FastEthernet0/12
switchport access vlan 20
!
interface FastEthernet0/13
switchport access vlan 20
!
interface FastEthernet0/14
switchport access vlan 20
!
interface FastEthernet0/15
switchport access vlan 20
!
interface FastEthernet0/16
switchport access vlan 20
!
```

```
interface FastEthernet0/17
switchport access vlan 30
!
interface FastEthernet0/18
switchport access vlan 30
!
interface FastEthernet0/19
switchport access vlan 30
!
interface FastEthernet0/20
switchport access vlan 30
!
interface FastEthernet0/21
switchport access vlan 30
!
interface FastEthernet0/22
switchport access vlan 30
!
interface FastEthernet0/23
switchport access vlan 30
!
interface FastEthernet0/24
switchport access vlan 30
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
```

```
no ip address
shutdown
line con 0
!
line vty 0 4
login
line vty 5 15
login
```

5.switch10

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

```
switchport mode trunk
channel-group 1 mode active
!
interface FastEthernet0/2
switchport mode trunk
channel-group 1 mode active
!
interface FastEthernet0/3
switchport mode trunk
channel-group 2 mode active
!
interface FastEthernet0/4
switchport mode trunk
channel-group 2 mode active
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
```

```
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
```

```
!
interface Vlan1
no ip address
shutdown
!
line con 0
!
line vty 0 4
login
line vty 5 15
login
end
```