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 с ступеня бакалавра

здобувача Алексійчука Марко Романовича
(ПІБ)

академічної групи 123-21-2
(шифр)

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

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

на тему «Комп'ютерна система логістичної компанії з детальним опрацюванням побудови та налаштування корпоративної мережі з інтеграцією IoT-системи складського комплексу»
(назва за наказом ректора)

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

Дніпро
2025

ЗАТВЕРДЖЕНО:
завідувач кафедри
інформаційних технологій
та комп'ютерної інженерії
(повна назва)
_____ Гнатушенко В.В.
(підпис) (прізвище, ініціали)

"_" ___ 2025 року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавр

здобувача Алексійчука М.Р. **академічної групи** 123-21-2
(прізвище та ініціали) (шифр)

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

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

на тему «Комп'ютерна система логістичної компанії з детальним опрацюванням побудови та налаштування корпоративної мережі з інтеграцією IoT-системи складського комплексу»

затверджену наказом ректора НТУ «Дніпровська політехніка» від 05.05.2025 № 336-с

Розділ	Зміст	Термін виконання
Стан питання та постановка завдання	На основі матеріалів виробничих практик, інших науково-технічних джерел конкретизується предмет та мету роботи та виконується постановка завдання	10.05.2025
Розробка апаратної частини	На основі аналізу підприємства формулюються технічні вимоги до комп'ютерної системи та розробляється апаратна частина системи	17.05.2025
Розробка корпоративної мережі	Виконується розрахунок налаштувань корпоративної мережі та перевірка роботи системи, розробляються методи та налаштування обладнання для захисту інформації в системі	24.05.2025
Розробка компонента системи	Виконується детальна розробка компонента системи	31.05.2025

Завдання видано _____ доц. Бешта Д.О.
(підпис керівника) (прізвище, ініціали)

Дата видачі 25.02.2025

Дата подання до екзаменаційної комісії 16.06.2025

Прийнято до виконання _____ Алексійчук М.Р.

РЕФЕРАТ

Пояснювальна записка: 93 с., 44 рис., 6 табл., 1 додаток, 5 джерел.

КОМП'ЮТЕРНА СИСТЕМА, IOT, СКЛАД, БЕЗПЕКА, DHCP, EIGRP

Об'єкт розробки: комп'ютерна система логістичної компанії, що автоматизує роботу складського комплексу шляхом розробки, налаштування та забезпечення безпеки корпоративної мережі з використанням технологій Інтернету речей (IoT).

Мета: Метою даної роботи є розробка комп'ютерної системи для логістичної компанії, яка включає побудову корпоративної мережі з інтеграцією елементів Інтернету речей (IoT) для автоматизації складського комплексу.

У процесі розробки буде розроблено корпоративну мережу, яка забезпечить стабільну та захищену передачу даних, підтримку ключових мережевих служб, таких як DHCP, NAT, VPN і ACL, а також використання VLAN для сегментації трафіку. Можливості масштабування та подальшої модернізації мережі відповідно до потреб компанії будуть привертати особливу увагу.

Модель комп'ютерної мережі буде реалізована в середовищі Cisco Packet Tracer, яке забезпечить моделювання взаємодії мережевих вузлів, перевірку функціональності мережі та роботу пристроїв Інтернету речей. Щоб підтвердити працездатність запропонованого рішення, результати симуляцій будуть документовані у вигляді схем, таблиць та описів.

Розробка системи дозволить створити IT-інфраструктуру, яка може бути масштабована, гнучка та безпечна, здатну оптимізувати логістичні операції, покращити взаємодію між підрозділами та гарантувати ефективне управління ресурсами компанії.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАК, ОДИНИЦЬ І ТЕРМІНІВ

WMS (Warehouse Management System) – система керування складом, що автоматизує облік, зберігання і рух товарів на складі.

IoT (Internet of Things) – Інтернет речей, мережа фізичних пристроїв, які збирають і обмінюються даними через інтернет.

ПК – Персональний комп’ютер

CRM (Customer Relationship Management) – система управління взаємовідносинами з клієнтами для підвищення якості обслуговування і продажів.

LAN (Local Area Network) – локальна комп’ютерна мережа, що з’єднує пристрої в межах обмеженої території (офіс, будівля).

VLAN (Virtual Local Area Network) – віртуальна локальна мережа, що логічно розділяє фізичну мережу на декілька сегментів.

WCS (Warehouse Control System) – система керування складським обладнанням (конвеєри, роботи) для оптимізації руху товарів.

WES (Warehouse Execution System) – система виконання складських операцій, координує роботу між WMS і WCS для підвищення ефективності.

ERP (Enterprise Resource Planning) – комплексна система управління ресурсами підприємства (фінанси, виробництво, логістика).

VPN (Virtual Private Network) – віртуальна приватна мережа для безпечного захищеного доступу до мережі через інтернет.

NAT_ACL (Network Address Translation with Access Control List) – трансляція мережевих адрес із застосуванням списків контролю доступу.

RFID мітки (Radio Frequency Identification tags) – радіочастотні ідентифікатори для автоматичного зчитування інформації про об’єкти.

DHCP (Dynamic Host Configuration Protocol) – протокол автоматичного призначення IP-адрес пристроям у мережі.

EIGRP (Enhanced Interior Gateway Routing Protocol) – покращений внутрішній протокол маршрутизації для швидкого і надійного обміну маршрутами в мережі.

ВСТУП

У сучасному світі стрімкий розвиток цифрових технологій змінює підходи до організації бізнес-процесів у різних сферах діяльності. Зокрема, у сфері логістики дедалі більшого значення набувають автоматизовані комп'ютерні системи, що дозволяють ефективно керувати потоками товарів, обміном інформації та внутрішніми процесами компаній. Одним із ключових напрямів модернізації логістичних підприємств є впровадження сучасних корпоративних мереж із підтримкою технологій Інтернету речей (IoT), що відкриває нові можливості для моніторингу, контролю та оптимізації логістичних операцій.

Успішне функціонування логістичної компанії значною мірою залежить від здатності швидко обробляти великі обсяги даних, забезпечувати безперервний обмін інформацією між підрозділами та підтримувати зв'язок із зовнішніми партнерами. Для досягнення цих цілей необхідно створити надійну та масштабовану комп'ютерну систему, яка інтегрує офісну та складську інфраструктуру в єдиний інформаційний простір.

У даній роботі розглядається процес розробки комп'ютерної системи для логістичної компанії, який включає побудову корпоративної мережі з урахуванням специфіки підприємства та впровадження IoT-рішень у складському комплексі. Основна увага приділяється розробці структури мережі, вибору відповідного мережевого та обчислювального обладнання, а також моделюванню системи у віртуальному середовищі Cisco Packet Tracer. Реалізація такого рішення сприятиме підвищенню ефективності логістичних процесів, покращенню керованості складських ресурсів та забезпеченню надійної роботи всіх IT-компонентів підприємства. Актуальність теми зумовлена потребою логістичних компаній у цифровій трансформації для забезпечення конкурентоспроможності на ринку.

1 СТАН ПИТАННЯ І ПОСТАНОВКА ЗАВДАННЯ

1.1 Характеристика логістичної компанії та умови впровадження комп'ютерної системи з інтеграцією IoT

Сучасні логістичні підприємства прагнуть забезпечити ефективне управління товаропотоком на всіх етапах – від постачання до кінцевого споживача. Рівень цифрової трансформації підприємства є важливим для досягнення високої операційної ефективності; це включає впровадження автоматизованих інформаційних систем і інтелектуальних технологій, таких як Інтернет речей (IoT).

Адміністративний офіс, диспетчерський центр, транспортний відділ і складський комплекс є основними підрозділами логістичної структури компанії. Необхідно створити корпоративну комп'ютерну мережу, щоб вони могли постійно спілкуватися один з одним. Це дозволить керувати, зберігати та обмінюватися даними в одному місці.

Як один із найбільш ресурсомістких компонентів логістичної інфраструктури, складський комплекс потребує постійного контролю за фізичними умовами зберігання, переміщенням вантажів, оптимізацією заповнення площі та мінімізацією впливу людей. У цій сфері використання Інтернету речей має найбільший потенціал. Рекомендовані технологічні рішення включають:

– Сенсори температури, вологості та освітленості для спостереження за станом зберігання;
– RFID-мітки, які дозволяють ідентифікувати працівників;
– інтелектуальні системи для управління доступом;
– роботизовані платформи для ваги та механізми переміщення вантажів.

Комп'ютерна система компанії повинна об'єднувати складські та офісні підрозділи, створюючи єдине інформаційне середовище. Це забезпечить централізований облік, координацію логістичних операцій і підтримку аналітики бізнесу на основі оперативних даних про стан складської та транспортної інфраструктури.

При проектуванні мережі особлива увага приділяється таким аспектам:

- захист інформації;
- забезпечення дублювання каналів зв’язку та джерел живлення є важливим компонентом резервування;
- масштабованість – це здатність розширювати IoT-інфраструктуру, щоб задовольнити зростаючі потреби компанії;
- висока відмовостійкість і надійність забезпечують безперервність роботи системи.

1.2.1 Огляд існуючих інженерних рішень систем в галузі та визначення можливих напрямків рішення поставлених завдань

Для того, щоб логістичні центри працювали ефективно, необхідні інженерні рішення для автоматизації складських процесів. Такі рішення базуються на використанні програмно-апаратних комплексів, спрямованих на автоматизацію управління ресурсами, процесами та взаємодією між усіма компонентами.

WMS – це система управління складами.Основним інструментом для управління всіма операціями з товарами, починаючи з моменту їх отримання та закінчуючи моментом відвантаження, є система управління складом. WMS оптимізує процеси, такі як інвентаризація, комплектування замовлень, управління запасами та розміщення продуктів. Система часто працює з мобільними пристроями, такими як сканери та термінали, і вона може працювати з іншими корпоративними платформами, такими як ERP.

Система керування складом (WCS).Система керування обладнанням складу призначена для безпосередньої координації роботи автоматизованих механізмів, таких як автоматичні візки (AGV), сортувальники, конвеєри та крани-штабелери. WCS служить «посередником» між WMS і фізичними пристроями, що дозволяє виконувати логістичні завдання на рівні обладнання. Це забезпечує високу точність і швидкість виконання операцій у реальному часі.

WES (Warehouse Execution System) Розумний рівень управління складом, який поєднує функції WMS та WCS. Він приймає рішення в режимі реального часу

на основі пріоритетів, завантаженості системи та статусу обладнання, щоб оптимізувати поточні завдання. WES дозволяє зменшити затримки та уникнути перевантаження вузьких місць у логістичному ланцюгу, розподіляючи навантаження між зонами та адаптуючи плани виконання замовлень до поточних обставин.

ERP-система охоплює загальне управління підприємством – фінансами, людськими ресурсами, закупівлями, продажами та виробництвом. У контексті логістики ERP інтегрується з WMS, забезпечуючи наскрізну автоматизацію бізнес-процесів: від надходження замовлення до формування аналітики щодо обсягів продажів та залишків на складі.

Рисунок 1.1 – Повна інтегрована система для автоматизації складу WMS

1.2.2 Характеристика і організаційна структура підприємства логістичної компанії

Організаційна структура підприємства є важливим фактором, який визначає, наскільки добре працюють комп'ютерні системи та інтелектуальні технології, зокрема системи з інтеграцією Інтернету речей (IoT). Вона закладає основу для управління інформаційними потоками, розподілу функціональних обов'язків і оперативного реагування на зміни в будь-якому зовнішньому або внутрішньому середовищі. У сфері логістики він є основою для створення гнучкої, адаптивної системи управління, яка поєднує транспортні операції, автоматизовані складські комплекси та цифрову аналітиці.

Рівень стратегічно-адміністративного управління. На цьому етапі визначаються цілі та цілі компанії, а також приймаються важливі рішення щодо фінансування, розвитку інфраструктури, інтеграції IT-систем і інновацій.

Генеральний директор керує всією компанією та визначає її шлях розвитку, особливо стратегічні напрями цифровізації. приймає рішення щодо розширення IoT-систем, автоматизації логістичних операцій і впровадження ERP-платформ.

Заступник директора з операційної діяльності відповідає за координацію взаємодії між усіма функціональними підрозділами, нагляд за виконанням операційних планів і відповідає за впровадження інструментів WMS, WES і WCS.

Відділ стратегічного планування аналізує тенденції в галузі, готує аналітичні висновки щодо доцільності впровадження цифрових технологій, прогнозує майбутні потреби компанії в IT-інфраструктурі та управлінні ланцюгом постачання.

Секретаріат відповідає за адміністративну підтримку, внутрішню комунікацію та організацію нарад; він також керує документацією IT-проектів і організовує зустрічі з підрядниками програмного та апаратного забезпечення.

Блок логістики та виробництваЦей рівень забезпечує виконання основних логістичних завдань компанії, таких як формування маршрутів доставки та управління складськими запасами, які активно підтримуються цифровими платформами.

Логістичний керівник підрозділу відповідає за загальне управління

логістичними операціями; розробка логістичних схем; нагляд за взаємодією з постачальниками; і використання WMS/WES для управління потоками вантажів і KPI для процесів управління потоками вантажів.

Планувальники-логісти співпрацюють з системами ERP для управління ланцюгом постачання. аналізують минулі дані для планування маршрутів, відстежують терміни доставки та оптимізують використання транспорту.

Диспетчерська служба спостерігає за рухом транспорту в режимі реального часу та використовує GPS-трекери та мобільні пристрої IoT, щоб приймати рішення щодо корекції маршрутів, враховуючи дорожні умови та інциденти.

Фахівці з телематики відповідають за налаштування, технічну підтримку та калібрування транспортного обладнання IoT, такого як датчики температури, вібродатчики та системи контролю доступу, які передають дані в центральну систему зберігання управління (WMS) або ERP-систему.

Впровадження Інтернету речей починається на складі.RFID-технології, сенсорні мережі, мобільні сканери, автономні транспортні системи та роз'ємні системи зберігання широко застосовуються на складах, які є основними об'єктами автоматизації.

Планування та контроль усіх внутрішніх логістичних процесів, впровадження автоматизованих систем зберігання та інтеграція з Warehouse Control System (WCS), який керує технічним обладнанням, таким як сортувальники та стрічкові транспортери, належать до обов'язків начальника складу.

Оператори приймання та відвантаження використовують RFID-мітки, планшети або термінали збору даних (TSD) для контролю над вантажами. Вони працюють із цифровими картами складу, створеними WMS.

Комірники здійснюють інвентаризацію за допомогою цифрових шаблонів, сканують товари за допомогою мобільних пристроїв і виконують внутрішньоскладські переміщення відповідно до маршрутів, сформованих WES.

Комплектувальники працюють з автоматизованими конвеєрами, роботизованими каретками, системами «взяття до світла» та «взяття голосу», які в реальному житті отримують команди від WCS.

Підрозділ IT: цифрові аспекти управління підприємством. Цей підрозділ відповідає за кібербезпеку та інтеграцію зовнішніх платформ, керує внутрішніми сервісами та підтримує зв’язок між відділами. Він також відповідає за функціонування всієї цифрової інфраструктури компанії.

Керівник IT-відділу відповідає за стратегічне управління всією IT-інфраструктурою, підбір програмного забезпечення, впровадження хмарних рішень (наприклад, гібридних ERP-платформ) і впровадження.

Системні адміністратори відповідають за безперебійну роботу мережі, доступ до корпоративних систем, налаштування віртуальної приватної мережі, моніторинг безпеки, резервне копіювання даних і захист даних від несанкціонованого доступу.

Фахівці з інтеграції Інтернету речей займаються встановленням і налаштуванням пристроїв Інтернету речей (IoT), таких як контролери, шлюзи та сенсори. Вони також керують збором і передачею телеметрії, проводять моніторинг працездатності систем і оптимізують взаємодію між IoT-пристроями та центральним WMS/ERP.

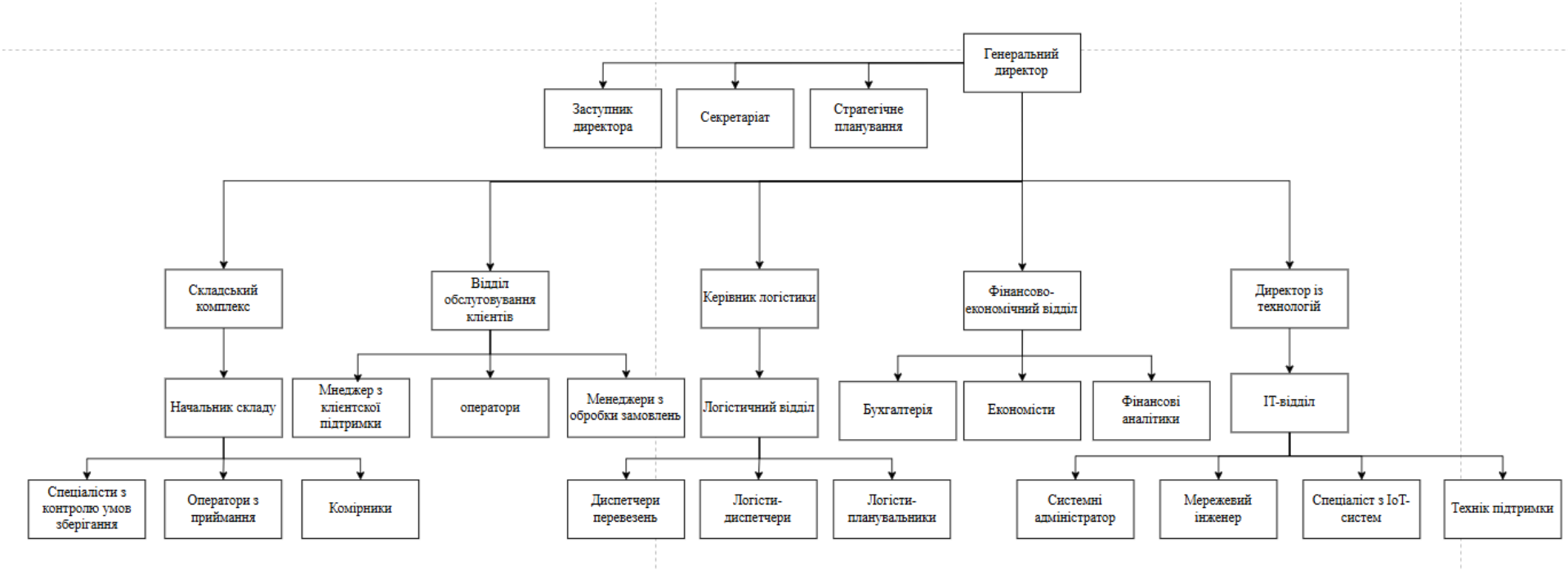


Рисунок 1.2 – Схема організаційної структури логістичної компанії

1.3 Схема розміщення об'єкта та внутрішнє планування приміщень

Ефективне функціонування логістичного підприємства значною мірою залежить від правильно організованого просторового планування, яке забезпечує оптимальні умови для переміщення матеріальних і інформаційних потоків. Раціональне зонування адміністративних, складських і технічних приміщень сприяє безперервності логістичних процесів, полегшує доступ до ключових ділянок роботи та створює відповідні умови для впровадження цифрових рішень, зокрема технологій Інтернету речей (IoT).

Будівля логістичної компанії має два поверхи з чітким функціональним розподілом. Перший поверх призначено для операційної діяльності, а другий – для аналітичної, технічної та управлінської роботи. Такий поділ дозволяє ефективно організувати робочі процеси та логічно згрупувати персонал відповідно до його функціональних обов’язків.

На першому поверсі розміщено складський комплекс, який включає центральну зону зберігання зі стелажними системами для різних типів товарів. Тут працюють комірники, начальник складу та спеціалісти з контролю умов зберігання. Склад обладнаний сенсорами IoT для моніторингу температури, вологості, рівня заповнення зон, а також RFID-мітками, сканерами штрихкодів і терміналами збору даних, інтегрованими з системами WMS та ERP. Зона приймання та відвантаження вантажів розташована вздовж одного з фасадів складу, де встановлені рампи з платформами-доклеверами, промислові сканери, вагові модулі. У цій зоні здійснюється первинна ідентифікація вантажів, фіксація їх у базі даних та звірка з інформацією про замовлення.

Поряд розташований відділ обслуговування клієнтів, у якому працюють менеджери з клієнтської підтримки, оператори та менеджери з обробки замовлень. Цей відділ забезпечує оперативне реагування на запити, уточнення статусу замовлень, обробку рекламацій і підтримку через CRM-систему, з інтеграцією до облікових і логістичних модулів.

У межах першого поверху також розміщено логістичний відділ, у якому

працюють диспетчери перевезень, логісти-диспетчери та логісти-планувальники. Вони відповідають за формування маршрутів доставки, контроль графіків перевезень, облік транспортних засобів і взаємодію з водіями. Робочі місця обладнані інтерфейсами WMS, WES і GPS-моніторингу.

У зоні головного управління компанією знаходиться робочий кабінет керівника, інтегрований із системами стратегічного планування, ERP, CRM і відеозв'язку. Поруч розташований відділ охорони, що контролює доступ до об'єкта, слідкує за сигналізацією, керує системами відеоспостереження, датчиками руху та пожежною безпекою. Система контролю доступу забезпечує фіксацію входів/виходів, а охоронний пост функціонує цілодобово.

Другий поверх призначений для розміщення IT-відділу та фінансово-економічного підрозділу. В IT-відділі працюють системні адміністратори, мережеві інженери, спеціалісти з IoT-систем і технічна підтримка. Тут також знаходиться тестова зона для перевірки сенсорного обладнання, шлюзів, маршрутизаторів і серверного обладнання. Передбачено клімат-контроль, вентиляцію та систему пожежогасіння для забезпечення надійної роботи IT-інфраструктури.

У фінансово-економічному відділі зосереджені фінансові аналітики, економісти та працівники бухгалтерії, які працюють із системами фінансового обліку, формуванням звітності, управлінням бюджетом і контролем витрат. Їхнє розміщення забезпечує зручний доступ до управлінських систем і тісну взаємодію з іншими підрозділами, що сприяє ефективному управлінню ресурсами компанії.

Загальна архітектура об'єкта дозволяє забезпечити ефективну організацію роботи персоналу, оптимальні логістичні маршрути всередині приміщення, а також масштабованість для впровадження нових технологій та розширення функціональності в майбутньому.

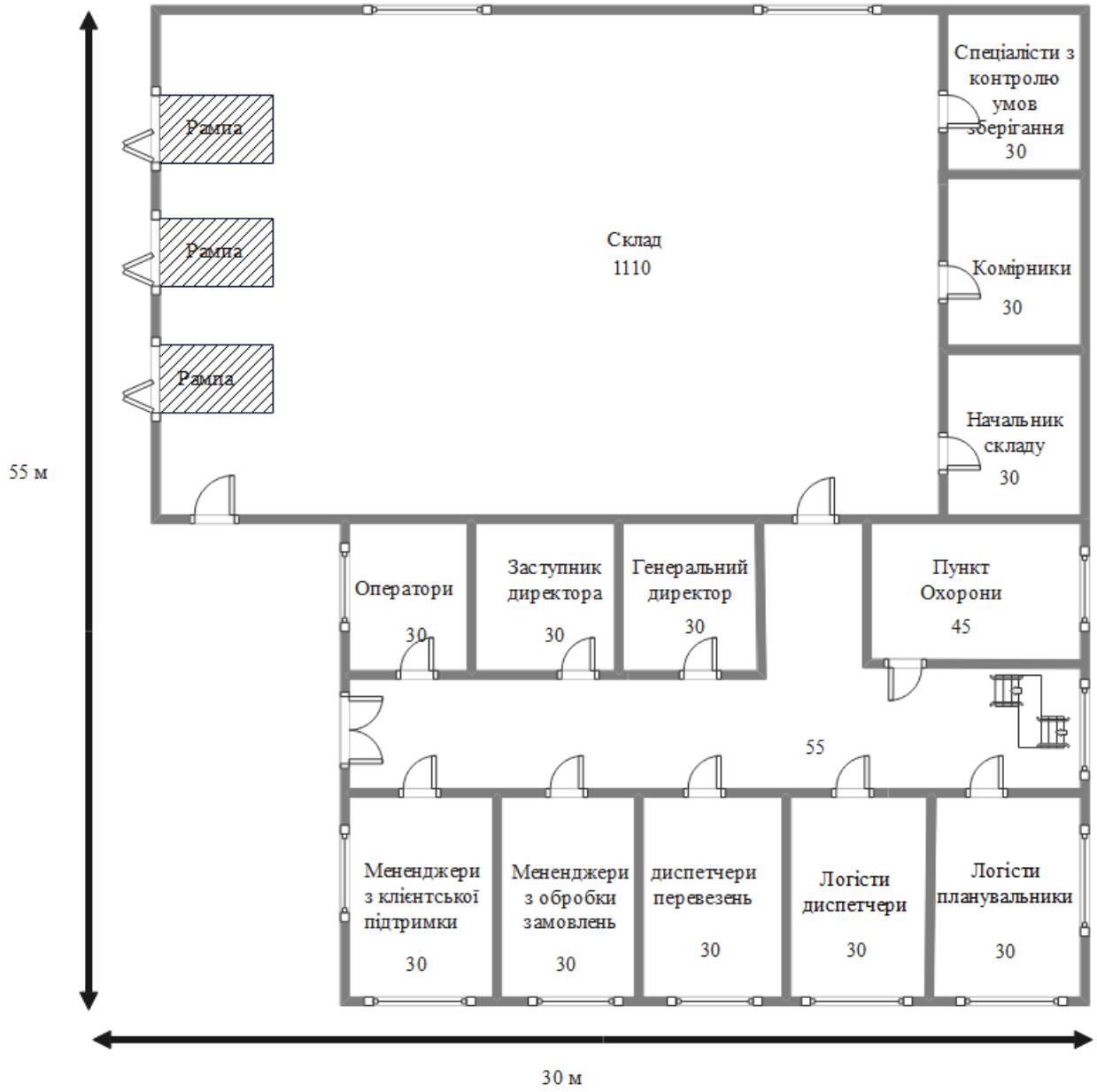


Рисунок 1.3 – План першого поверху логістичної компанії

По розроблену плану на першому поверсі:

– пункт охорони;
– начальник складу;
– головне управління;
– відділ обслуговування клієнтів;
– логістичний відділ;
– склад.

Рисунок 1.4 – План другого поверху логістичної компанії

По розроблену плану на другому поверсі:

– серверна;
– фінансові аналітики;
– економісти;
– бухгалтерія;
– системні адміністратори;
– мережевий інженер;
– спеціалісти з IoT систем;

Інформаційне забезпечення є важливою частиною сучасного логістичного бізнесу, оскільки воно дозволяє забезпечувати безперервну взаємодію між усіма структурними підрозділами, оптимізувати транспортно-складські процеси та ефективно керувати ресурсами. У сучасному ринку від логістичних компаній вимагається максимальна прозорість, точність і оперативність прийняття рішень, що можна досягти лише за допомогою сучасної інформаційної інфраструктури.

1.4 Види сучасних методів побудов комп'ютерних мереж

У комп'ютеризованих логістичних системах, де працюють багато пристроїв, від IoT-сенсорів і серверів до робочих станцій працівників, добре підібрана мережна інфраструктура є життєво важливою. Тип комп'ютерної мережі не обмежується швидкістю обміну даними та надійністю зв'язку; він також впливає на масштабованість, безпеку та гнучкість всієї цифрової системи. У цьому випадку було б розумно розглянути основні види мереж і обґрунтувати вибір найкращої для потреб логістичної компанії.

Найпоширенішим типом мережі в межах одного фізичного об'єкта (наприклад, складу або офісу) є локальна мережа. Всі робочі станції, сервери, принтери, камери відеоспостереження, RFID-сканери та інше обладнання об'єднані в LAN. Передача даних може відбуватися за допомогою Ethernet (кабель) або Wi-Fi (бездротовий зв'язок).

WAN охоплює від кількох будівель до цілих країн. Великі логістичні корпорації, які мають кілька віддалених складів або офісів, використовують такий тип мережі. Використовуються орендовані канали зв'язку або Інтернет для зв'язку. WAN дозволяє проводити аналітику та контроль у центрі, синхронізувати дані між регіональними підрозділами та створювати єдину IT-екосистему на основі ERP. Однак WAN потребує більших заходів безпеки, таких як VPN, фаєрволи та шифрування трафіку, а також більших вимог до резервування каналів.

Персональна мережа, або PAN – це невелика мережа, яка з'єднує пристрої одного користувача в радіусі кількох метрів. Логістика: PAN може підключатися до гарнітури працівника складу, сканера та мобільного терміналу через Bluetooth. Вона

не призначена для перенесення великих обсягів даних, і її значення обмежене.

Виберіть ідеальну архітектуру. Найбільш ефективною для сучасних логістичних компаній з багаторівневою структурою є гібридна модель мережі, яка включає:

- як основа для всіх офісних і складських інформаційних систем, локальна мережа зв'язку (LAN);
- для бездротового доступу в складських приміщеннях з високою швидкістю, Wi-Fi 6/6E з підтримкою MU-MIMO та Mesh-технологіями;
- мережа мережі Інтернету речей, яка використовується для збору телеметрії з сенсорів у режимі реального часу;
- можна використовувати захищену WAN VPN для підключення філій, доступу до ERP та централізованих систем управління;
- LPWAN (LoRaWAN або NB-IoT) призначений для об'єктів, які знаходяться за межами основної інфраструктури, зокрема для контейнерів і мобільного транспорту.

1.5 Постановка завдання

У межах проєкту буде побудована корпоративна комп'ютерна система логістичної компанії з інтеграцією IoT для автоматизації складського комплексу.

У структурі об'єкта ключову роль відіграватиме локальна комп'ютерна мережа (LAN), яка об'єднає сервери, робочі станції, термінали збору даних, принтери етикеток, відеокамери, системи контролю доступу, RFID-зчитувачі та інші пристрої. Передача даних здійснюватиметься через Ethernet Cat6, що гарантує високу швидкість, стабільність і відмовостійкість. Для забезпечення мобільності буде впроваджено бездротову мережу Wi-Fi 6, яка забезпечить стабільне підключення великої кількості пристроїв одночасно.

У межах складського комплексу буде реалізовано окрему IoT-мережу .Для об'єднання центрального складу з віддаленими офісами, транспортними вузлами та підрядниками буде побудовано глобальну мережу (WAN). Вона працюватиме через VPN-тунелі з використанням маршрутизаторів Cisco, що забезпечать захищене

шифрування трафіку, авторизацію користувачів та фільтрацію доступу. Це дозволить уніфікувати логістичну ERP-систему, синхронізувати облік, формувати маршрути доставки та контролювати запаси товарів у реальному часі.

WAN буде побудовано для об’єднання складу з офісами й підрядниками через VPN-з’єднання з використанням маршрутизаторів Cisco. Забезпечуватиметься шифрування, авторизація та фільтрація трафіку.

PAN забезпечить взаємодію між Bluetooth-терміналами, сканерами та гарнітурами комплектувальників.

1.6 Визначення можливих напрямків рішення поставлених завдань

Перш ніж розпочати розробку комп’ютерної системи з інтеграцією Інтернету речей для логістичного підприємства, необхідно визначити основні технологічні напрямки, необхідні для досягнення цілей цифрової трансформації. Основна мета полягає у створенні масштабованої, багаторівневої та захищеної інформаційної інфраструктури. Це дозволить керувати бізнес-процесами, спостерігати за логістичними операціями в режимі реального часу та приймати рішення на основі перевірених даних.

Вибір архітектури локальної обчислювальної мережі (LAN), яка підтримує бездротові технології передачі даних, є важливим напрямком. Враховуючи особливості функціонування логістичного складу та потреби в мобільності IoT-пристроїв, таких як сканери, сенсори, та автоматизовані візки, доцільно реалізувати комбіновану модель. Ця комбінація включає дротову мережу Ethernet для стаціонарних робочих місць і серверного обладнання, а також мережу Wi-Fi або іншу сітчасту бездротову інфраструктуру для рухомих об’єктів і пристроїв у складських зонах.

Розробка IoT-інфраструктури є ще одним важливим напрямком. Це включає в себе установку датчиків температури, вологості, освітленості, руху, RFID-міток. Вкрай важливо, щоб ці апарати були інтегровані в платформу для збору, передачі та аналізу даних. Для цього використовують IoT-шлюзи, контролери та хмарні сервіси для обробки великих кількостей даних.

2. РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ КОМП'ЮТЕРНОЇ СИСТЕМИ

2.1 Технічні вимоги до системи

2.1.1 Найменування та функціональне призначення логістичної компанії

Вимоги до структури і призначення логістичної компанії визначаються її головною метою – забезпечення ефективного управління ланцюгами постачання, обробки замовлень, зберігання, транспортування та взаємодії з клієнтами.

Структура компанії повинна бути організована таким чином, щоб усі елементи логістичного процесу працювали узгоджено, швидко та надійно. У її основі лежить поділ на функціональні підрозділи, кожен з яких виконує чітко визначені завдання.

Складський комплекс є ключовим елементом і відповідає за приймання, зберігання та відвантаження вантажів, контроль за умовами зберігання, інвентаризацію та взаємодію з іншими відділами. Логістичний відділ здійснює планування маршрутів, моніторинг транспорту, диспетчеризацію та оптимізацію доставки. Відділ обслуговування клієнтів забезпечує якісний зворотний зв'язок, прийом запитів і контроль за виконанням замовлень. IT-відділ відповідає за підтримку інформаційної інфраструктури, впровадження цифрових рішень та інтеграцію IoT-технологій. Фінансово-економічний блок здійснює бюджетування, аналітику, контроль витрат і облік. Керівна ланка організовує роботу всієї компанії, приймає стратегічні рішення та координує взаємодію між підрозділами.

Усі підрозділи мають працювати в єдиному цифровому середовищі, що забезпечує централізоване управління даними, аналітику в реальному часі та контроль виконання завдань.

Така структура дозволяє досягти високого рівня гнучкості, адаптивності до ринкових умов і швидкої реакції на зміну потреб клієнтів. Призначення логістичної компанії полягає в ефективній організації переміщення матеріальних потоків, оптимізації витрат, підвищенні якості сервісу та забезпеченні стабільності постачання в межах ланцюга створення цінності.

2.1.2 Вимоги до ключових функціональних характеристик системи

2.1.2.1 Перелік підсистем логістичної компанії та їх призначення

Логістична компанія функціонує на основі взаємодії низки спеціалізованих підсистем, кожна з яких виконує чітко визначені функції в межах загальної інформаційної та операційної структури підприємства. Для забезпечення надійності, безпеки та ефективної роботи всі підсистеми організовані повинні бути реалізовані у вигляді окремих локальних обчислювальних мереж (LAN), що дозволяє розмежувати потоки даних, забезпечити сегментування за функціональними ознаками та оптимізувати роботу цифрової інфраструктури.

LAN 1 призначена для IT-відділу, який виконує критично важливі функції з технічного обслуговування комп’ютерної інфраструктури. У цій підсистемі працюють системні адміністратори, мережеві інженери, фахівці з підтримки та інтеграції IoT-систем. Вони повинні відповідати за налаштування серверного обладнання, моніторинг мережевих вузлів, підтримку безпеки та резервування даних, впровадження нових цифрових рішень, а також тестування та впровадження сенсорних пристроїв, IoT-шлюзів і контролерів. LAN 1 також об'єднує серверну частину компанії, забезпечуючи надійне зберігання та обробку корпоративних даних.

LAN 2 охоплює фінансово-економічний відділ, у якому здійснюються процеси фінансового планування, бухгалтерського обліку, економічного аналізу та підготовки звітності. Ця підсистема повинна включати автоматизовані робочі місця фінансових аналітиків, економістів та бухгалтерів, які використовують спеціалізоване програмне забезпечення для роботи з фінансовими документами, базами даних, електронними звітами та ERP-модулями. LAN 2 має підвищений рівень безпеки доступу, враховуючи конфіденційність фінансової інформації та регуляторні вимоги до обробки персональних і фінансових даних.

LAN 3 об'єднує керівництво компанії та відділ охорони. У керівництва є доступ до стратегічних інструментів управління, включаючи аналітичні панелі, модулі планування, CRM- і ERP-системи, а також системи відеоконференцій для зв’язку з партнерами та замовниками. Водночас відділ охорони повинен

забезпечувати фізичну безпеку об'єкта, контроль доступу на територію підприємства, реагування на надзвичайні ситуації, а також управління сигналізаційними та пожежними системами. Цей сегмент має підвищені вимоги до надійності з’єднання та безперервності доступу.

LAN 4 повинен забезпечувати функціонування логістичного відділу та відділу обслуговування клієнтів. У логістичному відділі працюють диспетчери, логісти-диспетчери та логісти-планувальники, які займаються оперативним управлінням перевезеннями, плануванням маршрутів, оптимізацією доставки та контролем виконання замовлень. У відділі обслуговування клієнтів оператори й менеджери опрацьовують запити клієнтів, надають підтримку, координують процеси виконання замовлень та взаємодіють із клієнтами через CRM-системи. Цей сегмент активно обмінюється даними з ERP та WMS для забезпечення точного й швидкого обслуговування клієнтів.

LAN 5 є наймасштабнішою підсистемою, яка повинна охоплювати складський комплекс і систему Інтернету речей (IoT). Тут реалізована повноцінна цифрова інфраструктура для управління запасами, моніторингу умов зберігання товарів та автоматизації внутрішньо-складських процесів. До LAN 5 підключені сенсори температури, вологості, освітленості, датчики руху, RFID-мітки, сканери штрих-кодів, мобільні термінали збору даних, автоматизовані візки та контролери. Всі ці пристрої інтегруються в єдину систему для фіксації подій у реальному часі, обміну телеметрією, створення аналітичних звітів та взаємодії з WMS і ERP-платформами.

Загалом, поділ логістичної компанії на окремі функціональні підсистеми з власними LAN-сегментами забезпечує високу ефективність, надійність, масштабованість та інформаційну безпеку в умовах сучасного цифрового середовища. Такий підхід дозволяє централізовано керувати ресурсами, мінімізувати ризики, сприяти автоматизації логістичних операцій.

2.1.2.2 Вимоги до способів і засобів зв’язку для інформаційного обміну між компонентами системи

Для ефективного функціонування сучасної логістичної компанії необхідно забезпечити надійні, швидкі та безпечні способи і засоби зв’язку між усіма компонентами інформаційної системи. Обмін даними має відбуватись у режимі реального часу, з урахуванням різних типів навантаження, мобільності пристроїв, вимог до безпеки та масштабованості мережі.

Основною вимогою є побудова багаторівневої мережевої інфраструктури, що включає дротові (Ethernet) та бездротові (Wi-Fi, Bluetooth, LPWAN) засоби комунікації. Для високошвидкісного та стабільного з’єднання між стаціонарними робочими місцями, серверним обладнанням і мережевими сховищами застосовується Gigabit Ethernet або 10 Gigabit Ethernet, що гарантує високу пропускну здатність і низьку затримку при обміні великими обсягами даних. Такі з’єднання використовуються у фінансово-економічному відділі, IT-відділі, відділі керівництва та адміністративних структурах.

Для забезпечення мобільності персоналу в складських зонах, зоні прийому та відправки товарів застосовується бездротова мережа Wi-Fi , що підтримує технології MU-MIMO, OFDMA та Mesh. Це дозволяє підключати велику кількість IoT-пристроїв – сканерів, сенсорів, терміналів збору даних – без втрати якості сигналу, навіть у складних умовах із великою кількістю перешкод і металевих конструкцій. У критично важливих зонах впроваджується резервне підключення через системи або дублюючі точки доступу для уникнення простоїв.

Зв’язок між віддаленими філіями, складами, транспортними засобами та центральною системою забезпечується через захищені канали VPN поверх Інтернету або з використанням орендованих каналів зв’язку (MPLS, SD-WAN). Це дозволяє централізовано керувати логістичними операціями, обмінюватися даними ERP, CRM і WMS у реальному часі та зберігати єдиний цифровий контур компанії.

Для IoT-пристроїв, розміщених за межами основної інфраструктури (наприклад, GPS-трекерів на транспорті, сенсорів у контейнерах), застосовуються технології LPWAN – LoRaWAN або NB-IoT. Вони забезпечують енергоефективний,

довготривалий і стабільний зв’язок на великих відстанях, навіть у складних умовах з обмеженим покриттям.

Також важливу роль відіграють програмні засоби управління трафіком, моніторингу стану мережі, балансування навантаження, а також технології QoS (Quality of Service), які дозволяють пріоритезувати критичні пакети даних. Безпека зв’язку реалізується за допомогою шифрування, автентифікації, фаєрволів, міжмережевих екранів і контролю доступу.

2.1.2.3 Вимоги до взаємодії комп’ютерної системи логістичної компанії із зовнішніми сервісами та суміжними інформаційними системами

У створюваній комп’ютерної системі, яка інтегрується з зовнішніми або внутрішніми суміжними системами, важливим є чітке визначення вимог до характеристик взаємозв’язків. Це включає вимоги до інтерфейсів, протоколів обміну, періодичності передавання даних, характеру інформації, що передається, а також кількісних показників і навантаження, яке система повинна витримувати без втрати стабільності чи цілісності даних.

Інтерфейси мають бути уніфікованими й стандартизованими для забезпечення сумісності із сучасними ERP, WMS, TMS, CRM-системами, транспортними платформами, а також державними інформаційними системами (наприклад, митними або податковими базами даних). Найчастіше використовуються Web-сервіси, а також можливість роботи через формат обміну JSON, XML або CSV.

Протоколи обміну даними повинні забезпечувати надійність, захищеність та підтримку великого обсягу запитів. Найбільш поширеними є HTTPS для безпечного обміну інформацією з зовнішніми системами, wireless для зв’язку з IoT-пристроями, а також FTP/SFTP або WebDAV для передавання файлів між серверами.

Періодичність обміну інформацією залежить від типу даних. Для критично важливих логістичних процесів (наприклад, переміщення вантажів, сканування продукції, контроль температурного режиму на складі) потрібна передача даних у режимі реального часу або з мінімальним інтервалом (1–2 секунди). Для звітності

або синхронізації з бухгалтерськими системами допускається пакетний обмін із періодичністю від 5 хвилин до 1 разу на годину.

Характер даних, якими здійснюється обмін, може бути поділений на структурований (RFID, інформація про замовлення, графіки транспорту) та неструктурований. Структуровані дані передаються через автоматизовані канали, а неструктуровані – через файлові шлюзи або потокове передавання (наприклад, RTSP).

Кількісні показники обміну повинні враховувати масштаби діяльності компанії. Продуктивність системи має забезпечувати обробку щонайменше кількох тисяч транзакцій за годину без втрати продуктивності. Для IoT-зв’язків система повинна обробляти десятки тисяч телеметричних подій на добу. Пропускна здатність інтерфейсів має бути не нижче 100 Мбіт/с для дротових каналів і не нижче 500 Мбіт/с для бездротових внутрішніх обмінів.

2.1.2.4 Вимоги до режимів функціонування комп’ютерної системи

Комп’ютерна система має функціонувати в цілодобовому режимі (24/7). Це обумовлено необхідністю постійного контролю логістичних процесів, безперервного моніторингу складських операцій, а також забезпечення оперативного доступу до інформації для всіх підрозділів компанії незалежно від часу доби.

Однією з критичних причин необхідності цілодобової роботи є постійне живлення RFID-міток, які використовуються для контролю доступу через головний вхід на об'єкт. Система ідентифікації працівників та облік переміщень потребують безперервного функціонування, щоб забезпечити безпеку об’єкта, відслідковувати зміни у складі персоналу та фіксувати події в логах.

Крім того, логістична система повинна постійно відслідковувати стан вантажів на складі, включаючи дані від температурних сенсорів, руху, освітлення та інших IoT-пристроїв. Це важливо для збереження товарів, дотримання умов зберігання та оперативного реагування у випадку відхилень від допустимих значень.

Оскільки будь-яке відключення системи може спричинити збої в обліку, затримки в обробці замовлень або втрату даних, комп’ютерна система повинна передбачити використання безперебійного живлення. Це включає джерела безперебійного живлення (UPS) для ключових вузлів, резервні сервери, мережеве обладнання, а також дизель-генератори або альтернативні джерела енергії у випадку тривалих відключень електропостачання. Наявність таких засобів дозволяє підтримувати працездатність системи у будь-яких позаштатних ситуаціях і забезпечує безперервність бізнес-процесів.

2.1.2.5 Вимоги до меж розвитку та можливостей модернізації системи

Система логістичної компанії повинна передбачати можливість масштабування, зокрема розширення кількості робочих місць у міру зростання обсягів операційної діяльності. Комп’ютерна інфраструктура має бути побудована з урахуванням потенціалу для розвитку: маршрутизатори, комутатори, серверне обладнання й програмне забезпечення повинні підтримувати додаткове навантаження без зниження продуктивності. Це дозволить оперативно інтегрувати нові користувацькі пристрої, а також забезпечити підключення нових відділів чи окремих підрозділів без необхідності суттєвої перебудови мережевої архітектури.

Окрему увагу слід приділити розвитку IoT-інфраструктури. Враховуючи зростання кількості сенсорних пристроїв для контролю за умовами зберігання, переміщенням вантажів, станом обладнання та рівнем заповнення зон, система має бути готова до масштабного впровадження нових IoT-рішень. Архітектура повинна дозволяти підключення нових датчиків та контролерів у реальному часі без зупинки існуючих процесів. Крім того, слід забезпечити підтримку сучасних технологій, таких як LoRaWAN, NB-IoT, Wi-Fi 6/6E та протоколів, здатних ефективно працювати при високій щільності пристроїв.

Інформаційна система має бути відкритою до модульної модернізації, тобто дозволяти оновлення окремих її частин – від сегментів локальної мережі до серверного обладнання – без повного відключення або перезавантаження всієї системи.

2.1.3 Вимоги до показників призначення комп’ютерної системи

Система логістичної компанії має бути призначена для стабільної та ефективної роботи в умовах сучасного складського комплексу з високим рівнем цифровізації. Вона повинна забезпечувати безперервну обробку логістичних, інформаційних і аналітичних процесів із мінімальним втручанням людини. Основними показниками призначення є здатність системи працювати в режимі 24/7, з мінімальними затримками обробки даних (менше 1 секунди для локальних операцій у межах однієї підмережі), підтримка великої кількості одночасно активних пристроїв та сумісність з корпоративними інформаційними платформами (ERP, WMS, CRM, GPS-моніторингом тощо).

Система експлуатується в приміщеннях класу С – це закриті виробничо-складські приміщення з регульованим мікрокліматом, де можливе часткове потрапляння пилу та коливання температури в межах 0…+35 °С. У таких умовах мережеве обладнання, сервери, сенсорні пристрої та комп’ютери мають бути захищені від перегріву, коротких замикань і порушення функцій унаслідок підвищеної вологості. Для цього передбачається встановлення кондиціонерів, систем вентиляції та пожежогасіння.

Для пристроїв, які розташовані ближче до зон відкритого доступу – рамп, доків, технічних воріт – необхідно забезпечити додатковий захист: відповідність IP54 і вище, стійкість до короткочасної дії пилу, протягів, вібрацій і зміни температур. У разі встановлення елементів системи (наприклад, IoT-трекерів, антен або контролерів) на відкритому повітрі, вони повинні відповідати нормам експлуатації в умовах зовнішнього середовища: температурний діапазон –20…+50 °С, вологість до 90%, захист корпусу щонайменше IP65.

Усі компоненти системи мають бути надійними в умовах постійної експлуатації та підтримувати централізоване резервне живлення, щоб уникнути втрати даних або переривання функціонування при аварійних ситуаціях, перебоях електропостачання або перевантаженнях.

2.1.4 Додаткові вимоги

2.1.4.1 Вимоги до експлуатації системи в серверному приміщенні

Серверна кімната виконує критично важливу функцію – забезпечує зберігання, обробку та передачу великого обсягу даних. У зв’язку з цим до умов її експлуатації висуваються особливі вимоги щодо мікроклімату, енергозабезпечення та безпеки.

Приміщення має бути окремим, із контролем доступу, охоронною сигналізацією та відеоспостереженням. Температурний режим повинен підтримуватися в межах +18…+24 °C з допустимим рівнем вологості до 50%. Обов’язкове встановлення кондиціонерів із резервуванням, вентиляційної системи з фільтрацією повітря, а також безперебійного живлення з джерелами UPS та можливістю автоматичного перемикання на генератор.

2.1.4.2 Вимоги до експлуатації системи в умовах складського середовища

Щодо складських приміщень, то тут умови експлуатації є менш контрольованими, але не менш важливими. У зонах приймання, зберігання та відправлення товару спостерігається підвищений рівень запиленості, вібрацій, зміни температур (особливо при відкритті воріт), можливе потрапляння вологи або перепади освітлення. У зв’язку з цим усі IoT-пристрої, такі як RFID-зчитувачі, датчики температури, вологості, руху, а також комунікаційне обладнання (маршрутизатори, точки доступу Wi-Fi) мають бути захищені від механічного впливу, пилу та бризок згідно стандарту не нижче IP54, а для зовнішнього або вуличного використання – IP65.

Додатково необхідно забезпечити антивандальний захист обладнання, що розташовується на рівні доступу персоналу або у відкритих зонах. В умовах високої інтенсивності роботи на складі вся система повинна бути максимально надійною, працювати в реальному часі та витримувати великі навантаження з боку пристроїв і користувачів.

2.2 Розробка інженерних рішень для реалізації комп’ютерної системи

2.2.1 Розробка структурної схеми технічних засобів комп’ютерної системи, відповідно до топологічних характеристик об’єкта

Розробка структурної схеми комп’ютерної системи є важливим етапом проектування локальної обчислювальної мережі логістичного підприємства. Оскільки об’єкт має чітку функціональну зональність з виробничо-логістичними та адміністративними приміщеннями на першому поверсі, ієрархічна багаторівнева структура з центральною комутацією є оптимальною. Це дозволяє об’єднати мережеву інфраструктуру в один керований простір, зберігаючи високу масштабованість і безпеку, а також гнучке розмежування трафіку.

Така структура має класичну трирівневу модель, яка складається з ядра мережі (core layer), рівня розподілу (distribution layer) і рівня доступу. На другому поверсі знаходиться серверна кімната, де встановлюється високопродуктивний маршрутизатор або L3-комутатор, де знаходиться ядро мережі.

Міжповерхова магістраль використовує оптоволоконний канал, який забезпечує високу пропускну здатність і мінімальні затримки передачі даних. Усередині магістралі використовується кабель категорії Cat6a. Керовані PoE-комутатори з підтримкою резервування каналів і віддаленого управління є активним обладнанням, яке дозволяє живити пристрої спостереження, точки доступу та сенсори Інтернету речей без додаткової інфраструктури.

Таким чином, запропонована структурна схема відповідає як просторовим особливостям об’єкта, так і сучасним вимогам до гнучкості, масштабованості, керованості та безпеки корпоративних комп’ютерних мереж. Вона гарантує безпеку інформаційного середовища, високу доступність послуг і централізоване керування всіма компонентами системи.

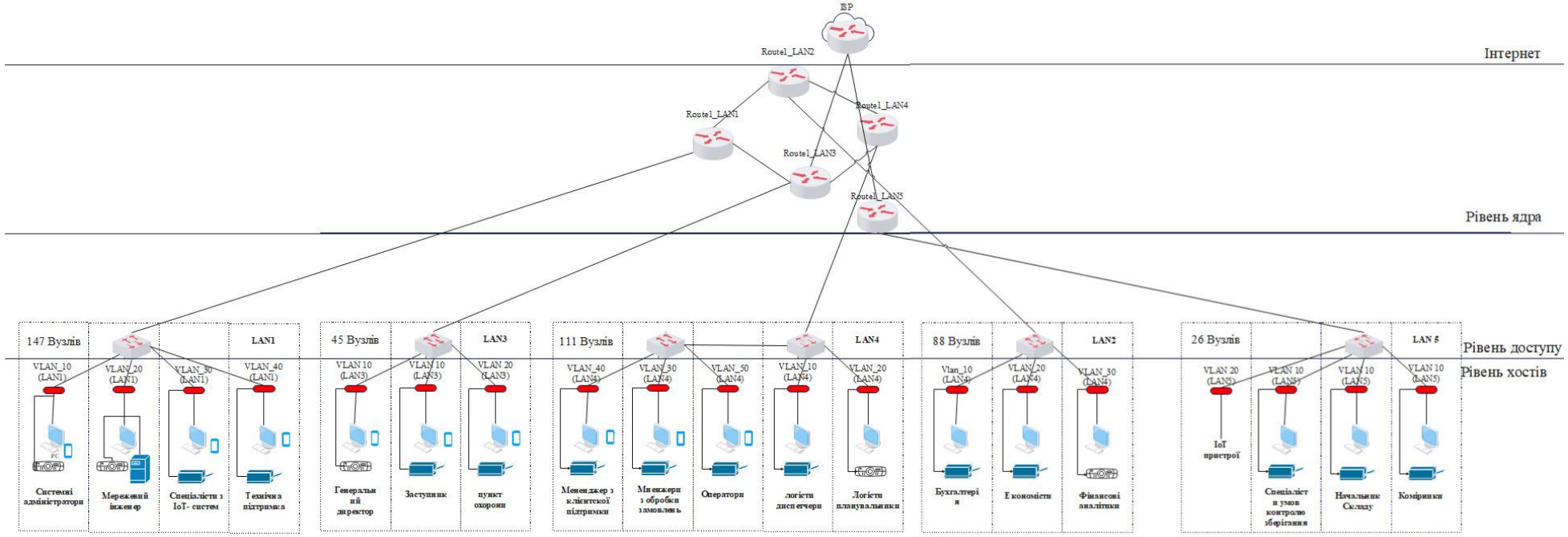


Рисунок 2.1 – Структурна схема комплексу технічних засобів комп’ютерної системи

2.2.2 Складання технічної специфікації апаратних засобів комп'ютерної системи

Розробка комп'ютерної системи для логістичного підприємства передбачає чітке розташування мережевої інфраструктури, щоб розподілити персонал відповідно до їхніх функціональних обов'язків і забезпечити ефективне використання апаратних ресурсів. Для досягнення цього було створено п'ять логічно ізольованих локальних мережевих сегментів (LAN), які об'єднують робочі місця відповідно до їх професійної приналежності та типу навантаження на мережу.

Підрозділ складу включає вісім робочих місць у LAN 1. Сюди входять начальники складу, фахівці з контролю умов зберігання, комірники, а також різноманітні пристрої Інтернету речей, такі як датчики безпеки, камери відеоспостереження, переміщення вантажів, температури та вологості. Ця мережа потребує використання комутаторів із пріоритетом трафіку (QoS) і підтримкою VLAN, щоб надійно відокремити трафік Інтернету речей від робочого місця, забезпечуючи стабільну взаємодію з сенсорами в реальному часі.

LAN 2 має чотири користувача: пункт охорони, генерального директора та його заступника. Інформаційна безпека та конфіденційність цього сектора надзвичайно важливі, тому він обладнаний комутаторами, які підтримують протоколи шифрування, доступ через захищені VLAN і резервні канали зв'язку. Крім того, це включає обладнання для відеоспостереження та контролю доступу.

У LAN 3 є дев'ять комп'ютерів, призначених для операторів, менеджерів з обробки замовлень і менеджерів з клієнтської підтримки. У цьому випадку швидкий обмін даними з телефонними шлюзами, базами замовлень і CRM-системами є життєво важливим, щоб забезпечити стабільність мережі з мінімальною затримкою. Комутатори цього підрозділу забезпечують функції моніторингу продуктивності та керування навантаженням.

Найбільший LAN 5 містить сімнадцять комп'ютерів. Бухгалтерія, економіка, фінансові аналітики та IT-персонал – системні адміністратори, мережеві інженери, спеціалісти з Інтернету речей, технічна підтримка та інші – складають цю мережу. Всі сервери підприємства, включаючи файлові, поштові, базові та сервери

CRM/ERP, а також сервери IoT-моніторингу, розташовані тут. Комутатори цього сегмента пропонують найбільшу кількість функцій, включаючи підтримку VLAN, SNMP, резервне живлення, масштабування, інтелектуальний аналіз трафіку та підтримку агрегації каналів.

Маршрутизатор Cisco 2911/K9 обраний як головний маршрутизатор через свій збалансований набір функцій. Він підтримує сервіси безпеки (VPN, брандмауер), голосові сервіси, має високу продуктивність і масштабованість, необхідну для централізованого управління мережею. У порівнянні з менш потужними моделями, як-от Cisco 881 або 1941, він має кращу обробку трафіку та більше слотів для модулів розширення. З іншого боку, сучасні ISR 4000 серії (наприклад, 4331) пропонують ще вищу продуктивність, але вартість і надлишкова потужність роблять їх не доцільними для даної інфраструктури.

Комутатори Cisco WS-C2960-24TT-L вибрані як робочі комутатори рівня доступу. Вони забезпечують підтримку VLAN, базову безпеку, QoS та моніторинг – все, що потрібно для LAN-сегментів офісів, складів і сервісних зон. У порівнянні з більш функціональними Cisco 3560 або 3750 (які підтримують Layer 3), ці комутатори простіші та дешевші, але й менш складні в обслуговуванні. Якщо ж брати нові серії, як Cisco Catalyst 9200 або 9300, то вони мають розширені можливості (DNA Center, TrustSec, StackPower), але ці можливості не використовуються в цій мережі, а вартість їх значно вища. 2960 – це перевірене рішення для базового рівня, яке ідеально вписується у поточні потреби.

Точки доступу Cisco Aironet 1042 (AIR-AP1042-NK9-5) встановлені для забезпечення стабільного бездротового зв’язку. Вони підтримують стандарт 802.11n, працюють з технологією MIMO і розраховані на промислові умови з нормальною щільністю пристроїв. Якщо порівнювати з новішими точками доступу серій 2800 або 9100 (802.11ac Wave 2 і Wi-Fi 6), то вони безперечно продуктивніші, мають більшу пропускну здатність і підтримку сучасних протоколів. Але для складу, де головні клієнти – термінали збору даних, сканери та планшети, Aironet 1042 справляється без проблем.

Промисловий маршрутизатор Cisco IG20R Rugged Series використовується у складських умовах та працюють різноманітні IoT-пристрої. У порівнянні з класичними маршрутизаторами ISR або навіть зовнішніми LTE-шлюзами, серія IG - це рішення, яке фізично розраховане на важкі умови. Він підтримує протоколи, які потрібні саме для IoT – MQTT, IPSec, HTTPS – і забезпечує безпечний зв'язок із сенсорами, автоматизованими візками, RFID. Альтернативи типу Cisco IR1101 або IR829 могли б підійти, але IG20R має простішу архітектуру, меншу вартість і легшу інтеграцію, що робить його ідеальним вибором під конкретні завдання в цій мережі.

Таблиця 2.1 – Специфікація обладнання системи

№	Обладнання	Модель / Артикул	Кількість	Функціональне призначення
1	Ядровий маршрутизатор з багатопортовою підтримкою 3x Gigabit Ethernet, розширення EHWIC, підтримка DSP та ISM, базовий IP-набір	Cisco 2911/K9	6	Основне мережеве ядро для кожного поверху (1 пристрій на поверх)
2	Комутатор доступу 2-го рівня 24x Fast Ethernet портів + 2x Gigabit uplink	Cisco WS-C2960-24TT-L	13	Розміщення у функціональних LAN (1-4), розподілення по приміщеннях
3	Бездротова точка доступу Wi-Fi 802.11n 2x2 MIMO, підтримка a/b/g/n, автономний режим	Cisco Aironet 1042 (AIR-AP1042-NK9-5)	3	Покриття офісної і складської зон бездротовим доступом
4	Сервер для веб-додатків і сайту Intel Xeon Silver 4210, 32 ГБ RAM, 2x480 ГБ SSD, RAID 1	Dell PowerEdge R240	1	Розміщення сайту компанії, внутрішніх веб-сервісів
5	DNS та IoT сервер Xeon Silver 4210, 16 ГБ RAM, SSD 480 ГБ	Dell PowerEdge T140	1	Відповідальний за адресацію та інтеграцію IoT-пристроїв
6	Сервер DHCP Core i5, 8 ГБ оперативної пам'яті, SSD 256 ГБ	HP ProDesk 400 G6	1	Автоматична видача IP-адрес для внутрішньої мережі
7	Промисловий шлюз для IoT з підтримкою LTE 2x Ethernet, GNSS, захищений корпус, монтування на DIN-рейку	Cisco IG20R Rugged Series	1	Передача даних від IoT-пристроїв через мобільну мережу 4G

Для визначення витрат на підключення комп’ютерної системи для всього другого поверху була створена схема структурованої кабельної мережі (СКМ). Вона забезпечує точне планування розміщення всіх ключових мережевих елементів і дозволяє точно розрахувати необхідну кількість обладнання, а також довжину кабельних ліній. Така схема є важливим інструментом для ефективного проектування і подальшого монтажу мережевої інфраструктури.

Рисунок 2.2 – Схема розміщення кабельних мереж для другого поверху

Для побудови надійної та ефективної мережевої інфраструктури логістичної компанії було ретельно підібрано ключові елементи, що забезпечують якісний зв’язок, стабільне живлення та безпеку обладнання.

Розетка комп’ютерна подвійна RJ45 Cat6 (Legrand).Обрана розетка відповідає категорії Cat6 та забезпечує швидкість передачі даних до 1 Гбіт/с. Подвійне гніздо дає змогу підключення двох мережевих пристроїв, що підвищує функціональність робочого місця. Продукція компанії Legrand відзначається

високою якістю збірки, надійністю контактних груп та довговічністю в експлуатації. Schneider Electric (вища вартість за аналогічної якості), китайські ноунейм-виробники (нижча ціна, проте ненадійна якість контактів і матеріалів).

LAN-кабель Ethernet Cat6 RJ45 (Belkin).Кабель типу UTP категорії 6 забезпечує швидку та стабільну передачу даних на швидкості до 1 Гбіт/с. Бренд Belkin є визнаним виробником у галузі мережевого обладнання, що гарантує відповідність стандартам якості та електричних характеристик.

Аналоги: Digitus, Viko – аналогічні за характеристиками, проте з незначними коливаннями якості оболонки; дешеві китайські моделі можуть не відповідати заявленій категорії та мати низький коефіцієнт крученості пар.

Розетка подвійна вологозахищена IP44 (Legrand).Ця розетка забезпечує захист від вологи та пилу згідно зі стандартом IP44, що дозволяє її використання у вологих або запилених приміщеннях. Виріб Legrand характеризується надійною конструкцією, стійкістю до зношування та герметичністю.Аналог ABB та Schneider Electric пропонують якісні рішення у вищому ціновому сегменті; дешеві моделі мають послаблену герметичність та погану фіксацію кришки.

Кабель живлення мідний ПВС 3×1.5 мм² (Prysmian).ВС-кабель із трьома жилами перерізом 1.5 мм² використовується для електроживлення офісного обладнання. Мідна жила забезпечує гнучкість, надійність та стійкість до механічних навантажень. Prysmian – європейський виробник із бездоганною репутацією. Аналог «Одесакабель» – український бренд хорошої якості, маловідомі виробники можуть використовувати менший переріз жили при збереженні маркування.

Кабельний канал 40×25 мм (Legrand).Використовується для організованого та безпечного прокладання сигнальних (мережевих) кабелів. Розмір 40×25 мм є оптимальним для невеликих груп кабелів. Продукція Legrand має високу міцність, зручність монтажу, не втрачає колір під впливом світла. Аналог Kopos (менш міцна кришка), IEK (нижча естетика, менша товщина стінок).

Кабельний канал 60×40 мм (Legrand).Призначений для прокладання силових кабелів. Такий розмір дозволяє зручно організувати електроживлення без перевантаження внутрішнього простору. Legrand гарантує відповідність

вогнестійким та екологічним нормам. Аналог Schneider Electric – якісний, але дорожчий; IEK – дешевший варіант, проте з меншою міцністю.

Мережевий патч-корд RJ45 Cat.6A, 1 м (Legrand).Використовується для з’єднання комп’ютерів, комутаторів та іншого обладнання з мережею. Cat.6A забезпечує передачу даних до 10 Гбіт/с на коротких відстанях. Legrand гарантує точність виготовлення конекторів та відповідність специфікаціям. Аналог D-Link, Digitus – аналогічна якість, часто вищі ціни; безіменні патч-корди – високий ризик переривання сигналу через неякісні роз’єми.

Таблиця 2.2 – Специфікація кабельної мережі

№	Найменування і технічна характеристика	Тип, марка, позначення	Одиниця виміру	Кількість	Примітки
1	Розетка комп’ютерна подвійна RJ45 Cat6	Розетка подвійна Legrand Cat6	шт		Для монтажу в стандартну коробку
2	LAN-кабель Ethernet Cat6 RJ45	Кабель UTP Cat6 Belkin	пог. м		Для швидкості до 1 Гбіт/с
3	Розетка подвійна вологозахищена IP44	Вологозахищена розетка Legrand IP44	шт		Захист від вологи і пилу
4	Кабель живлення мідний ПВС 3*1.5 мм²	Кабель ПВС 3x1.5 мм² Prysmian	пог. м		Гнучкий, для живлення обладнання
5	Кабельний канал 40x25	Кабельний канал Legrand 40x25	пог. м		Пластиковий, для захисту кабелів
6	Кабельний канал для захисту кабелю живлення 60x40	Кабельний канал Legrand 60x40	пог. м		Для прокладання кабелів живлення
7	Мережевий патч-корд RJ45 Cat.6A, 1м	Патч-корд RJ45 Cat.6A Legrand, 1 м	шт		Для з’єднання обладнання з мережею

3. ПРОЕКТУВАННЯ КОРПОРАТИВНОЇ МЕРЕЖІ

3.1 Розробка схеми адресації корпоративної мережі

Для того, щоб побудувати ефективну, масштабовану та безпечну мережеву інфраструктуру компанії, було розроблено ідею логічного розділення корпоративної мережі на декілька незалежних локальних мереж (LAN) сегментів відповідно до діяльності компанії. Механізм VLAN використовується в кожному LAN для подальшої логічної ізоляції користувачів і послуг.

Використання VLAN дозволяє запроваджувати політики доступу та пріоритетності передачі даних, збільшувати безпеку та оптимізувати управління мережею. Крім того, ця схема дозволяє централізовано керувати доступом до ресурсів, відокремлювати проблемні частини та швидко адаптувати мережу до змін у структурі компанії.

Таблиця 3.1 – Кількість вузлів в підмережах

LAN 1	LAN 2	LAN 3	LAN 4	LAN 5
147	88	45	111	26

LAN 1 – IT-відділ: тут розміщуються всі IT-фахівці, які відповідають за технічне обслуговування, безперебійну роботу обладнання, адміністрування систем і підтримку інфраструктури Інтернету речей. У зв’язку з високими вимогами до безпеки та контрольованості трафіку було вирішено розділити VLAN на окремі групи:

– VLAN 10 – Системні адміністратори: ця підмережа включає адміністраторів резервного копіювання, сховищ, доменів і серверів. Вони мають повний доступ до мережевої інфраструктури та систем, які є життєво важливими.
– VLAN 20 – мережевий інженер, який контролює, підтримує та налаштовує комутатори, маршрутизатори, Wi-Fi-точки та міжмережеві екрани. Для того, щоб зменшити вплив зовнішніх факторів, його мережеве середовище ізольоване.

- VLAN 30 – Спеціалісти з IoT-систем працюють зі шлюзами, датчиками, автоматизацією та промисловим обладнанням. Політики QoS і безпеки для їхніх VLAN різні.
- VLAN 40 – Технічна підтримка. Включає співробітників, що займаються обробкою внутрішніх звернень, виїзним обслуговуванням обладнання та допомогою користувачам. Їхній трафік сегментовано для відокремлення від адміністративного.

LAN 2 – Фінансово-економічний відділ, ведення бухгалтерії, розрахунки, економічний аналіз і звітність належать до фінансового відділу LAN 2. Кожна функція передана в окремий VLAN, оскільки безпека фінансових даних є надзвичайно важливою:

- VLAN 10 – Бухгалтерія : підтримує бухгалтерські програми, фінансові системи та банківське обслуговування, а також має доступ до конфіденційних фінансових документів.
- VLAN 20 – Економісти . Аналізують економічні показники, роблять прогнози та планують гроші. Їм неможливо отримати доступ до необхідних джерел даних.
- VLAN 30 – аналітики фінансів. Часто використовують зовнішні джерела, коли працюють з великими кількостями даних. Під час обробки звітів і аналітичних запитів пріоритетом має бути трафік VLAN.

LAN 3 – Управління та безпека. Відповідальність за підключення адміністративного апарату та служб безпеки лежить на цьому LAN:

- VLAN 10 – Керівництво: Генеральний директор, заступники та адміністративний персонал мають доступ до управлінських систем, конфіденційної звітності та внутрішніх і зовнішніх комунікацій.

– VLAN 20 – Охорона: Управління системами відеоспостереження, системами доступу та засобами моніторингу та сигналізації. Стабільність і доступність з’єднання надзвичайно важливі.

LAN 4 – Логістика та підтримка клієнтів. Відділи, які працюють з клієнтами, планують перевезення та контролюють замовлення, можуть використовувати цей сегмент:

– VLAN 10 – диспетчери логістики. Відповідають за планування маршрутів і перевезень, а також співпрацюють із транспортними компаніями;
– VLAN 20 для планувальників логістики. Розробляють логістичні плани та розраховують ефективність доставки;
– VLAN 30: Менеджери з клієнтської підтримки працюють із системами CRM і надають клієнтам технічну або консультаційну допомогу;
– VLAN 40: менеджери замовлень. Приймають, перевіряють і виконують замовлення клієнтів;
– VLAN 50 для операторів. Роблять запити та документацію, працюють із базами даних товарів.

LAN 5 – складський комплекс і Інтернет речей
У найновішому LAN об’єднані всі складські системи та пристрої Інтернету речей. Автоматизація процесів зберігання, контроль навколишнього середовища та забезпечення безперервної роботи – головні завдання цього відділу.

– VLAN 10 – персонал складу. Комірники, контролери зберігання та начальник складу Системи включають облік, програмне забезпечення для обліку та відстеження переміщення товарів.
– VLAN 20 – Пристрої IoT включають RFID-зчитувачі, автоматизовані ворота та шлюзи, датчики температури, вологості та освітлення.

ISP та зовнішній трафік. Для організації доступу до Інтернету використовується окрема маршрутизована зона, яка поєднується з міжмережевим екраном. Правила доступу та NAT ізолюють ISP-з’єднання від внутрішніх сегментів.

У зоні DMZ можна розмістити публічні ресурси, такі як веб-сервери, FTP та поштові шлюзи.

Таблиця 3.2 – Схема адресації мережі комп’ютерної системи

Назва мережі	Роз-мір	IP-адреса	Маска	Початкове значення діапазону можливих адрес вузлів у підмережі	Початкове значення діапазону можливих адрес вузлів у підмережі
LAN_1	147	172.25.16.0	/24	172.25.16.1	172.25.16.254
Vlan10 (Lan 1)	64	172.25.16.0	/26	172.25.16.1	172.25.16.62
Vlan20 (Lan 1)	64	172.25.16.64	/26	172.25.16.65	172.25.16.127
Vlan30 (Lan 1)	64	172.25.16.128	/26	172.25.16.129	172.25.16.183
Vlan40 (Lan 1)	16	172.25.16.192	/28	172.25.16.193	172.25.16.208
LAN_2	88	172.25.15.0	/25	172.25.15.1	172.25.16.126
Vlan 10 (Lan 2)	32	172.25.15.0	/27	172.25.15.1	172.25.15.30
Vlan 20 (Lan 2)	32	172.25.15.32	/27	172.25.15.33	172.25.15.62
Vlan 30 (Lan 2)	32	172.25.15.64	/27	172.25.15.65	172.25.15.94
LAN_3	45	172.25.14.0	/26	172.25.14.1	172.25.14.62
Vlan 10 (Lan3)	32	172.25.14.0	/27	172.25.14.1	172.25.14.30
Vlan 20 (Lan3)	32	172.25.14.32	/27	172.25.14.33	172.25.14.62
LAN_4	111	172.25.14.0	/24	172.25.14.1	172.25.14.254
Vlan 10 (Lan4)	32	172.25.13.0	/27	172.25.13.1	172.25.13.30
Vlan 20 (Lan4)	32	172.25.13.32	/27	172.25.13.33	172.25.13.62
Vlan 30 (Lan4)	32	172.25.13.64	/27	172.25.13.65	172.25.13.95
Vlan 40 (Lan4)	32	172.25.13.96	/27	172.25.13.97	172.25.13.126
Vlan 50 (Lan4)	32	172.25.13.128	/27	172.25.13.129	172.25.13.158
LAN_5	26	172.25.12.0	/26	172.25.12.1	172.25.12.62
Vlan 10 (Lan5)	32	172.25.12.0	/27	172.25.12.1	172.25.12.30
Vlan 20 (Lan5)	32	172.25.12.32	/27	172.25.12.33	172.25.12.62
ISP	256	30.25.16.0	/24	30.25.16.1	30.25.16.254
WAN 1	4	10.25.16.4	/30	10.25.16.5	10.25.16.6
WAN 2	4	10.25.16.20	/30	10.25.16.21	10.25.16.22
WAN 3	4	10.25.16.28	/30	10.25.16.29	10.25.16.30
WAN 4	4	10.25.16.32	/30	10.25.16.33	10.25.16.34

Закінчення таблиці 3.2

WAN 5	4	10.25.16.24	/30	10.25.16.25	10.25.16.26
WAN 6	4	10.25.16.52	/30	10.25.16.53	10.25.16.54
WAN 7	4	10.25.16.60	/30	10.25.16.61	10.25.16.62

Після розробки схеми адресації вся мережа компанії була логічно поділена на окремі сегменти відповідно до внутрішньої структури компанії. VLAN об’єднують функціональні підрозділи в кожному LAN. Такий підхід забезпечує гнучкість у масштабуванні, контроль доступу, підвищення безпеки та ефективне керування трафіком. Мережеве розмежування зменшує ризик конфліктів, полегшує управління та прискорює обробку запитів. Кожен VLAN має свій власний діапазон IP-адрес для розширення. Це дозволяє підтримувати високу продуктивність мережі та централізовано керувати ресурсами.

Таблиця 3.3 – Схема адресації мережі комп’ютерної системи

Пристрій	Інтерфейс	IP-адреса	Маска	шлюз	VLAN	Інтерфейс
1	2	3	4	5	6	7
LAN1 – IT Відділ						
Router1- Lan1	S0/1/0	10.25.16.5	/4	-	-	S0/1/0
	S0/1/1	10.25.16.29	/4	-	-	S0/1/0
	S0/2/0	10.25.16.21	/4	-	-	S0/2/0
	G0/0.10	172.25.16.0	/26	172.25.16.1	10(L1)	G0/1
	G0/0.20	172.25.16.64	/26	172.25.16.65	20(L1)	G0/1
	G0/0.30	172.25.16.128	/26	172.25.16.129	30(L1)	G0/1
	G0/0.40	172.25.16.192	/28	172.25.16.193	40(L1)	G0/1
Sw1_LAN1	Vlan 30	172.25.16.128	/26	172.25.16.129	30(L1)	Fa0/1-10
	Vlan 40	172.25.16.192	/26	172.25.16.193	40(L1)	Fa0/11-15
Sw2_ LAN1	Vlan 20	172.25.16.64	/26	172.25.16.65	20(L1)	Fa0/1-10
Sw3_ LAN1	Vlan 10	172.25.16.0	/26	172.25.16.1	10(L1)	Fa0/1-10
PC1-2	NIC	172.25.16.197-198	/28	172.25.45.193	40 (L1)	Fa0/11-12

Продовження таблиці 3.3

PC3-5	NIC	172.25.16.135-137	/26	172.25.45.129	30 (L1)	Fa0/1-3
PC6-8	NIC	172.25.16.71-73	/26	172.25.45.65	20 (L1)	Fa0/1-3
PC9	NIC	172.25.16.6	/26	172.25.45.1	10 (L1)	Fa0/3
Servers	NIC	172.25.16.2-4	/26	172.25.45.1	10 (L1)	Fa0/1-4
LAN2 – Фінансово економічний відділ						
Router1- LAN2	S0/1/0	10.25.16.6	/4	-	-	S0/1/1
	S0/1/1	10.25.16.34	/4	-	-	S0/1/0
	S0/2/0	10.25.16.25	/4	-	-	S0/2/0
	G0/0.10	172.25.15.0	/27	172.25.16.1	10(L2)	Fa0/24
	G0/0.20	172.25.15.32	/27	172.25.15.33	20(L2)	Fa0/24
	G0/0.30	172.25.15.64	/27	172.25.15.65	30(L2)	Fa0/24
Sw1_LAN2	Vlan 30	172.25.15.65	/27	172.25.16.164	30(L2)	Fa0/1-10
Sw2_ LAN2	Vlan 20	172.25.15.32	/27	172.25.16.33	20(L2)	Fa0/1-10
	Vlan 10	172.25.15.0	/27	172.25.15.1	10(L2)	Fa0/11-15
PC1-3	NIC	172.25.15.71-73	/27	172.25.15.65	30(L2)	Fa0/1-3
PC4-6	NIC	172.25.15.38-40	/27	172.25.15.33	20(L2)	Fa0/1-3
PC7-9	NIC	172.25.15.6-8	/27	172.25.15.1	10(L2)	Fa0/11-13
LAN3 – Управління та безпека						
Router1- LAN3	S0/1/0	10.25.16.53	/4	-	-	S0/1/1
	S0/1/1	10.25.16.30	/4	-	-	S0/1/0
	S0/2/0	10.25.16.33	/4	-	-	S0/2/0
	S0/2/1	10.25.16.62	/4	-	-	S0/2/1
	G0/0.10	172.25.14.0	/27	172.25.14.1	10(L3)	G0/1
	G0/0.20	172.25.14.32	/27	172.25.14.65	20(L3)	G0/1
Sw2_LAN3	Vlan 10	172.25.14.0	/27	172.25.14.1	10(L3)	Fa0/1-10
Sw3_LAN3	Vlan 20	172.25.14.32	/27	172.25.15.33	20(L3)	Fa0/1-10
PC1-3	NIC	172.25.14.71-73	/27	172.25.14.65	30(L3)	Fa0/1-3
PC4-6	NIC	172.25.14.38-40	/27	172.25.14.33	20(L3)	Fa0/1-3
PC7-9	NIC	172.25.14.6-8	/27	172.25.14.1	10(L3)	Fa0/11-13

Закінчення таблиці 3.3

LAN4 – Логістика та підтримка клієнтів						
Router1- LAN4	S0/1/0	10.25.16.54	/4	-	-	S0/1/1
	S0/1/1	10.25.16.25	/4	-	-	S0/1/0
	S0/2/0	10.25.16.22	/4	-	-	S0/2/0
	G0/0.10	172.25.13.0	/27	172.25.13.1	10(L4)	G0/2
	G0/0.20	172.25.13.32	/27	172.25.13.33	20(L4)	G0/2
	G0/0.30	172.25.13.64	/27	172.25.13.65	30(L4)	G0/2
	G0/0.40	172.25.13.96	/27	172.25.13.97	40(L4)	G0/2
	G0/0.50	172.25.13.128	/27	172.25.13.69	50(L4)	G0/2
Sw1_LAN4	Vlan 30	172.25.13.64	/27	172.25.13.65	30(L4)	Fa0/1-5
	Vlan 40	172.25.13.96	/27	172.25.13.97	40(L4)	Fa0/6-10
	Vlan 50	172.25.13.128	/27	172.25.13.129	30(L4)	Fa0/11-15
Sw2_LAN4	Vlan 10	172.25.13.0	/27	172.25.13.1	20(L4)	Fa0/1-10
	Vlan 20	172.25.13.64	/27	172.25.13.65	20(L4)	Fa0/11-15
PC1	Vlan 50	172.25.13.135-138	/27	172.25.13.129	50(L4)	Fa0/11
PC2-4	Vlan 30	172.25.13.70-72	/27	172.25.13.65	30(L4)	Fa0/1-3
PC5-7	Vlan 40	172.25.13.102-104	/27	172.25.13.97	40(L4)	Fa0/5-7
PC8-10	Vlan 10	172.25.13.6-8	/27	172.25.13.1	10(L4)	Fa0/1-3
PC11-13	Vlan 20	172.25.13.38-40	/27	172.25.13.33	10(L4)	Fa0/10-12
LAN5 – Логістика та IoT						
Router1- LAN5	S0/2/1	10.25.16.61	/4	-	-	S0/2/1
	G0/0.10	172.25.14.0	/27	172.25.14.1	10(L5)	G0/1
	G0/0.20	172.25.14.32	/27	172.25.14.65	20(L5)	G0/1
Sw1_LAN5	Vlan 10	172.25.12.0	/27	172.25.14.1	10(L5)	Fa0/1-10
	Vlan 20	172.25.12.32	/27	172.25.14.33	10(L5)	Fa0/11-15
Sw2_LAN5	Vlan 10	172.25.12.0	/27	172.25.15.1	20(L5)	Fa0/1-10
PC1-6	Vlan 10	172.25.12.0	/27	172.25.15.1	20(L5)	Fa0/1-10
IoT	Vlan 20	172.25.12.38	/27	172.25.15.32	10(L5)	Fa0/11-15

3.1.2 Розробка топологічної схеми корпоративної мережі

Ієрархічна модель, яка включає рівні доступу, розподілу та ядра, вже використовується для реалізації топологічної схеми корпоративної мережі. У центрі мережі встановлений основний маршрутизатор, а розподільчі комутатори об’єднують локальні сегменти кожного функціонального підрозділу компанії. Кожен із п’яти LAN-сегментів має власні керовані комутатори рівня доступу, які гарантують швидку та стабільну взаємодію між пристроями.

Використання VLAN у кожному LAN дозволяє розподіляти трафік між різними підрозділами, такими як IT-відділ, фінанси, керівництво, логістика, служба підтримки та складський комплекс. Це підвищує безпеку та продуктивність мережевих ресурсів.

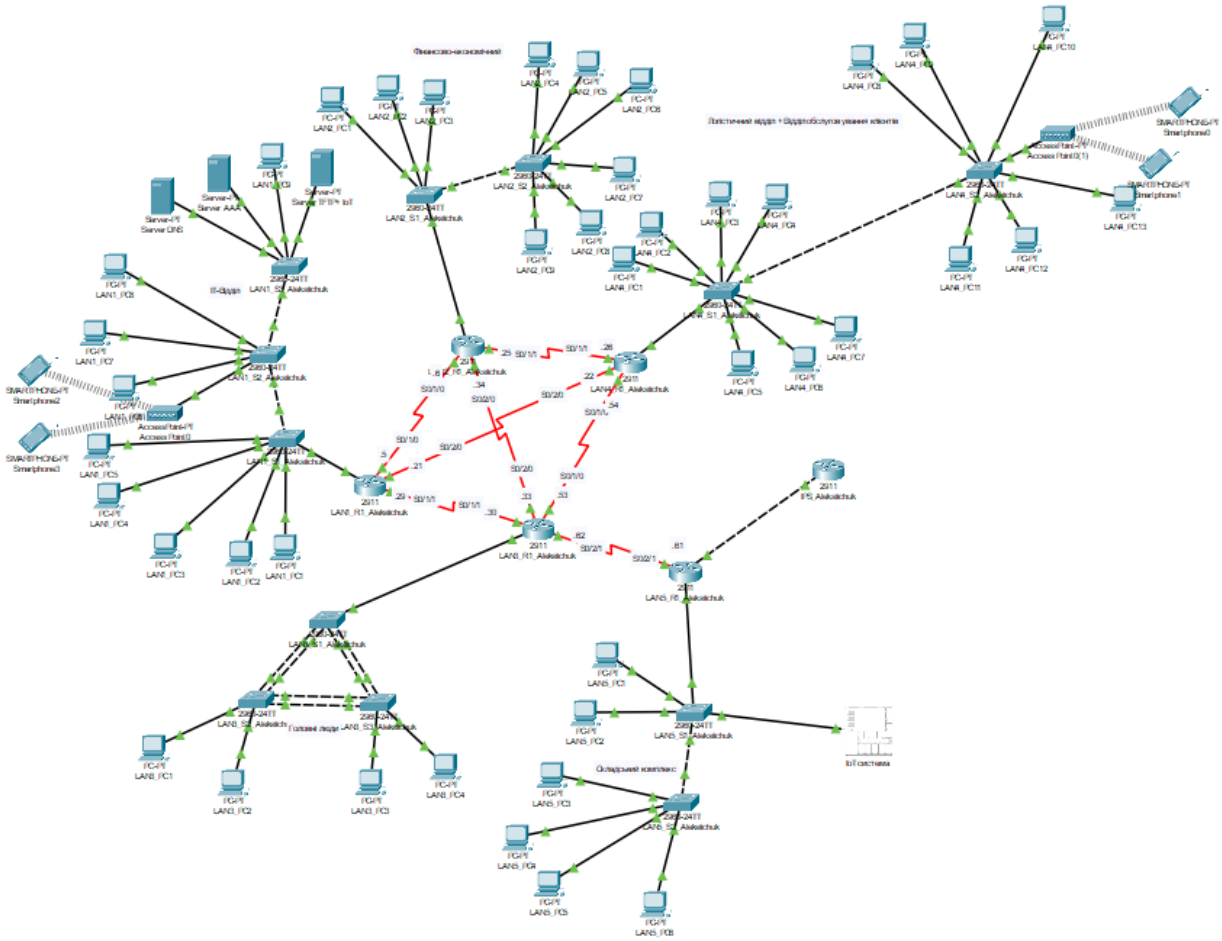


Рисунок 3.1 – мережева архітектура логістичної компанії

3.2 Базові налаштування конфігурації пристроїв

Основні параметри безпеки доступу були налаштовані під час першої конфігурації маршрутизатора. Це дозволяє обмежити несанкціонований доступ до пристрою як з локального, так і з віддаленого підключення. Щоб досягти цього, спочатку потрібно перейти у привілейований режим. У цьому режимі адміністратор отримує повний доступ до приладу та має можливість змінювати його конфігурацію.

Далі встановлюється режим глобальної конфігурації, який дозволяє налаштувати кожну частину роботи маршрутизатора. Після цього встановлюється зашифрований пароль Enable Secret, який використовується для доступу до привілейованого EXEC-режиму. Цей зашифрований пароль підвищує захист у порівнянні зі стандартним Enable Password, оскільки він зберігається в зашифрованому вигляді.

Після цього налаштовується доступ через консольний порт. Для цього використовується команда line console 0, яка дозволяє отримати доступ до параметрів локального входу. Потім встановлюється пароль MarkoAdmin123, який буде запитуватися при фізичному підключенні до пристрою, і використовується команда входу для активації перевірки пароля. Після цього конфігуруються віртуальні термінальні лінії vty 0 4, які використовуються для підключення через Telnet.

Крім того, на них встановлюється пароль CiscoMarko; при спробі віддаленого доступу команда входу вмикає перевірку пароля. Хоча ці налаштування є базовими, вони мають вирішальне значення для безпеки корпоративної мережі, оскільки вони контролюють доступ до мережевого обладнання та створюють основу для подальшої деталізованої конфігурації.

LAN1_R1_Aleksiichuk>enable

Перехід до привілейованого режиму EXEC

LAN1_R1_Aleksiichuk#configure terminal

Вхід у режим глобальної конфігурації

LAN1_R1_Aleksiichuk(config)#enable secret Marko123

Встановлення захищеного пароля доступу до режиму enable

LAN1_R1_Aleksiichuk(config)#exit

Вихід з режиму конфігурації

LAN1_R1_Aleksiichuk#configure terminal

Повторний вхід у режим конфігурації

LAN1_R1_Aleksiichuk(config)#line console 0

Перехід до налаштувань консольного порту

LAN1_R1_Aleksiichuk(config-line)#password MarkoAdmin123

Встановлення пароля для локального доступу

LAN1_R1_Aleksiichuk(config-line)#login

Активація перевірки пароля для консолі

LAN1_R1_Aleksiichuk(config-line)#exit

Вихід до попереднього режиму

LAN1_R1_Aleksiichuk(config)#line vty 0 4

Перехід до налаштування віртуальних ліній (Telnet/SSH)

LAN1_R1_Aleksiichuk(config-line)#password CiscoMarko

Встановлення пароля для віддаленого доступу

LAN1_R1_Aleksiichuk(config-line)#login

Увімкнення перевірки пароля на VTY-лініях

LAN1_R1_Aleksiichuk(config-line)#exit

Завершення конфігурації

LAN1_R1_Aleksiichuk(config)#exit

Повернення до привілейованого режиму

LAN1_R1_Aleksiichuk#

3.2.1 Налаштування маршрутизаторів корпоративної мережі

Протокол маршрутизації EIGRP (покращений внутрішній gateway routing protocol) є основним механізмом обміну маршрутною інформацією між підрозділами корпоративної мережі. EIGRP, вдосконалений протокол Cisco, поєднує переваги протоколів внутрішньої маршрутизації (IGP), включаючи швидке використання пропускної здатності та високу швидкість конвергенції.

Використання алгоритму DUAL, який відрізняє EIGRP від інших протоколів типу RIP, дозволяє вибирати найкращі маршрути для кожної мережі та підтримувати резервні (feasible) шляхи без необхідності постійного обміну повними маршрутними таблицями. Завдяки цьому EIGRP може швидко адаптуватися до змін у топології, що гарантує безперервний обмін даними навіть у разі аварії на одному маршруті.

Включені мережі 172.0.0.0.0, 10.0.0.0, 30.0.0.0 включає всі основні підмережі організації. Вони передаються іншим маршрутизаторам EIGRP, щоб забезпечити повну взаємодію між логістикою, адміністрацією, фінансами, технічною допомогою, компонентами Інтернету речей і керівництвом.

LAN1_R1_Aleksiichuk(config)#interface g0/1

Вибір інтерфейсу GigabitEthernet0/1

LAN1_R1_Aleksiichuk(config-if)#ip address 30.25.16.2 255.255.255.0

Присвоєння IP-адреси та маски підмережі

LAN1_R1_Aleksiichuk(config-if)#exit

Вихід із конфігурації інтерфейсу

LAN1_R1_Aleksiichuk(config)#interface s0/2/1

Вибір серіального інтерфейсу для з’єднання з іншим маршрутизатором

LAN1_R1_Aleksiichuk(config-if)#ip address 10.25.16.61 255.255.255.252

IP-адреса для точкового з’єднання

LAN1_R1_Aleksiichuk(config-if)#exit

Вихід із конфігурації інтерфейсу

LAN1_R1_Aleksiichuk(config)#router eigrp 100

Активація протоколу EIGRP з автономною системою 100

LAN1_R1_Aleksiichuk(config-router)#passive-interface GigabitEthernet0/0

Вимкнення Hello-пакетів на інтерфейсі G0/0

LAN1_R1_Aleksiichuk(config-router)#passive-interface GigabitEthernet0/1

LAN1_R1_Aleksiichuk(config-router)#passive-interface GigabitEthernet0/2

LAN1_R1_Aleksiichuk(config-router)#network 172.0.0.0 0.255.255.255

LAN1_R1_Aleksiichuk(config-router)#network 10.0.0.0

LAN1_R1_Aleksiichuk(config-router)#network 30.0.0.0

```
LAN1_R1_Aleksiichuk#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     8.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       8.8.8.0/24 is directly connected, Loopback0
L       8.8.8.8/32 is directly connected, Loopback0
     10.0.0.0/8 is variably subnetted, 10 subnets, 2 masks
C       10.25.16.4/30 is directly connected, Serial0/1/0
L       10.25.16.5/32 is directly connected, Serial0/1/0
C       10.25.16.20/30 is directly connected, Serial0/2/0
L       10.25.16.21/32 is directly connected, Serial0/2/0
D       10.25.16.24/30 [90/2681856] via 10.25.16.22, 03:26:18, Serial0/2/0
C       10.25.16.28/30 is directly connected, Serial0/1/1
L       10.25.16.29/32 is directly connected, Serial0/1/1
D       10.25.16.32/30 [90/2681856] via 10.25.16.30, 03:26:30, Serial0/1/1
D       10.25.16.52/30 [90/11023872] via 10.25.16.30, 03:26:26, Serial0/1/1
                       [90/11023872] via 10.25.16.22, 03:26:18, Serial0/2/0
D       10.25.16.60/30 [90/2681856] via 10.25.16.30, 05:49:02, Serial0/1/1
     30.0.0.0/24 is subnetted, 1 subnets
D       30.25.16.0/24 [90/2682112] via 10.25.16.30, 00:15:14, Serial0/1/1
     172.25.0.0/16 is variably subnetted, 20 subnets, 4 masks
D       172.25.12.0/27 [90/2684416] via 10.25.16.30, 05:48:19, Serial0/1/1
D       172.25.12.32/27 [90/2684416] via 10.25.16.30, 05:48:19, Serial0/1/1
D       172.25.13.0/27 [90/2172416] via 10.25.16.22, 03:26:18, Serial0/2/0
D       172.25.13.32/27 [90/2172416] via 10.25.16.22, 03:26:18, Serial0/2/0
D       172.25.13.64/27 [90/2172416] via 10.25.16.22, 03:26:18, Serial0/2/0
D       172.25.13.96/27 [90/2172416] via 10.25.16.22, 03:26:18, Serial0/2/0
D       172.25.13.128/27 [90/2172416] via 10.25.16.22, 03:26:18, Serial0/2/0
D       172.25.14.0/27 [90/2172416] via 10.25.16.30, 05:49:02, Serial0/1/1
D       172.25.14.32/27 [90/2172416] via 10.25.16.30, 05:49:02, Serial0/1/1
D       172.25.15.0/27 [90/2684416] via 10.25.16.30, 03:26:24, Serial0/1/1
                       [90/2684416] via 10.25.16.22, 03:26:18, Serial0/2/0
D       172.25.15.32/27 [90/2684416] via 10.25.16.30, 03:26:24, Serial0/1/1
                        [90/2684416] via 10.25.16.22, 03:26:18, Serial0/2/0
D       172.25.15.64/27 [90/2684416] via 10.25.16.30, 03:26:24, Serial0/1/1
                        [90/2684416] via 10.25.16.22, 03:26:18, Serial0/2/0
C       172.25.16.0/26 is directly connected, GigabitEthernet0/0.10
L       172.25.16.1/32 is directly connected, GigabitEthernet0/0.10
C       172.25.16.64/26 is directly connected, GigabitEthernet0/0.20
L       172.25.16.65/32 is directly connected, GigabitEthernet0/0.20
C       172.25.16.128/26 is directly connected, GigabitEthernet0/0.30
L       172.25.16.129/32 is directly connected, GigabitEthernet0/0.30
C       172.25.16.192/28 is directly connected, GigabitEthernet0/0.40
L       172.25.16.193/32 is directly connected, GigabitEthernet0/0.40
```

Рисунок 3.2 – маршрутизація роутера Lan1

```
LAN2_R1_Aleksiichuk#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     8.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       8.8.8.0/24 is directly connected, Loopback0
L       8.8.8.8/32 is directly connected, Loopback0
     10.0.0.0/8 is variably subnetted, 10 subnets, 2 masks
C       10.25.16.4/30 is directly connected, Serial0/1/0
L       10.25.16.6/32 is directly connected, Serial0/1/0
D       10.25.16.20/30 [90/2681856] via 10.25.16.26, 03:27:41, Serial0/1/1
C       10.25.16.24/30 is directly connected, Serial0/1/1
L       10.25.16.25/32 is directly connected, Serial0/1/1
D       10.25.16.28/30 [90/2681856] via 10.25.16.33, 03:27:47, Serial0/2/0
C       10.25.16.32/30 is directly connected, Serial0/2/0
L       10.25.16.34/32 is directly connected, Serial0/2/0
D       10.25.16.52/30 [90/11023872] via 10.25.16.33, 03:27:47, Serial0/2/0
                       [90/11023872] via 10.25.16.26, 03:27:41, Serial0/1/1
D       10.25.16.60/30 [90/2681856] via 10.25.16.33, 03:27:47, Serial0/2/0
     30.0.0.0/24 is subnetted, 1 subnets
D       30.25.16.0/24 [90/2682112] via 10.25.16.33, 00:16:36, Serial0/2/0
     172.25.0.0/16 is variably subnetted, 19 subnets, 4 masks
D       172.25.12.0/27 [90/2684416] via 10.25.16.33, 03:27:47, Serial0/2/0
D       172.25.12.32/27 [90/2684416] via 10.25.16.33, 03:27:47, Serial0/2/0
D       172.25.13.0/27 [90/2172416] via 10.25.16.26, 03:27:42, Serial0/1/1
D       172.25.13.32/27 [90/2172416] via 10.25.16.26, 03:27:42, Serial0/1/1
D       172.25.13.64/27 [90/2172416] via 10.25.16.26, 03:27:42, Serial0/1/1
D       172.25.13.96/27 [90/2172416] via 10.25.16.26, 03:27:42, Serial0/1/1
D       172.25.13.128/27 [90/2172416] via 10.25.16.26, 03:27:42, Serial0/1/1
D       172.25.14.0/27 [90/2172416] via 10.25.16.33, 03:27:47, Serial0/2/0
D       172.25.14.32/27 [90/2172416] via 10.25.16.33, 03:27:47, Serial0/2/0
C       172.25.15.0/27 is directly connected, GigabitEthernet0/0.10
L       172.25.15.1/32 is directly connected, GigabitEthernet0/0.10
C       172.25.15.32/27 is directly connected, GigabitEthernet0/0.20
L       172.25.15.33/32 is directly connected, GigabitEthernet0/0.20
C       172.25.15.64/27 is directly connected, GigabitEthernet0/0.30
L       172.25.15.65/32 is directly connected, GigabitEthernet0/0.30
D       172.25.16.0/26 [90/2684416] via 10.25.16.33, 03:27:47, Serial0/2/0
                       [90/2684416] via 10.25.16.26, 03:27:41, Serial0/1/1
D       172.25.16.64/26 [90/2684416] via 10.25.16.33, 03:27:47, Serial0/2/0
                        [90/2684416] via 10.25.16.26, 03:27:41, Serial0/1/1
D       172.25.16.128/26 [90/2684416] via 10.25.16.33, 03:27:47, Serial0/2/0
                         [90/2684416] via 10.25.16.26, 03:27:41, Serial0/1/1
D       172.25.16.192/28 [90/2684416] via 10.25.16.33, 03:27:47, Serial0/2/0
                         [90/2684416] via 10.25.16.26, 03:27:41, Serial0/1/1
```

Рисунок 3.3 – маршрутизація роутера Lan2

```
LAN3_R1_Aleksiichuk#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     8.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       8.8.8.0/24 is directly connected, Loopback0
L       8.8.8.8/32 is directly connected, Loopback0
     10.0.0.0/8 is variably subnetted, 11 subnets, 2 masks
D       10.25.16.4/30 [90/11023872] via 10.25.16.34, 03:28:03, Serial0/2/0
                      [90/11023872] via 10.25.16.29, 01:38:30, Serial0/1/1
D       10.25.16.20/30 [90/2681856] via 10.25.16.29, 03:28:05, Serial0/1/1
D       10.25.16.24/30 [90/2681856] via 10.25.16.34, 03:28:03, Serial0/2/0
C       10.25.16.28/30 is directly connected, Serial0/1/1
L       10.25.16.30/32 is directly connected, Serial0/1/1
C       10.25.16.32/30 is directly connected, Serial0/2/0
L       10.25.16.33/32 is directly connected, Serial0/2/0
C       10.25.16.52/30 is directly connected, Serial0/1/0
L       10.25.16.53/32 is directly connected, Serial0/1/0
C       10.25.16.60/30 is directly connected, Serial0/2/1
L       10.25.16.62/32 is directly connected, Serial0/2/1
     30.0.0.0/24 is subnetted, 1 subnets
D       30.25.16.0/24 [90/2170112] via 10.25.16.61, 00:16:53, Serial0/2/1
     172.25.0.0/16 is variably subnetted, 18 subnets, 4 masks
D       172.25.12.0/27 [90/2172416] via 10.25.16.61, 05:49:58, Serial0/2/1
D       172.25.12.32/27 [90/2172416] via 10.25.16.61, 05:49:58, Serial0/2/1
D       172.25.13.0/27 [90/2684416] via 10.25.16.34, 03:27:59, Serial0/2/0
                       [90/2684416] via 10.25.16.29, 03:27:57, Serial0/1/1
D       172.25.13.32/27 [90/2684416] via 10.25.16.34, 03:27:59, Serial0/2/0
                        [90/2684416] via 10.25.16.29, 03:27:57, Serial0/1/1
D       172.25.13.64/27 [90/2684416] via 10.25.16.34, 03:27:59, Serial0/2/0
                        [90/2684416] via 10.25.16.29, 03:27:57, Serial0/1/1
D       172.25.13.96/27 [90/2684416] via 10.25.16.34, 03:27:59, Serial0/2/0
                        [90/2684416] via 10.25.16.29, 03:27:57, Serial0/1/1
D       172.25.13.128/27 [90/2684416] via 10.25.16.34, 03:27:59, Serial0/2/0
                         [90/2684416] via 10.25.16.29, 03:27:57, Serial0/1/1
C       172.25.14.0/27 is directly connected, GigabitEthernet0/0.10
L       172.25.14.1/32 is directly connected, GigabitEthernet0/0.10
C       172.25.14.32/27 is directly connected, GigabitEthernet0/0.20
L       172.25.14.33/32 is directly connected, GigabitEthernet0/0.20
D       172.25.15.0/27 [90/2172416] via 10.25.16.34, 03:28:03, Serial0/2/0
D       172.25.15.32/27 [90/2172416] via 10.25.16.34, 03:28:03, Serial0/2/0
D       172.25.15.64/27 [90/2172416] via 10.25.16.34, 03:28:03, Serial0/2/0
D       172.25.16.0/26 [90/2172416] via 10.25.16.29, 05:50:41, Serial0/1/1
D       172.25.16.64/26 [90/2172416] via 10.25.16.29, 05:50:41, Serial0/1/1
D       172.25.16.128/26 [90/2172416] via 10.25.16.29, 05:50:41, Serial0/1/1
D       172.25.16.192/28 [90/2172416] via 10.25.16.29, 05:50:41, Serial0/1/1
```

Рисунок 3.4 – маршрутизація роутера Lan3

```
LAN4_R1_Aleksiichuk#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     8.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       8.8.8.0/24 is directly connected, Loopback0
L       8.8.8.8/32 is directly connected, Loopback0
     10.0.0.0/8 is variably subnetted, 10 subnets, 2 masks
D       10.25.16.4/30 [90/11023872] via 10.25.16.25, 03:28:19, Serial0/1/1
                      [90/11023872] via 10.25.16.21, 01:38:50, Serial0/2/0
C       10.25.16.20/30 is directly connected, Serial0/2/0
L       10.25.16.22/32 is directly connected, Serial0/2/0
C       10.25.16.24/30 is directly connected, Serial0/1/1
L       10.25.16.26/32 is directly connected, Serial0/1/1
D       10.25.16.28/30 [90/2681856] via 10.25.16.21, 03:28:17, Serial0/2/0
D       10.25.16.32/30 [90/2681856] via 10.25.16.25, 03:28:19, Serial0/1/1
C       10.25.16.52/30 is directly connected, Serial0/1/0
L       10.25.16.54/32 is directly connected, Serial0/1/0
D       10.25.16.60/30 [90/3193856] via 10.25.16.25, 03:28:19, Serial0/1/1
                       [90/3193856] via 10.25.16.21, 03:28:17, Serial0/2/0
     30.0.0.0/24 is subnetted, 1 subnets
D       30.25.16.0/24 [90/3194112] via 10.25.16.21, 00:17:13, Serial0/2/0
                      [90/3194112] via 10.25.16.25, 00:17:13, Serial0/1/1
     172.25.0.0/16 is variably subnetted, 21 subnets, 4 masks
D       172.25.12.0/27 [90/3196416] via 10.25.16.25, 03:28:19, Serial0/1/1
                       [90/3196416] via 10.25.16.21, 03:28:17, Serial0/2/0
D       172.25.12.32/27 [90/3196416] via 10.25.16.25, 03:28:19, Serial0/1/1
                        [90/3196416] via 10.25.16.21, 03:28:17, Serial0/2/0
C       172.25.13.0/27 is directly connected, GigabitEthernet0/0.10
L       172.25.13.1/32 is directly connected, GigabitEthernet0/0.10
C       172.25.13.32/27 is directly connected, GigabitEthernet0/0.20
L       172.25.13.33/32 is directly connected, GigabitEthernet0/0.20
C       172.25.13.64/27 is directly connected, GigabitEthernet0/0.30
L       172.25.13.65/32 is directly connected, GigabitEthernet0/0.30
C       172.25.13.96/27 is directly connected, GigabitEthernet0/0.40
L       172.25.13.97/32 is directly connected, GigabitEthernet0/0.40
C       172.25.13.128/27 is directly connected, GigabitEthernet0/0.50
L       172.25.13.129/32 is directly connected, GigabitEthernet0/0.50
D       172.25.14.0/27 [90/2684416] via 10.25.16.25, 03:28:19, Serial0/1/1
                       [90/2684416] via 10.25.16.21, 03:28:17, Serial0/2/0
D       172.25.14.32/27 [90/2684416] via 10.25.16.25, 03:28:19, Serial0/1/1
                        [90/2684416] via 10.25.16.21, 03:28:17, Serial0/2/0
D       172.25.15.0/27 [90/2172416] via 10.25.16.25, 03:28:19, Serial0/1/1
D       172.25.15.32/27 [90/2172416] via 10.25.16.25, 03:28:19, Serial0/1/1
D       172.25.15.64/27 [90/2172416] via 10.25.16.25, 03:28:19, Serial0/1/1
D       172.25.16.0/26 [90/2172416] via 10.25.16.21, 03:28:17, Serial0/2/0
D       172.25.16.64/26 [90/2172416] via 10.25.16.21, 03:28:17, Serial0/2/0
D       172.25.16.128/26 [90/2172416] via 10.25.16.21, 03:28:17, Serial0/2/0
D       172.25.16.192/28 [90/2172416] via 10.25.16.21, 03:28:17, Serial0/2/0
```

Рисунок 3.5 – маршрутизація роутера Lan4

3.2.2 Налаштування роботи мережі інтернет

У цьому розділі реалізовано налаштування маршрутизатора, щоб організувати доступ корпоративної мережі до мережі Інтернет, включаючи базові функції безпеки, маршрутизації та трансляції NAT.

На інтерфейсі GigabitEthernet0/1, який підключений до провайдера, було налаштовано IP-адресу 30.25.16.2, а маску було налаштовано 255.255.255.0. Цей інтерфейс маркується директивою IP NAT outside, що означає, що він є поза зоною NAT. Усі внутрішні адреси, або внутрішні інтерфейси мережі, називають IP-адресою NAT.

Динамічна трансляція внутрішніх адрес у зовнішні з перевантаженням (PAT) здійснюється командою ip nat inside source list NAT_ACL interface GigabitEthernet0/1 overload. Це дозволяє кільком внутрішнім пристроям одночасно виходити в Інтернет за допомогою однієї зовнішньої IP-адреси. Це призводить до ефективного використання адресного простору та спрощеного керування.

Використовуючи команду ip nat inside source list NAT_ACL interface GigabitEthernet0/1 overload, можна динамічно транслювати внутрішні адреси у зовнішні з перевантаженням (PAT). Це дозволяє кільком внутрішнім пристроям одночасно виходити в Інтернет за допомогою однієї зовнішньої IP-адреси. Це призводить до ефективного використання адресного простору та спрощеного керування.

Крім того, використовується статична внутрішня IP-адреса 172.25.0.0 30.25.16.10, яка забезпечує статичне зіставлення внутрішньої підмережі 172.25.0.0 із зовнішньою IP-адресою 30.25.16.10. Це може бути корисним для сервісів, які потребують зовнішнього доступу, наприклад поштових серверів і веб-серверів, які повинні бути доступними користувачам Інтернету.

LAN5_R1_Aleksiichuk(config)# interface GigabitEthernet0/1

LAN5_R1_Aleksiichuk(config-if)# ip address 30.25.16.2 255.255.255.0

Задання IP-адреси зовнішнього інтерфейсу

LAN5_R1_Aleksiichuk(config-if)# ip nat outside

Позначення інтерфейсу як зовнішнього для NAT

LAN5_R1_Aleksiichuk(config-if)# exit

LAN5_R1_Aleksiichuk(config)# interface GigabitEthernet0/0

LAN5_R1_Aleksiichuk(config-if)# ip address 172.25.0.1 255.255.0.0

IP-адреса внутрішнього інтерфейсу

LAN5_R1_Aleksiichuk(config-if)# ip nat inside

Визначення як внутрішнього інтерфейсу NAT

LAN5_R1_Aleksiichuk(config-if)# exit

LAN5_R1_Aleksiichuk(config)# ip nat inside source list NAT_ACL interface GigabitEthernet0/1 overload

Динамічний NAT з перевантаженням через зовнішній інтерфейс

LAN5_R1_Aleksiichuk(config)# ip nat inside source static 172.25.0.0 30.25.16.10

Статичне зіставлення приватної підмережі з зовнішньою IP-адресою

LAN5_R1_Aleksiichuk(config)# ip classless

Увімкнення безкласової маршрутизації

LAN5_R1_Aleksiichuk(config)# ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/1

Маршрут за замовчуванням до Інтернету

LAN5_R1_Aleksiichuk(config)# ip access-list extended PRIVATE_ACL

LAN5_R1_Aleksiichuk(config-ext-nacl)# deny ip 172.25.0.0 0.0.0.63 any

LAN5_R1_Aleksiichuk(config-ext-nacl)# exit

ACL для заборони трафіку певної частини мережі до зовнішніх ресурсів

LAN5_R1_Aleksiichuk(config)# ip access-list standard NAT_ACL

LAN5_R1_Aleksiichuk(config-std-nacl)# permit 172.25.0.0 0.0.255.255

LAN5_R1_Aleksiichuk(config-std-nacl)# permit any

LAN5_R1_Aleksiichuk(config-std-nacl)# exit

NAT Table for LAN5_R1_Aleksiichuk

Protocol	Inside Global	Inside Local	Outside Local	Outside Global
icmp	30.25.16.2:1	172.25.16.73:1	30.25.16.1:1	30.25.16.1:1
icmp	30.25.16.2:2	172.25.16.73:2	30.25.16.1:2	30.25.16.1:2
---	30.25.16.10	172.25.0.0	---	---
tcp	30.25.16.2:1042	172.25.12.39:1042	172.25.16.3:31000	172.25.16.3:31000
tcp	30.25.16.2:1045	172.25.12.39:1045	172.25.16.3:31000	172.25.16.3:31000
tcp	30.25.16.2:1046	172.25.12.39:1046	172.25.16.3:31000	172.25.16.3:31000

Рисунок 3.6 – перевірка працездатності NAT

3.2.3 Налаштування та перевірка DHCP

Маршрутизатор підтримує повну службу DHCP (Dynamic Host Configuration Protocol) для автоматичної конфігурації IP-адрес, шлюзів і DNS-серверів у корпоративній мережі. Це значно полегшує управління мережею та запобігає помилкам, пов’язаним із ручним призначенням IP-адрес. DHCP-сервер автоматично надає IP-адреси клієнтам кожного VLAN відповідно до їхніх цілей.

Перед налаштуванням DHCP були визначені винятки, наприклад адреси, які не повинні видаватися динамічно, оскільки вони зарезервовані для шлюзів, принтерів, серверів або іншого мережевого обладнання. Далі для кожного відділу логістичного та клієнтської підтримки були створені окремі DHCP-пули. Ці DHCP-пули містять параметри, такі як DNS-сервер, адреса шлюзу за замовчуванням і діапазон мережі. Крім того, інтерфейс trunk на фізичному порту маршрутизатора був налаштований і поділений на підінтерфейси для кожного VLAN. Це дозволяє маршрутизаторам працювати з кількома VLAN.

LAN4_R1_Aleksiichuk(config)# ip dhcp excluded-address 172.25.13.1 172.25.13.5

LAN4_R1_Aleksiichuk(config)# ip dhcp excluded-address 172.25.13.33 172.25.13.38

LAN4_R1_Aleksiichuk(config)# ip dhcp excluded-address 172.25.13.65 172.25.13.70

LAN4_R1_Aleksiichuk(config)# ip dhcp excluded-address 172.25.13.97 172.25.13.102

LAN4_R1_Aleksiichuk(config)# ip dhcp excluded-address 172.25.13.129 172.25.13.134

Вказуються IP-адреси, які DHCP-сервер не повинен видавати динамічно

LAN4_R1_Aleksiichuk(config)# ip dhcp pool Logist1

LAN4_R1_Aleksiichuk(dhcp-config)# network 172.25.13.0 255.255.255.224

LAN4_R1_Aleksiichuk(dhcp-config)# default-router 172.25.13.1

LAN4_R1_Aleksiichuk(dhcp-config)# dns-server 172.25.16.5

DHCP-пул для логістів-диспетчерів

LAN4_R1_Aleksiichuk(config)# ip dhcp pool Logist2

LAN4_R1_Aleksiichuk(dhcp-config)# network 172.25.13.32 255.255.255.224

LAN4_R1_Aleksiichuk(dhcp-config)# default-router 172.25.13.33

LAN4_R1_Aleksiichuk(dhcp-config)# dns-server 172.25.16.5

DHCP-пул для логістів-планувальників

LAN4_R1_Aleksiichuk(config)# ip dhcp pool Manager1

LAN4_R1_Aleksiichuk(dhcp-config)# network 172.25.13.64 255.255.255.224

LAN4_R1_Aleksiichuk(dhcp-config)# default-router 172.25.13.65

LAN4_R1_Aleksiichuk(dhcp-config)# dns-server 172.25.16.5

DHCP-пул для менеджерів з клієнтської підтримки

LAN4_R1_Aleksiichuk(config)# ip dhcp pool Manager2

LAN4_R1_Aleksiichuk(dhcp-config)# network 172.25.13.96 255.255.255.224

LAN4_R1_Aleksiichuk(dhcp-config)# default-router 172.25.13.97

LAN4_R1_Aleksiichuk(dhcp-config)# dns-server 172.25.16.5

DHCP-пул для менеджерів з обробки замовлень

LAN4_R1_Aleksiichuk(config)# ip dhcp pool Oper

LAN4_R1_Aleksiichuk(dhcp-config)# network 172.25.13.128 255.255.255.224

LAN4_R1_Aleksiichuk(dhcp-config)# default-router 172.25.13.129

LAN4_R1_Aleksiichuk(dhcp-config)# dns-server 172.25.16.5

LAN4_R1_Aleksiichuk(config)# interface GigabitEthernet0/0

LAN4_R1_Aleksiichuk(config-if)# no ip address

LAN4_R1_Aleksiichuk(config-if)# duplex auto

LAN4_R1_Aleksiichuk(config-if)# speed auto

LAN4_R1_Aleksiichuk(config-if)# exit

Налаштування фізичного інтерфейсу як trunk

LAN4_R1_Aleksiichuk(config)# interface GigabitEthernet0/0.10

LAN4_R1_Aleksiichuk(config-subif)# encapsulation dot1Q 10

LAN4_R1_Aleksiichuk(config-subif)# ip address 172.25.13.1 255.255.255.224

LAN4_R1_Aleksiichuk(config-subif)# ip nat inside

Підінтерфейс для VLAN 10 – логісти диспетчери

LAN4_R1_Aleksiichuk(config)# interface GigabitEthernet0/0.20

LAN4_R1_Aleksiichuk(config-subif)# encapsulation dot1Q 20

LAN4_R1_Aleksiichuk(config-subif)# ip address 172.25.13.33 255.255.255.224

LAN4_R1_Aleksiichuk(config-subif)# ip nat inside

VLAN 20 – логісти планувальники

LAN4_R1_Aleksiichuk(config)# interface GigabitEthernet0/0.30

LAN4_R1_Aleksiichuk(config-subif)# encapsulation dot1Q 30

LAN4_R1_Aleksiichuk(config-subif)# ip address 172.25.13.65 255.255.255.224

LAN4_R1_Aleksiichuk(config-subif)# ip nat inside

VLAN 30 – менеджери з підтримки

LAN4_R1_Aleksiichuk(config)# interface GigabitEthernet0/0.40

LAN4_R1_Aleksiichuk(config-subif)# encapsulation dot1Q 40

LAN4_R1_Aleksiichuk(config-subif)# ip address 172.25.13.97 255.255.255.224

LAN4_R1_Aleksiichuk(config-subif)# ip nat inside

VLAN 40 – обробка замовлень

LAN4_R1_Aleksiichuk(config)# interface GigabitEthernet0/0.50

LAN4_R1_Aleksiichuk(config-subif)# encapsulation dot1Q 50

LAN4_R1_Aleksiichuk(config-subif)# ip address 172.25.13.129 255.255.255.224

LAN4_R1_Aleksiichuk(config-subif)# ip nat inside

VLAN 50 – оператори

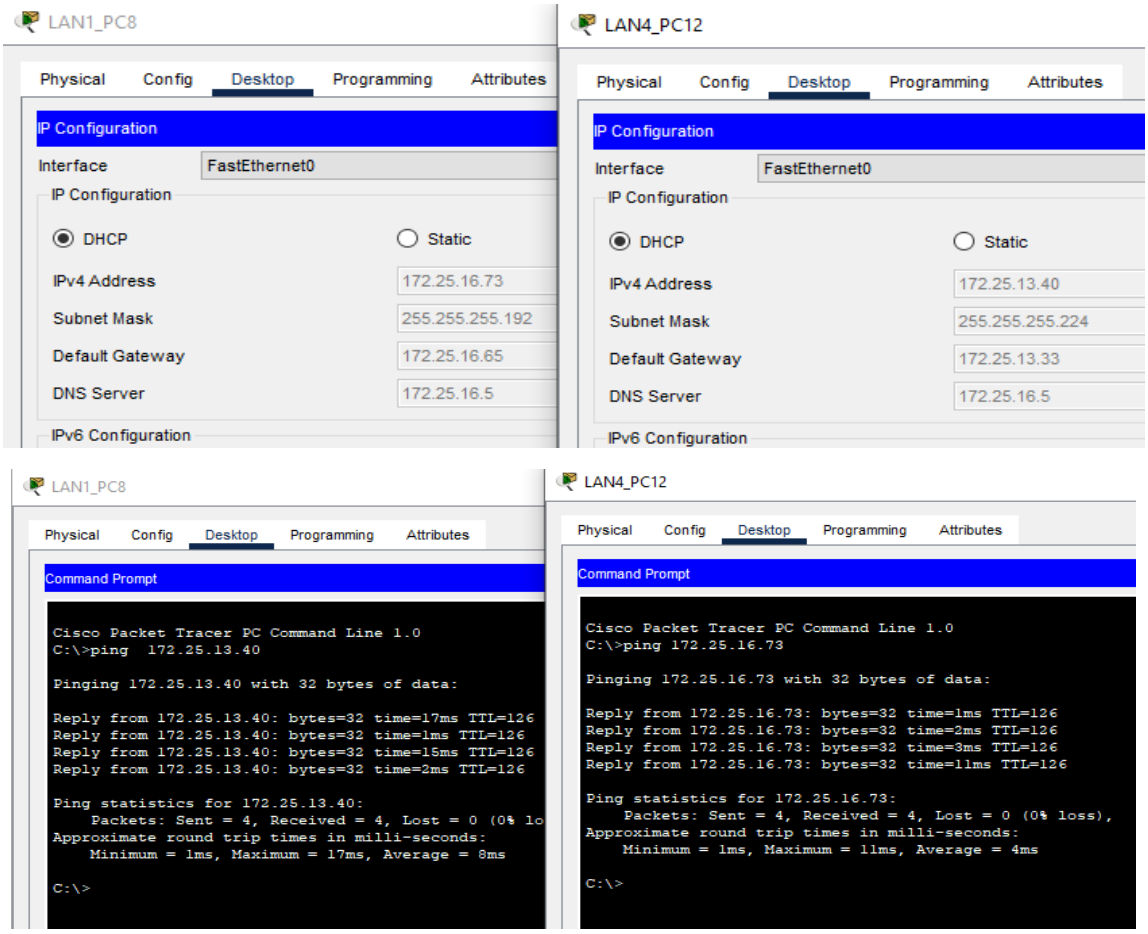


Рисунок 3.7 – Перевірка працездатності DHCP

```
LAN4_R1_Aleksiichuk#show ip dhcp binding
IP address       Client-ID/              Lease expiration        Type
                 Hardware address
172.25.13.6      0002.179E.AA72            --                    Automatic
172.25.13.7      0010.11D1.88EA            --                    Automatic
172.25.13.8      00E0.A345.5B34            --                    Automatic
172.25.13.41     0006.2A53.D596            --                    Automatic
172.25.13.42     00D0.D365.4D74            --                    Automatic
172.25.13.43     00E0.F9A0.14B0            --                    Automatic
172.25.13.74     000B.BEAB.CA43            --                    Automatic
172.25.13.75     0002.1624.1C30            --                    Automatic
172.25.13.72     000C.CF39.1A0B            --                    Automatic
172.25.13.106    00D0.BA9A.11A8            --                    Automatic
172.25.13.107    00D0.BA42.C95B            --                    Automatic
172.25.13.104    0002.4ABA.B293            --                    Automatic
172.25.13.135    000C.8536.88DE            --                    Automatic
LAN4_R1_Aleksiichuk#
```

Рисунок 3.8 – Перевірка працездатності DHCP

3.3 Захист інформації в комп’ютерній системі

3.3.1 Впровадження підтримки служби AAA

Для забезпечення централізованої автентифікації користувачів у корпоративній мережі було запроваджено підтримку служби AAA (Authentication, Authorization, Accounting). Це дозволяє запровадити єдину політику доступу до мережевих пристроїв. Використовується зовнішній сервер RADIUS замість локальної автентифікації, що базується на паролях CLI. Такий метод покращує безпеку, гнучкість управління обліковими записами та спрощення аудиту доступу.

У нижчій конфігурації включено новий модель AAA, реалізовано базове підключення до сервера RADIUS і налаштовано лінії віртуального терміналу VTY для використання автентифікації RADIUS.

LAN4_R1_Aleksiichuk(config)# aaa new-model

Вмикається нова модель AAA для централізованої автентифікації

LAN4_R1_Aleksiichuk(config)# radius-server host 172.25.16.2

Вказується IP-адреса сервера RADIUS, з яким буде встановлено зв’язок

LAN4_R1_Aleksiichuk(config)# radius-server key CiscoMarko

Задається ключ (shared secret) для шифрування взаємодії між пристроєм і RADIUS-сервером

LAN4_R1_Aleksiichuk(config)# line vty 0 4

Налаштування доступу до маршрутизатора по Telnet/SSH

LAN4_R1_Aleksiichuk(config-line)# login authentication AAA

Вказується, що для автентифікації потрібно використовувати механізм AAA

LAN4_R1_Aleksiichuk(config-line)# exit

LAN4_R1_Aleksiichuk(config)# end

LAN4_R1_Aleksiichuk# write memory

Збереження конфігурації в пам’ять (startup-config)

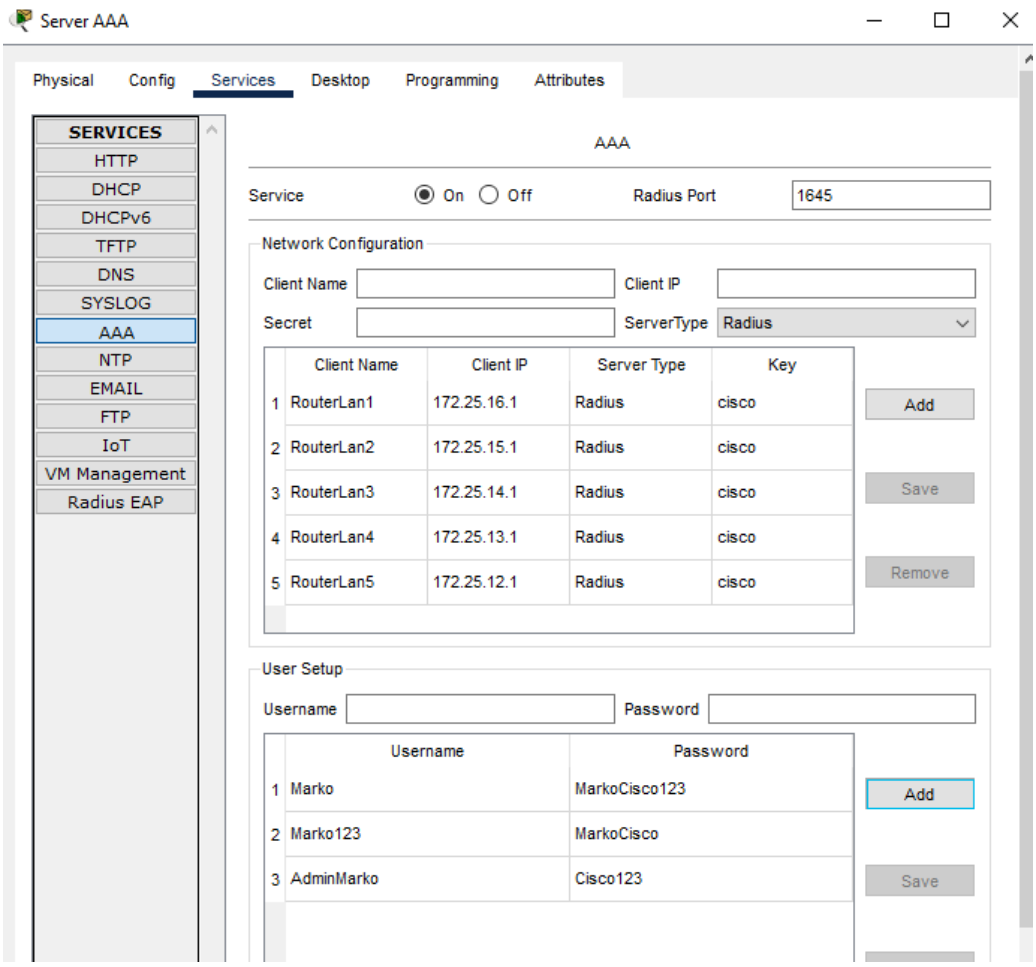


Рисунок 3.9 – Налаштування AAA на сервері

```
[Connection to 172.25.16.1 closed by foreign host]
C:\>telnet 172.25.16.1
Trying 172.25.16.1 ...Open


User Access Verification

Username: Marko
Password:
LAN1_R1_Aleksiichuk>
```

Рисунок 3.10 – Перевірка працездатності AAA захисту

3.3.2 Впровадження підтримки служби PgAC

Підтримка протоколу агрегування каналів, також відомого як PAgP, була введена для підвищення продуктивності та безпеки мережевих підключень у корпоративних мережах. Це дозволяє об’єднати кілька фізичних портів у один логічний канал, також відомий як EtherChannel. Це дозволяє балансувати навантаження між портами та усуває вузькі місця в мережі. PAgP забезпечує правильну синхронізацію параметрів і уникнення петлі в мережі, автоматично координуючи об’єднання портів між пристроями Cisco.

У цьому прикладі один комутатор використовує інтерфейс FastEthernet 0/22–24, щоб перейти в режим автоматичного очікування початку агрегування. Ті ж інтерфейси налаштовані на іншому комутаторі в режим бажаний, що означає активну ініціацію агрегування через PAgP. Обидва пристрої об’єднують ці порти в один логічний канал (канальна група 1). Зв’язок може відбутися лише після того, як обидві сторони погодяться про параметри каналу.

SW1(config)# interface range fastEthernet0/22 - 24

SW1(config-if-range)# channel-group 1 mode auto

Порти 0/22-0/24 налаштовані в режимі PAgP auto – пасивний режим очікування

SW2(config)# interface range fastEthernet0/22 - 24

SW2(config-if-range)# channel-group 1 mode desirable

Порти 0/22-0/24 налаштовані в режимі PAgP desirable – активний режим ініціювання агрегування

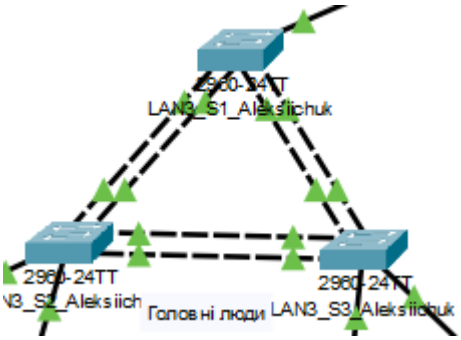


Рисунок 3.11 – Перевірка працездатності

3.3.3 Налаштування мереж VLAN на прикладі LAN5

Для розподілу трафіку між різними підрозділами та пристроями корпораційна мережа, зокрема сегмент LAN5, використовує налаштування логічних підмереж VLAN. Кожна VLAN має параметри маршрутизації, шлюз за замовчуванням, DNS-сервер і IP-діапазон. Коли DHCP-сервер розгортається безпосередньо на маршрутизаторі, він може динамічно видавати IP-адреси клієнтам у межах відповідних VLAN.

У наступному прикладі для кожної підмережі налаштовано DHCP-пул окремо:

– BLAN 10 обслуговується Logist1 через мережу 172.25.13.0/27 і шлюз 172.25.13.1;
– Для VLAN 20 Logist2 використовує мережу 172.25.13.32/27 і шлюз 172.25.13.33;
– Manager1 відповідає за VLAN 30, мережу 172.25.13.64/27 і шлюз 172.25.13.65;
– Manager2 має VLAN 40, мережу 172.25.13.96/27 і шлюз 172.25.13.97.
– Oper використовує VLAN 50, мережу 172.25.13.128/27 і шлюз 172.25.13.129.

```
LAN1_S1_Aleksiichuk#sh vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                Gig0/2
10   VLAN0010                         active
20   VLAN0020                         active
30   VLAN0030                         active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10
40   VLAN0040                         active    Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Рисунок 3.12 – Налаштування Vlan для маршрутизатора Lan1_s1

```
LAN1_S2_Aleksiichuk#sh vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                 Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                 Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                 Gig0/1, Gig0/2
10   VLAN0010                          active
20   VLAN0020                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10
30   VLAN0030                          active
40   VLAN0040                          active
50   VLAN0050                          active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

Рисунок 3.13 – Налаштування Vlan для маршрутизатора Lan1_s2

```
LAN1_S3_Aleksiichuk#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                 Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                 Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                 Fa0/23, Gig0/1, Gig0/2
10   VLAN0010                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

Рисунок 3.14 – Налаштування Vlan для маршрутизатора Lan1_s3

```
Device Name: LAN1_R1_Aleksiichuk
Device Model: 2911
Hostname: LAN1_R1_Aleksiichuk

Port                  Link   VLAN   IP Address         IPv6 Address                              MAC Address
GigabitEthernet0/0    Up     --     <not set>          <not set>                                 0002.4A86.9354
GigabitEthernet0/0.10 Up     --     172.25.16.1/26     <not set>                                 0002.4A86.9354
GigabitEthernet0/0.20 Up     --     172.25.16.65/26    <not set>                                 0002.4A86.9354
GigabitEthernet0/0.30 Up     --     172.25.16.129/26   <not set>                                 0002.4A86.9354
GigabitEthernet0/0.40 Up     --     172.25.16.193/28   <not set>                                 0002.4A86.9354
GigabitEthernet0/1    Up     --     <not set>          <not set>                                 0003.E457.1132
GigabitEthernet0/2    Up     --     <not set>          <not set>                                 0003.E403.5158
Serial0/1/0           Up     --     10.25.16.5/30      <not set>                                 <not set>
Serial0/1/1           Up     --     10.25.16.29/30     <not set>                                 <not set>
Serial0/2/0           Up     --     10.25.16.21/30     <not set>                                 <not set>
Serial0/2/1           Down   --     <not set>          <not set>                                 <not set>
Serial0/3/0           Down   --     <not set>          <not set>                                 <not set>
Serial0/3/1           Down   --     <not set>          <not set>                                 <not set>
Loopback0             Up     --     8.8.8.8/24         <not set>                                 0006.2A0C.59DB
Vlan1                 Down   1      <not set>          <not set>                                 0002.4A44.2251
```

Рисунок 3.15 – Перевірка налаштування головного роутера

3.3.4 Налаштування віртуальної приватної мережі VPN

У корпоративній мережі використовується технологія IPSec VPN Site-to-Site для налаштування віртуальної приватної мережі (VPN). Ця технологія дозволяє двом офісам або підрозділам компанії мати безпечний зашифрований зв’язок через мережу Інтернет. Це дозволяє безпечно передавати конфіденційні дані між віддаленими мережами.

Основною метою використання VPN є створення захищеного каналу між центральним офісом і віддаленим місцем, таким як склад, логістичний центр або сегмент Інтернету речей. Для досягнення цього на маршрутизаторі налаштовується обмін ключами (ISAKMP), параметри шифрування (IPSec), списки доступу до VPN-трафіку та криптографічна карта, яка підключена до відповідного інтерфейсу.

LAN1_R1_Aleksiichuk(config)# crypto isakmp policy 10

Створення політики ISAKMP (IKE Phase 1) з пріоритетом 10

LAN1_R1_Aleksiichuk(config-isakmp)# encryption 3des

Визначення алгоритму шифрування – Triple DES

LAN1_R1_Aleksiichuk(config-isakmp)# hash md5

Визначення хеш-функції для цілісності – MD5

LAN1_R1_Aleksiichuk(config-isakmp)# authentication pre-share

Вибір типу автентифікації – за попередньо узгодженим ключем

LAN1_R1_Aleksiichuk(config-isakmp)# group 2

LAN1_R1_Aleksiichuk(config)# crypto isakmp key cisco address 67.110.16.2

Встановлення загального ключа (pre-shared key) "cisco" для IP-адреси віддаленого партнера

LAN1_R1_Aleksiichuk(config)# crypto ipsec transform-set TS esp-3des esp-md5-hmac

Створення трансформ-набору IPsec для шифрування і хешування

LAN1_R1_Aleksiichuk(cfg-crypto-trans)# exit

LAN1_R1_Aleksiichuk(config)# ip access-list extended Marko-VPN

Створення розширеного ACL для дозволу трафіку через VPN-тунель

LAN1_R1_Aleksiichuk(config-ext-nacl)# permit ip 10.25.16.0 0.0.255.255 172.25.12.0 0.0.255.255

Дозвіл трафіку з підмережі офісу до віддаленої мережі

LAN1_R1_Aleksiichuk(config-ext-nacl)# permit ip 172.25.16.0 0.0.255.255 172.25.12.0 0.0.255.255

Дозвіл з іншого діапазону локальної мережі до тієї ж віддаленої підмережі

LAN1_R1_Aleksiichuk(config)# crypto map VPN-MAP 10 ipsec-isakmp

Створення карти криптографії VPN з пріоритетом 10, що базується на ISAKMP

LAN1_R1_Aleksiichuk(config-crypto-map)# set peer 97.128.46.2

Зазначення IP-адреси віддаленого маршрутизатора для з’єднання

LAN1_R1_Aleksiichuk(config-crypto-map)# set transform-set TS

Призначення раніше створеного трансформ-набору TS

LAN1_R1_Aleksiichuk(config-crypto-map)# match address Marko-VPN

Вказання ACL, яка визначає, який трафік має шифруватися

LAN1_R1_Aleksiichuk(config)# interface Serial0/1/1

Переходимо до інтерфейсу, який з’єднується з віддаленою мережею (наприклад, через провайдера)

LAN1_R1_Aleksiichuk(config-if)# crypto map VPN-MAP

Прив’язуємо криптографічну карту до інтерфейсу – активуємо IPsec тунель на ньому

```
interface: Serial0/1/1
    Crypto map tag: VPN-MAP, local addr 10.25.16.25

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (10.25.0.0/255.255.0.0/0/0)
   remote  ident (addr/mask/prot/port): (172.25.0.0/255.255.0.0/0/0)
   current_peer 97.128.46.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
   #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 0

     local crypto endpt.: 10.25.16.25, remote crypto endpt.:97.128.46.2
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1/1
     current outbound spi: 0x0(0)

     inbound esp sas:

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:

     outbound ah sas:

     outbound pcp sas:

   local  ident (addr/mask/prot/port): (172.25.0.0/255.255.0.0/0/0)
   remote  ident (addr/mask/prot/port): (172.25.0.0/255.255.0.0/0/0)
   current_peer 97.128.46.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
   #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 0

     local crypto endpt.: 10.25.16.25, remote crypto endpt.:97.128.46.2
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1/1
     current outbound spi: 0x0(0)
```

Рисунок 3.16 Перевірка VPN для Lan2_R1

```
LAN4_R1_Aleksiichuk(config)#do show crypto ipsec sa

interface: Serial0/1/1
    Crypto map tag: VPN-MAP, local addr 10.25.16.26

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (10.25.0.0/255.255.0.0/0/0)
   remote  ident (addr/mask/prot/port): (172.25.0.0/255.255.0.0/0/0)
   current_peer 97.128.46.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
   #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 0

     local crypto endpt.: 10.25.16.26, remote crypto endpt.:97.128.46.2
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1/1
     current outbound spi: 0x0(0)

     inbound esp sas:

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:

     outbound ah sas:

     outbound pcp sas:

   local  ident (addr/mask/prot/port): (172.25.0.0/255.255.0.0/0/0)
   remote  ident (addr/mask/prot/port): (172.25.0.0/255.255.0.0/0/0)
   current_peer 97.128.46.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
   #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 0

     local crypto endpt.: 10.25.16.26, remote crypto endpt.:97.128.46.2
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1/1
     current outbound spi: 0x0(0)
```

Рисунок 3.17 Перевірка VPN для Lan4_R1

4. РОЗРОБКА IOT СИСТЕМИ

4.1 Аналіз використання IoT пристроїв та розробка специфікації

Особлива увага приділяється інтеграції пристроїв Internet of Things (IoT) під час створення сучасної корпоративної мережі в середовищі складу та логістичного центру. Ці пристрої автоматизують і контролюють життєво важливі процеси, що значно підвищує продуктивність персоналу, знижує ризики та покращує безпеку об’єкта.

RFID-зчитувач – Impinj Speedway R420.Цей зчитувач вибрано через високу швидкість обробки міток, підтримку до 4 антен, стабільну роботу в промисловому середовищі та підтримку протоколів LLRP і REST API. Його легко інтегрувати з Cisco IR1101 через Ethernet. У порівнянні з аналогами, як-от Zebra FX9600, Impinj має кращу документацію, зручніші SDK для розробників та стабільніший мережевий стек.

Аварійна кнопка – Schneider Electric XB4. Це промислова кнопка з металевим корпусом, яка має високу зносостійкість і ступінь захисту IP66. Завдяки широкому вибору контактних блоків, легко підключається до I/O-модуля Cisco IR1101. У порівнянні з Siemens 3SB3, XB4 виграє за надійністю та механічною витривалістю. Дає змогу миттєво ініціювати аварійну зупинку всіх підключених систем.

Датчик диму – Honeywell 5808W3 + ZigBee шлюз. Цей димовий датчик має бездротове підключення через ZigBee і здатен автономно працювати до кількох років. У парі з ZigBee-шлюзом інтегрується до Cisco IR1101 по MQTT або REST API. Альтернативи на зразок Bosch FAP-425 потребують провідного монтажу й менш зручні для віддаленого моніторингу. Honeywell пропонує оптимальний баланс між автономністю, чутливістю та простотою інтеграції.

Датчик температури – Schneider Electric STP700.Має цифровий вихід Modbus RTU, що забезпечує високу точність та стабільність передачі даних у промисловому середовищі. На відміну від аналогових моделей (наприклад, Siemens QAA24), STP700 не потребує перетворення сигналу. Підключається безпосередньо

до шлюзу Cisco через послідовний або мережевий Modbus. Ідеальний для моніторингу температури у виробничих або серверних зонах.

Кондиціонер – Daikin SkyAir + шлюз DIII-Net. Промисловий кондиціонер з інверторною технологією, що забезпечує енергоефективне охолодження. Через шлюз DIII-Net підтримує BACnet і Modbus TCP. Інтегрується з Cisco IR1101 для віддаленого керування температурою та моніторингу стану. У порівнянні з Mitsubishi City Multi, Daikin має відкритіші протоколи і краще документовану інтеграцію.

Сигналізація – Ajax Hub 2 Plus. Сучасна бездротова охоронна система з Ethernet та LTE-підключенням. Підтримує MQTT і HTTP API, що дозволяє легко підключити її до Cisco IR1101 без додаткових шлюзів. На відміну від систем типу Jablotron або Paradox, Ajax забезпечує просту та швидку інтеграцію через відкритий API та інтуїтивний інтерфейс управління.

Автоматичне вікно – VELUX Integra + шлюз KLF 200. Вікно з моторизованим приводом, яким можна керувати дистанційно через REST API або сухі контакти. Шлюз KLF 200 дозволяє інтеграцію з будь-якою системою автоматизації, включаючи Cisco IR1101. Порівняно з Fakro Z-Wave, VELUX надає стабільніший API, офіційну технічну підтримку та гнучке підключення як до мережевих, так і до дискретних інтерфейсів.

Головний контролер – Cisco IR1101. Центральний елемент системи, який поєднує всі пристрої в одну IoT-мережу. Підтримує Docker, IOx, MQTT, Modbus, REST, BACnet, Ethernet, LTE/4G. Завдяки гнучкості та широкому спектру протоколів, Cisco IR1101 дозволяє підключати як цифрові, так і аналогові пристрої, шлюзи та системи автоматизації. У порівнянні з Siemens IoT2040 має більшу продуктивність, гнучкість і офіційну підтримку Cisco.

Пожежні спринклери – Tyco ESFR25 TY9226. Сертифіковані UL/FM спринклери для систем активного пожежогасіння. Активуються через електромагнітні клапани, які керуються контролером або I/O модулем. Порівняно з Viking або Reliable, Tyco пропонує розширену лінійку підвищеного тиску для швидкого гасіння. Вони сумісні з Belimo EV-клапанами.

Клапани до спринклерів – Belimo EV серія + шлюз MP-Bus/Modbus. Електронні клапани з підтримкою Modbus RTU або MP-Bus. Легко інтегруються з Cisco IR1101 для керування подачею води до спринкерів. У порівнянні з Siemens серії SFP, Belimo забезпечує точніше керування, кращу діагностику та менше споживання енергії.

Daikin SkyAir + шлюз DIII-Net. Інверторний кондиціонер з підтримкою Modbus TCP і BACnet через шлюз DIII-Net. Забезпечує ефективне охолодження та вентиляцію з можливістю віддаленого керування та моніторингу. Інтегрується з Cisco IR1101 через Ethernet. У порівнянні з Mitsubishi City Multi має простіший шлюз, краще документоване API та нижчу вартість впровадження.

Усі пристрої підібрано з урахуванням підтримки відкритих промислових протоколів: Modbus, BACnet, MQTT, REST API, LLRP, ZigBee. Завдяки багатофункціональному шлюзу Cisco IR1101, вони можуть бути об'єднані в єдину централізовану систему. Комунікація між компонентами забезпечується через Ethernet, цифрові входи/виходи, шлюзи та стандартні API. Така система є масштабованою, безпечною та придатною для розгортання в реальному виробничому середовищі.

Таблиця 4.1 Специфікація IoT пристроїв

Компонент	Модель/Тип	Призначення	Кількість	Примітка
RFID-зчитувач	Impinj Speedway R420	Зчитування RFID-міток на об'єктах або продукції	4	Ethernet-з'єднання, підтримка REST API або LLRP для Cisco IR1101
Аварійна кнопка	Schneider Electric XB4	Зупинка системи у надзвичайних ситуаціях	1	Підключення до I/O модуля Cisco IR1101 через дискретні входи
Датчик диму	Honeywell 5808W3 + ZigBee шлюз	Виявлення диму/пожежі у приміщенні	2	Інтеграція через ZigBee шлюз до Cisco IR1101, підтримка MQTT/REST API
Датчик температури	Siemens QAA2060 + модуль BACnet	Вимірювання температури з цифровим інтерфейсом BACnet	1	Підключення через BACnet до Cisco IR1101 або контролера через шлюз
Кондиціонер з підтримкою IoT	Daikin ARXF-A9 + шлюз DIII-Net	Охолодження/обігрів приміщень із віддаленим керуванням	1	Підтримка Modbus TCP або BACnet, інтеграція з Cisco IR1101 через шлюз

Закінчення таблиці 4.1

Сигналізаційна система	Ajax Hub 2 Plus	Охоронна сигналізація з передачею тривожних подій	1	Працює через Ethernet або 4G, підтримка MQTT/HTTP API для взаємодії з Cisco IR1101
Сигналізаційна система	Ajax Hub 2 Plus	Охоронна сигналізація з передачею тривожних подій	1	Працює через Ethernet або 4G, підтримка MQTT/HTTP API для взаємодії з Cisco IR1101
Автоматичне вікно з контролем	VELUX Integra + шлюз KLF 200	Автоматичне відкривання/закривання вікон	2	Керування через REST API або сухі контакти, підключення до шлюзу або I/O Cisco IR1101
Головний IoT контролер	Cisco IR1101	Центральне керування всією інфраструктурою IoT	1	Підтримка Docker, IOx, MQTT, Modbus TCP, REST API
Пожежні спринклери	Tyco ESFR25 TY9226	Автоматичне пожежогасіння	4	Активуються через електромагнітний клапан, сигнал із контролера або I/O модуля
Клапани до спринклерів	Belimo EV серія + шлюз MP-Bus/Modbus	Відкривання/закривання подачі води до спринклерів	4	Електронне керування, підтримка Modbus RTU/TCP, можливість підключення до Cisco IR1101
Кондиціонер з підтримкою IoT	Daikin ARXF-A9 + шлюз DIII-Net	Охолодження та вентиляція з підтримкою BACnet / Modbus TCP	1	Інтегрується з Cisco IR1101 через шлюз; підтримка керування та моніторингу

Таблиця 4.2 містить підбірку джерел живлення, адаптованих до потреб промислової IoT-системи, побудованої на базі Cisco IR1101. Усі джерела живлення мають захисти від короткого замикання, перенавантаження та перегріву, що підвищує загальну надійність системи. Всі пристрої сумісні з відкритими промисловими протоколами (Modbus, MQTT, REST API, LLRP, ZigBee, BACnet) і можуть бути інтегровані через Cisco IR1101 у єдину централізовану систему з гнучким управлінням, безпечним обміном даними та можливістю масштабування.

Таблиця 4.2 – Живлення IoT системи

Модель блока живлення	Вихідна напруга	Максимальний струм	Потужність	Захисти	Примітка (підходить для)
Mean Well RSP-100-24	24V DC	4.2 A	100 W	Захист від короткого замикання, перенавантаження, перегрів	Impinj Speedway R420, Cisco IR1101
Mean Well HDR-60-24	24V DC	2.5 A	60 W	Захист від КЗ, перенавантаження	Honeywell 5808W3 (шлюз), Daikin SkyAir шлюз, Belimo EV клапани
Mean Well HDR-30-24	24V DC	1.3 A	30 W	Захист від КЗ, перенавантаження	Schneider Electric STP700
Mean Well GSM60 A24-P1J	24V DC	2.5 A	60 W	Захист від КЗ, перенавантаження	VELUX Integra + шлюз KLF 200

4.2 Налаштування сервера IoT в моделі комп’ютерній мережі

Обробка даних від усіх встановлених сенсорів, виконавчих механізмів і контролерів централізовано обробляються завдяки використанню сервера IoT-пристроїв у комп’ютерній мережі. Сервер служить зв’язком між програмним забезпеченням та фізичними пристроями, забезпечуючи постійний обмін інформацією, керування обладнанням і моніторинг у режимі реального часу. Він використовує шлюзи для прийому IoT-сигналів, обробляє їх і передає їх на системи візуалізації та управління.

На сервері розгорнуто спеціалізоване програмне середовище, яке підтримує популярні протоколи взаємодії з пристроями, такі як MQTT і HTTP API. База даних використовується сервером для зберігання та аналізу даних. Це дозволяє накопичувати інформацію про події, сигнали та статуси.

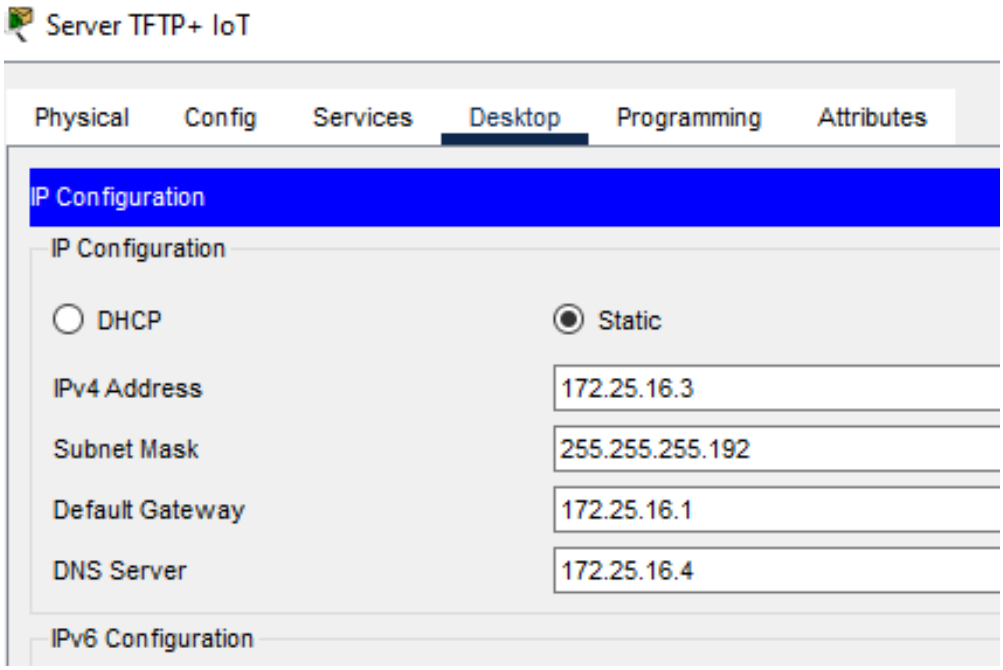


Рисунок 4.1 – Налаштування IoT серверу

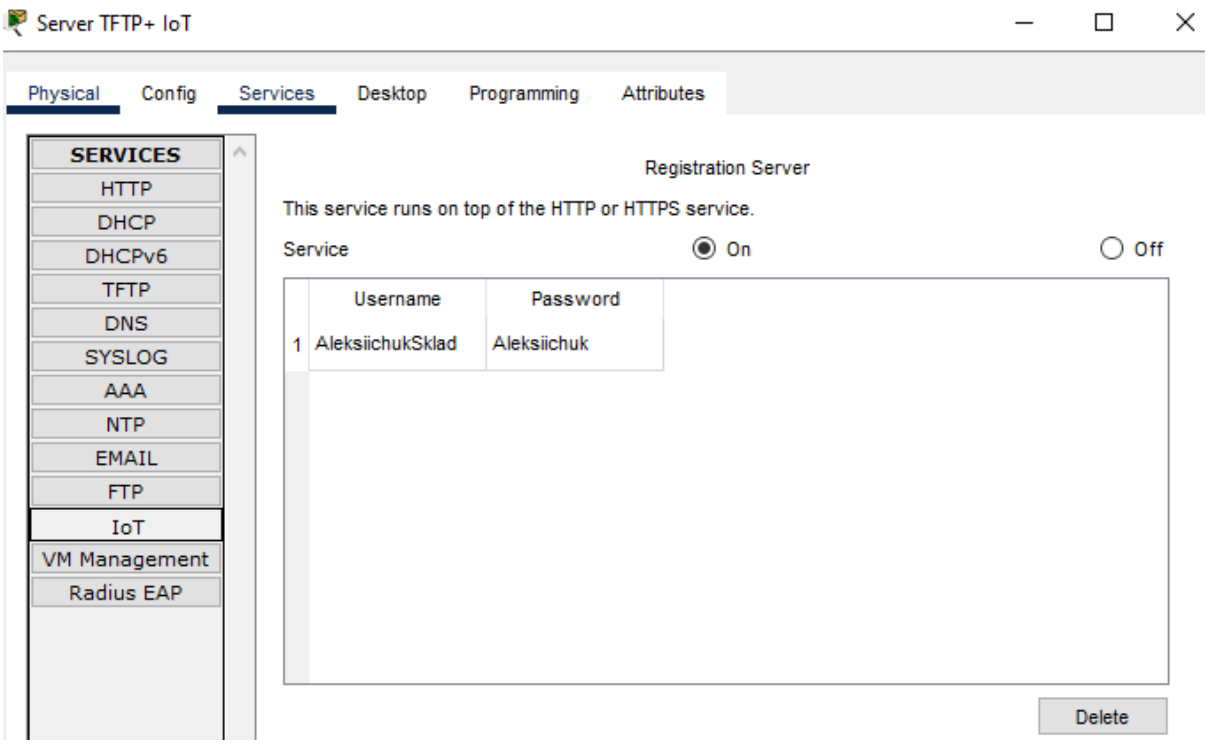


Рисунок 4.2 – Додавання головного користувача в IoT

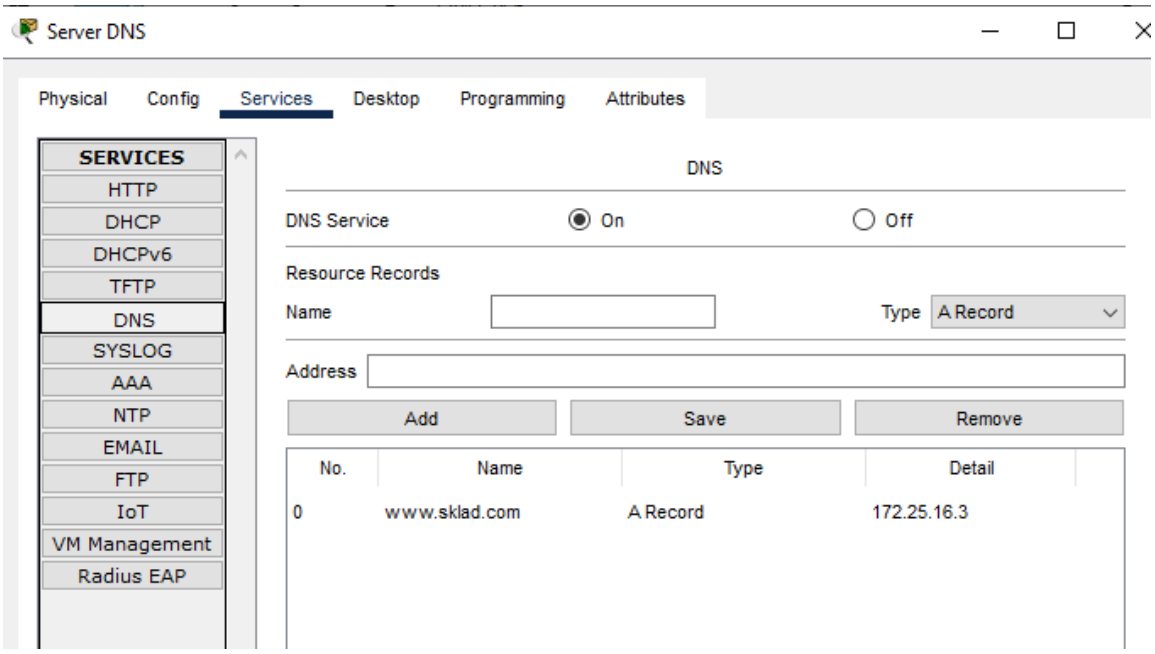


Рисунок 4.3 – Налаштування домену для IoT серверу

4.3 Налаштування протипожежної IoT системи

У системі протипожежної безпеки комп’ютерної мережі підприємства є пристрої Інтернету речей (IoT), які автоматично виявлюються та реагують на ознаки загоряння. Два основних датчики системи – датчики диму та температури – постійно спостерігають за станом навколишнього середовища. Ці сенсори повідомляють головний контролер IoT-системи, коли вони виявили дим або незвичайну температуру.

Алгоритм реагування активується після надходження сигналу і керує двома встановленими пожежними сплінклерами. Воду подають у зону ризику, і вони автоматично вмикаються, щоб знайти вогнище. Одразу після цього включається система звукового та світлового оповіщення, щоб повідомити персонал про необхідність евакуації. Сигналізація включається автоматично, створюючи звуковий фон для попередження.

Уся система працює автономно та в режимі реального часу, що дозволяє швидке виявлення пожежі, миттєве реагування та передачу даних на сервер для аналізу та журналювання подій.

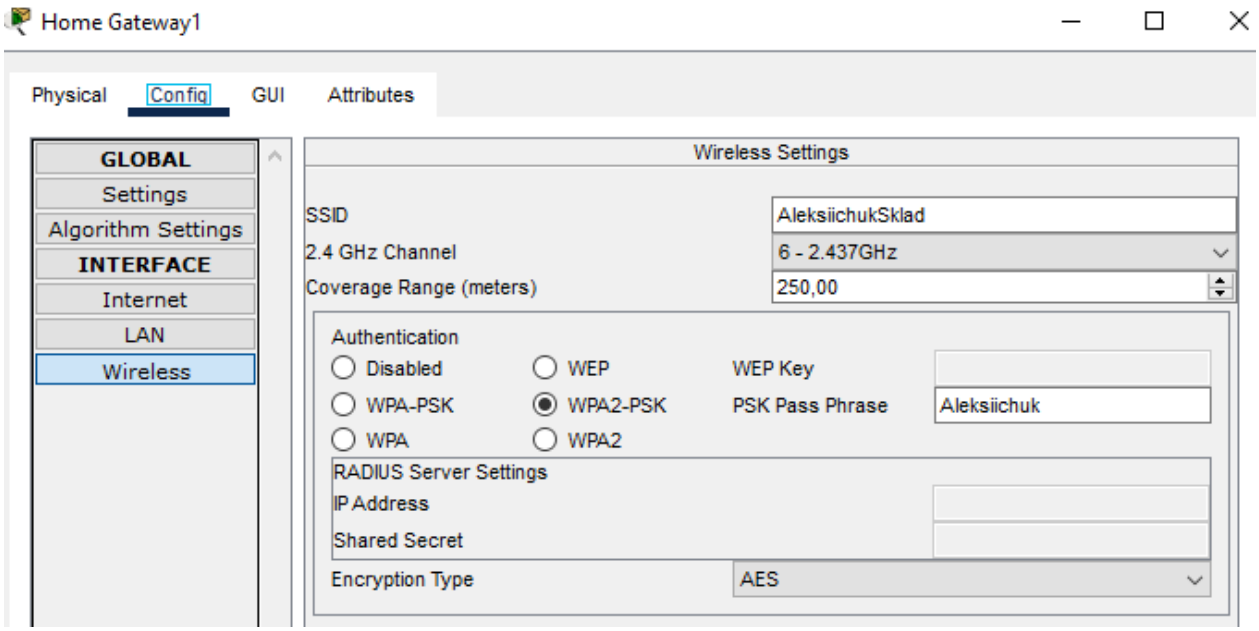


Рисунок 4.4 – Налаштування wireless Home Gateway

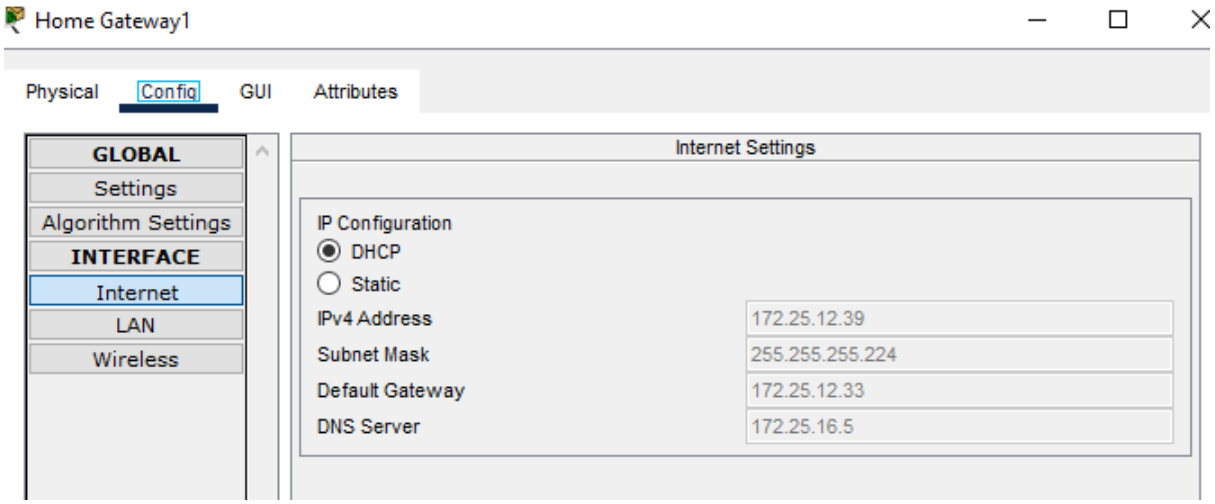


Рисунок 4.5 – Надання DHCP ip Home Gateway

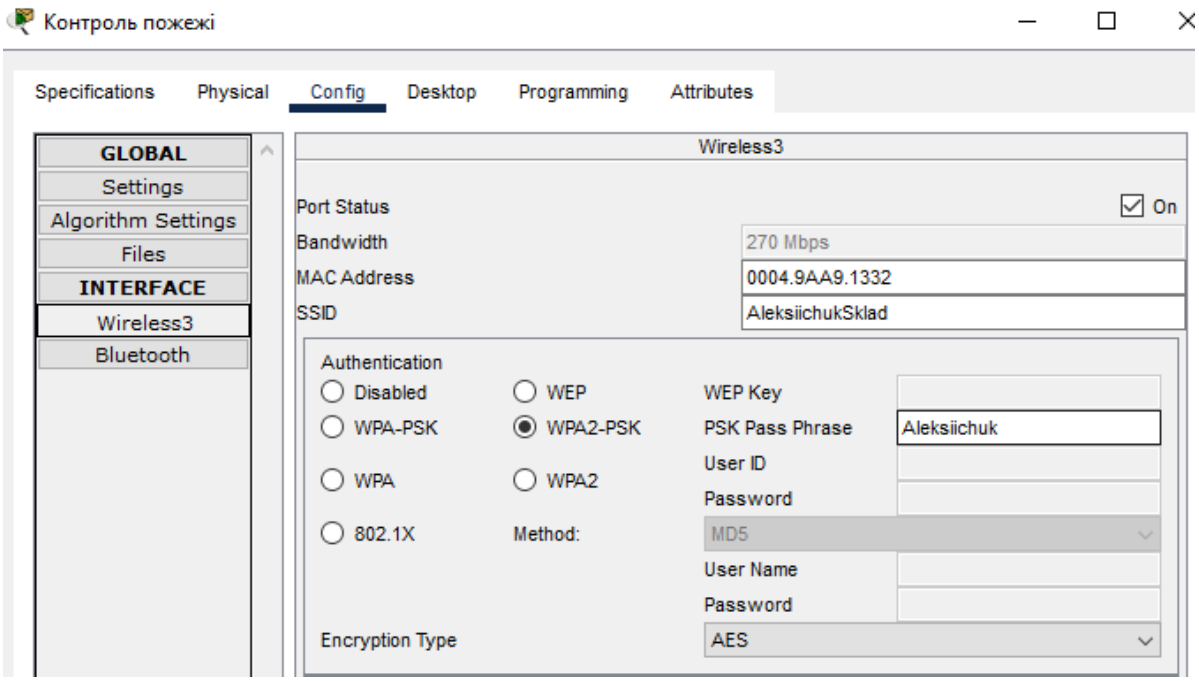


Рисунок 4.4 – Налаштування wireless плати контролера пожежі

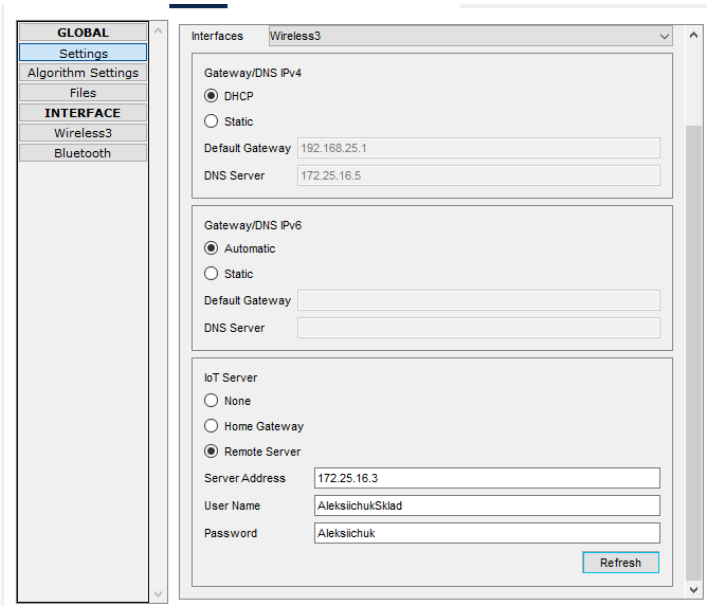


Рисунок 4.5 – Підключення контролера до IoT серверу

```
from gpio import *
from time import *
from ioeclient import *
import math

# Порти
SmokeSensor = 0     # D0
Alarm = 1           # D1
FireSprinkler1 = 2  # D2
FireSprinkler2 = 3  # D3
FireSprinkler3 = 4  # D4
TemperatureSensor = 6  # D6 (analog)

# Ініціалізація IoT
IoEClient.setup({
    "type": "FIRE_DETECTION_MINI",
    "states": [
        {"name": "Smoke", "type": "bool"},
        {"name": "Alarm", "type": "bool"},
        {"name": "Sprinklers", "type": "bool"},
        {"name": "Temperature", "type": "number", "unit": "~C", "decimalDigits": 1}
    ]
})

def main():
    pinMode(SmokeSensor, IN)
    pinMode(TemperatureSensor, IN)
    pinMode(Alarm, OUT)

    print(u" Fire Detection System Active")

    while True:
        # Зчитування температури (ADC: 0-1023 → -100°C до 100°C)
        temperature = ((analogRead(TemperatureSensor) * 200 / 1023) - 100)

        # Зчитування диму (ADC: 0-255 → 0-100%)
        smoke_value = analogRead(SmokeSensor)
        smoke_level = math.floor(smoke_value * 100 / 255)
        smoke_detected = smoke_level > 10  # детекція, якщо понад 10%

        print(u" Temp:", round(temperature, 1), u"°C | □ Smoke Level:", smoke_level, "%")

        # Реакція на дим або перегрів
        if temperature > 50 or smoke_detected:
            print(u"Пожежа! Temp:", round(temperature, 1), "Smoke:", smoke_level)
            digitalWrite(Alarm, HIGH)
            customWrite(FireSprinkler1, "1")
            customWrite(FireSprinkler2, "1")
            customWrite(FireSprinkler3, "0")
            alarm_state = True
            sprinkler_state = True
        else:
            digitalWrite(Alarm, LOW)
            customWrite(FireSprinkler1, "0")
            customWrite(FireSprinkler2, "0")
            customWrite(FireSprinkler3, "0")
            alarm_state = False
            sprinkler_state = False

        # Надсилання станів на IoT-сервер
        IoEClient.reportStates([
            smoke_detected,
            alarm_state,
            sprinkler_state,
            round(temperature, 1)
        ])

        delay(500)

if __name__ == "__main__":
    main()
```

Рисунок 4.6 - Код котроллера пожежі

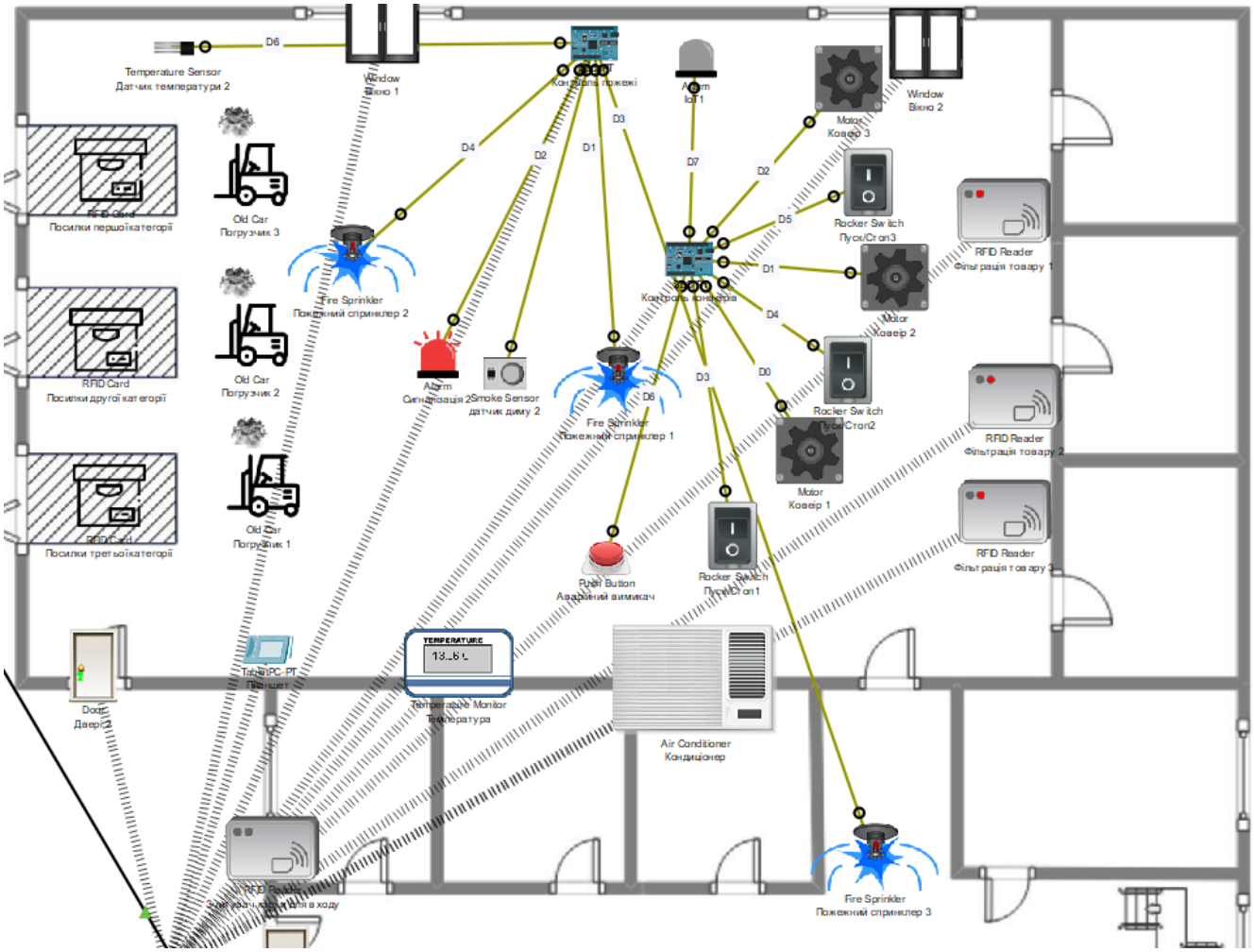


Рисунок 4.7 – Перевірка працездатності, задимлення приміщення

4.4 Налаштування IoT системи безпеки складського приміщення

Система безпеки IoT у складському приміщенні використовує RFID-технології для контролю доступу. На вході до складу встановлено RFID-зчитувач, який автоматично ідентифікує працівників за допомогою RFID-карток, розроблених за їхніми індивідуальними потребами. Після того, як картка підноситься до зчитувача, код передається на центральний контролер системи, який перевіряє, чи відповідає він дозволеним даним у базі даних.

Система дозволяє доступ до приміщення, якщо RFID-картка визнана дійсною. Якщо код системи виявляється неправильним або відсутнім, автоматично включається сигналізація. Це включає світлову та звукову тривогу, щоб повідомити охоронним персоналам про спробу несанкціонованого доступу.

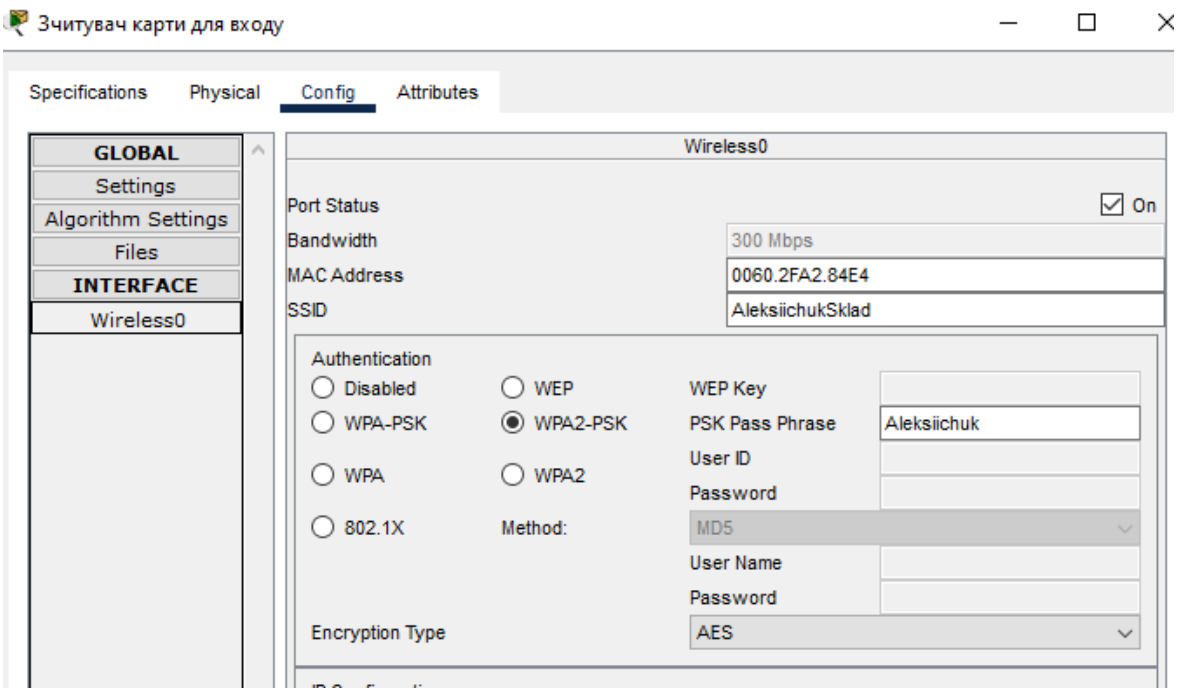


Рисунок 4.8 – Налаштування Wireless для RFID зчитувача

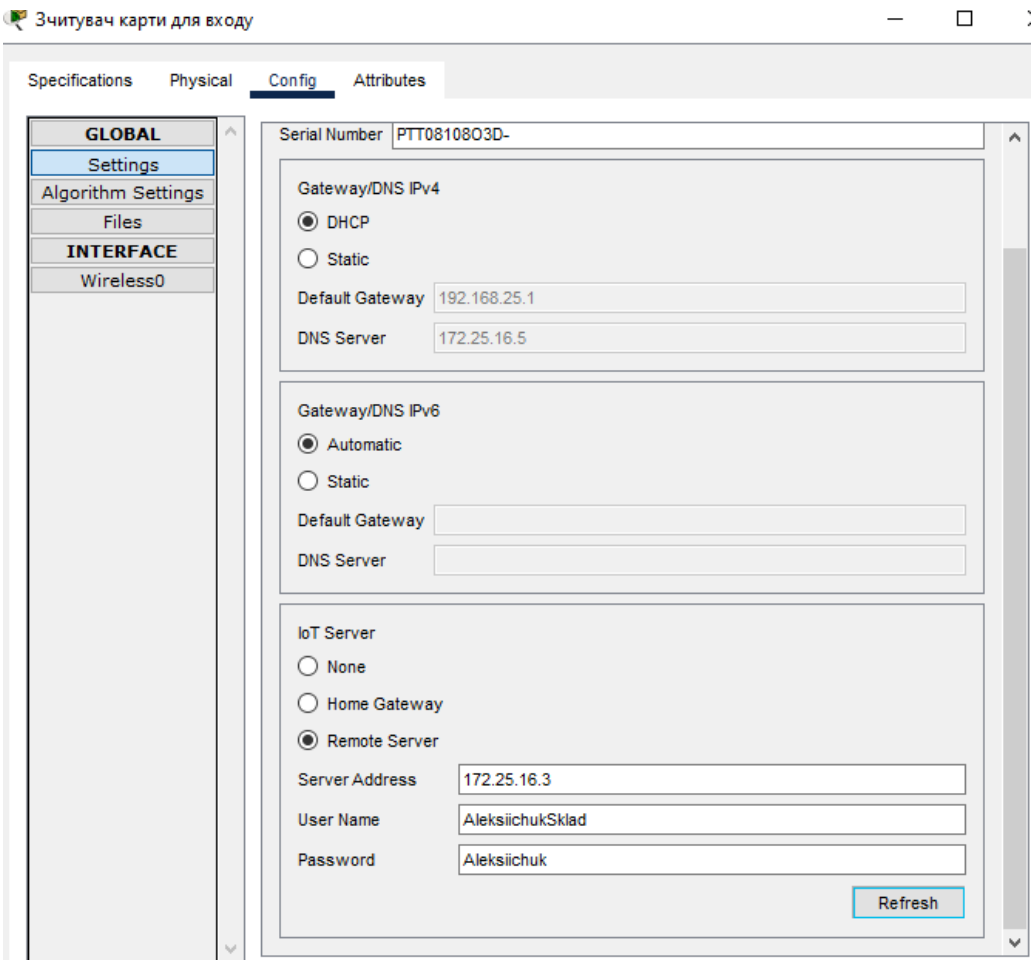


Рисунок 4.9 – Підключаємо RFID зчитувач до IoT серверу

Планшет

Physical | Config | Desktop | Programming | Attributes

Web Browser

< > URL http://172.25.16.3/conditions.html Go Stop

IoT Server - Device Conditions

Home | Conditions | Editor | Log Out

Actions	Enabled	Name	Condition	Actions
Edit Remove	Yes	RFID відкриття дверей	Зчитувач карти для входу Status is Valid	Set Двері 1 Lock to Unlock Set Двері 2 Lock to Unlock
Edit Remove	Yes	RFID зачинені двері	Match any: • Зчитувач карти для входу Status is Invalid • Зчитувач карти для входу Status is Waiting	Set Двері 1 Lock to Lock Set Двері 2 Lock to Lock
Edit Remove	Yes	RFID ключ дверей	Зчитувач карти для входу Card ID is between 1 and 25	Set Зчитувач карти для входу Status to Valid
Edit Remove	Yes	RFID неправильна карта	Зчитувач карти для входу Card ID > 25	Set Зчитувач карти для входу Status to Invalid
Edit Remove	Yes	Тривога	Зчитувач карти для входу Status is Invalid	Set Сигналізація On to true
Edit Remove	Yes	Тривога 2	Зчитувач карти для входу Status is Valid	Set Сигналізація On to false

Рисунок 4.10 – Готові сценарії для системи безпеки

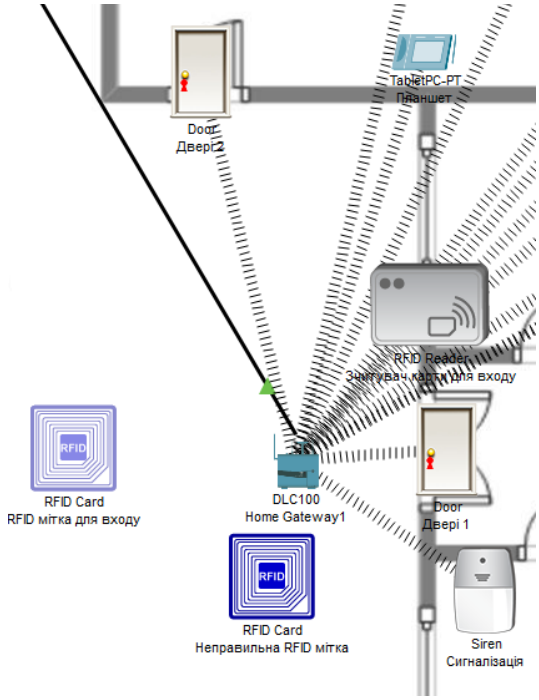


Рисунок 4.11 – Перевірка системи безпеки, режим спокою

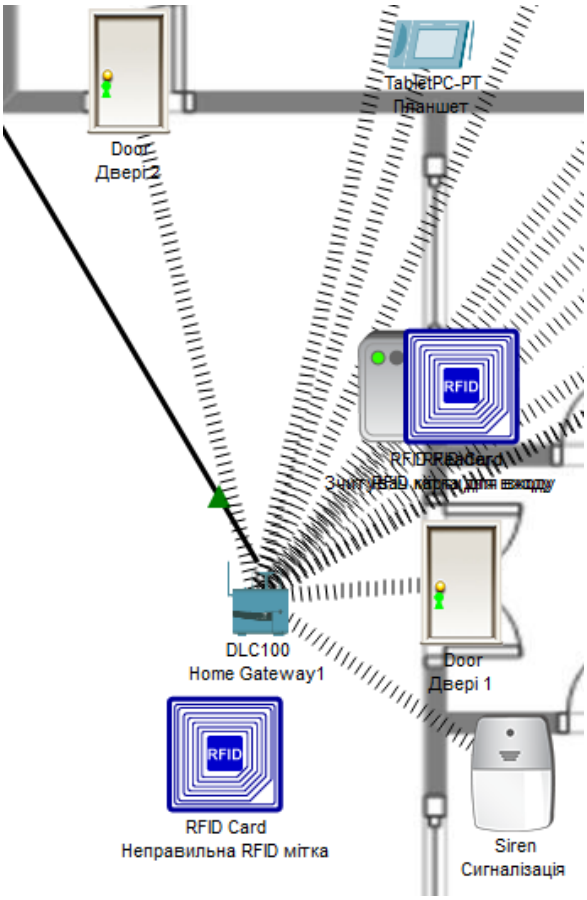


Рисунок 4.12 – Перевірка системи, зчитуємо правильну RFID мітку

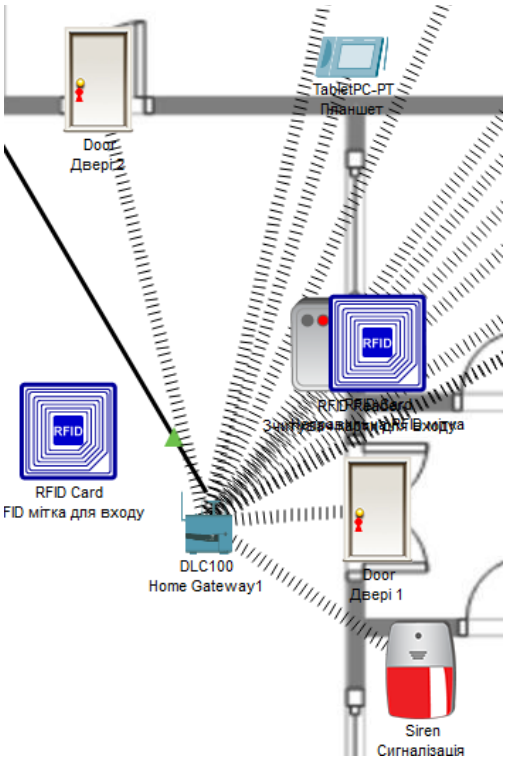


Рисунок 4.13 – Перевірка системи, зчитуємо неправильну RFID мітку

4.5 Налаштування клімат контролю

У складському приміщенні та технічних зонах корпоративної мережі встановлено систему клімат-контролю, яка базується на Інтернеті речей (IoT). Забезпечення стабільного мікроклімату для зберігання товарів, обладнання та персоналу є основною метою впровадження.

Датчики температури та централізований кондиціонер у системі контролюються контролером. Датчик температури в режимі реального часу постійно інформує контролера про стан повітря. Контролер автоматично надсилає команду на активацію або деактивацію кондиціонера, якщо температура перевищує або опускається нижче визначеного порогу.

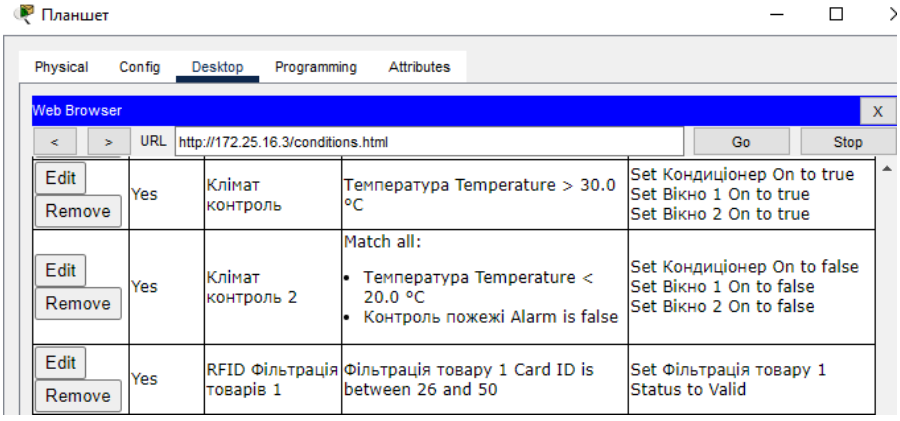


Рисунок 4.14 – Реалізація сценаріїв клімат контролю

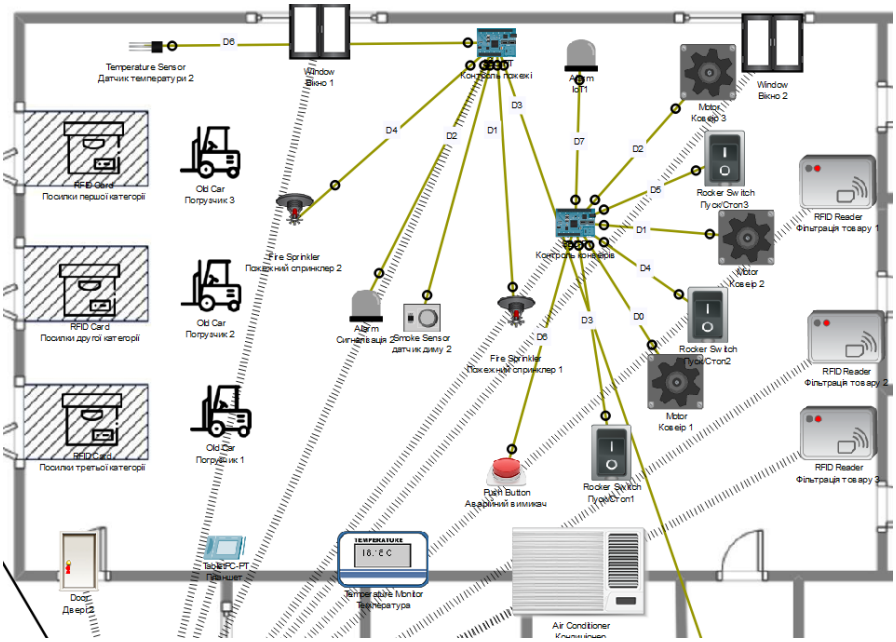
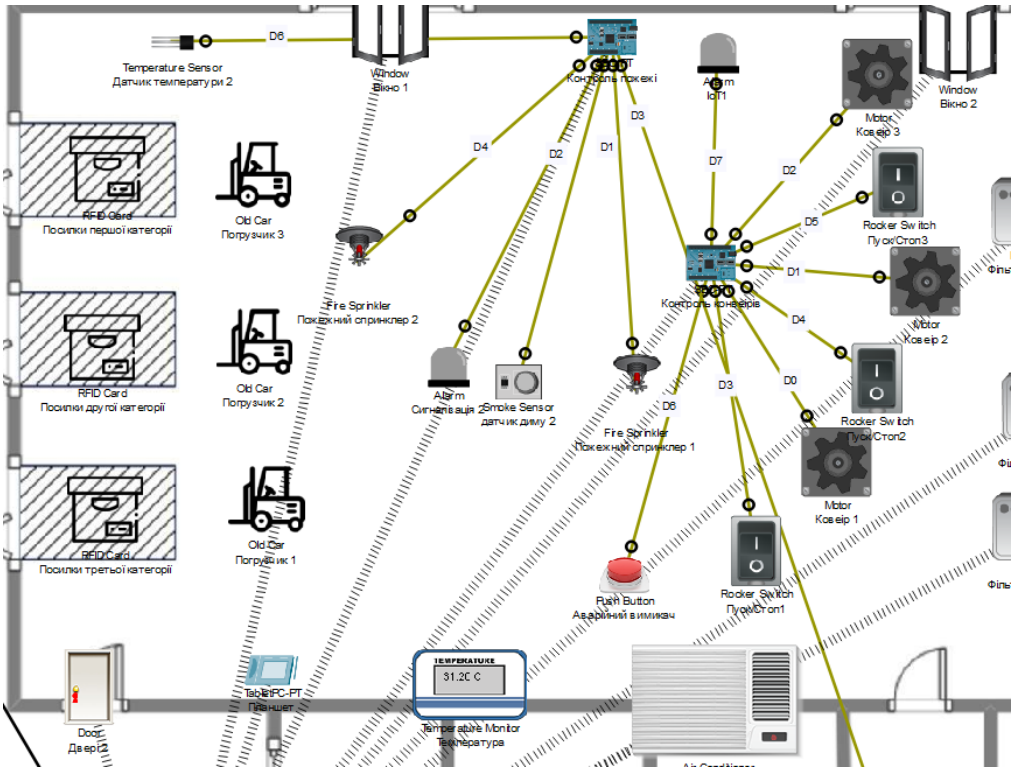


Рисунок 4.15 – Перевірка працездатності, звичайний режим



4.16 – Перевірка працездатності, в приміщені висока температура

4.6 Налаштування IoT сортування

Впровадження автоматизованої логістичної схеми з трьома навантажувачами є частиною проекту IoT-системи сортування. Ці навантажувачі переміщують товари до автоматизованих конвеєрів, де RFID-технологія ідентифікує предмети.

Кожен предмет має RFID-мітку, яку може прочитати відповідний RFID-зчитувач, встановлений уздовж транспортної лінії. Після зчитування мітки система визначає місце зберігання товару на складі. Центральний IoT-контролер керує всією логікою маршрутизації. Він обробляє дані та надсилає відповідні сигнали виконавчим механізмам на конвеєрі.

```python
from gpio import *
from time import *
from ioeclient import *

# Ports configuration
Motor1 = 0  # A0
Motor2 = 1  # A1
Motor3 = 2  # A2

Switch1 = 3  # D3
Switch2 = 4  # D4
Switch3 = 5  # D5

EmergencyStop = 6  # D6
Alarm = 7          # D7

# Motor speed
MOTOR_OFF = 0
MOTOR_SPEED = 255

# IoT client setup
IoEClient.setup({
    "type": "MOTOR_CONTROL_SYSTEM",
    "states": [
        {"name": "Motor1", "type": "bool"},
        {"name": "Motor2", "type": "bool"},
        {"name": "Motor3", "type": "bool"},
        {"name": "Switch1", "type": "bool"},
        {"name": "Switch2", "type": "bool"},
        {"name": "Switch3", "type": "bool"},
        {"name": "EmergencyStop", "type": "bool"},
        {"name": "Alarm", "type": "bool"}
    ]
})

def main():
    pinMode(Switch1, IN)
    pinMode(Switch2, IN)
    pinMode(Switch3, IN)
    pinMode(EmergencyStop, IN)
    pinMode(Alarm, OUT)

    alarm_active = False
    last_emergency_state = False

    print("Motor control system initialized.")

    while True:
        emergency_pressed = digitalRead(EmergencyStop) == HIGH

        # Toggle alarm on button press (edge detection)
        if emergency_pressed and not last_emergency_state:
            alarm_active = not alarm_active
            if alarm_active:
                print("Alarm toggled to ON.")
            else:
                print("Alarm toggled to OFF.")
        last_emergency_state = emergency_pressed

        # Update alarm output
        digitalWrite(Alarm, HIGH if alarm_active else LOW)

        # Motor control
        if alarm_active:
            motor1_state = MOTOR_OFF
            motor2_state = MOTOR_OFF
            motor3_state = MOTOR_OFF
            sw1 = False
            sw2 = False
            sw3 = False
            print("Alarm active. Motors disabled.")
        else:
            sw1 = digitalRead(Switch1) == HIGH
            sw2 = digitalRead(Switch2) == HIGH
            sw3 = digitalRead(Switch3) == HIGH

            motor1_state = MOTOR_SPEED if sw1 else MOTOR_OFF
            motor2_state = MOTOR_SPEED if sw2 else MOTOR_OFF
            motor3_state = MOTOR_SPEED if sw3 else MOTOR_OFF

        analogWrite(Motor1, motor1_state)
        analogWrite(Motor2, motor2_state)
        analogWrite(Motor3, motor3_state)

        IoEClient.reportStates([
            motor1_state != MOTOR_OFF,
            motor2_state != MOTOR_OFF,
            motor3_state != MOTOR_OFF,
            sw1,
            sw2,
            sw3,
            emergency_pressed,
            alarm_active
        ])

        delay(100)


if __name__ == "__main__":
    main()
```

Рисунок 4.17 – Код головного контролера сортування

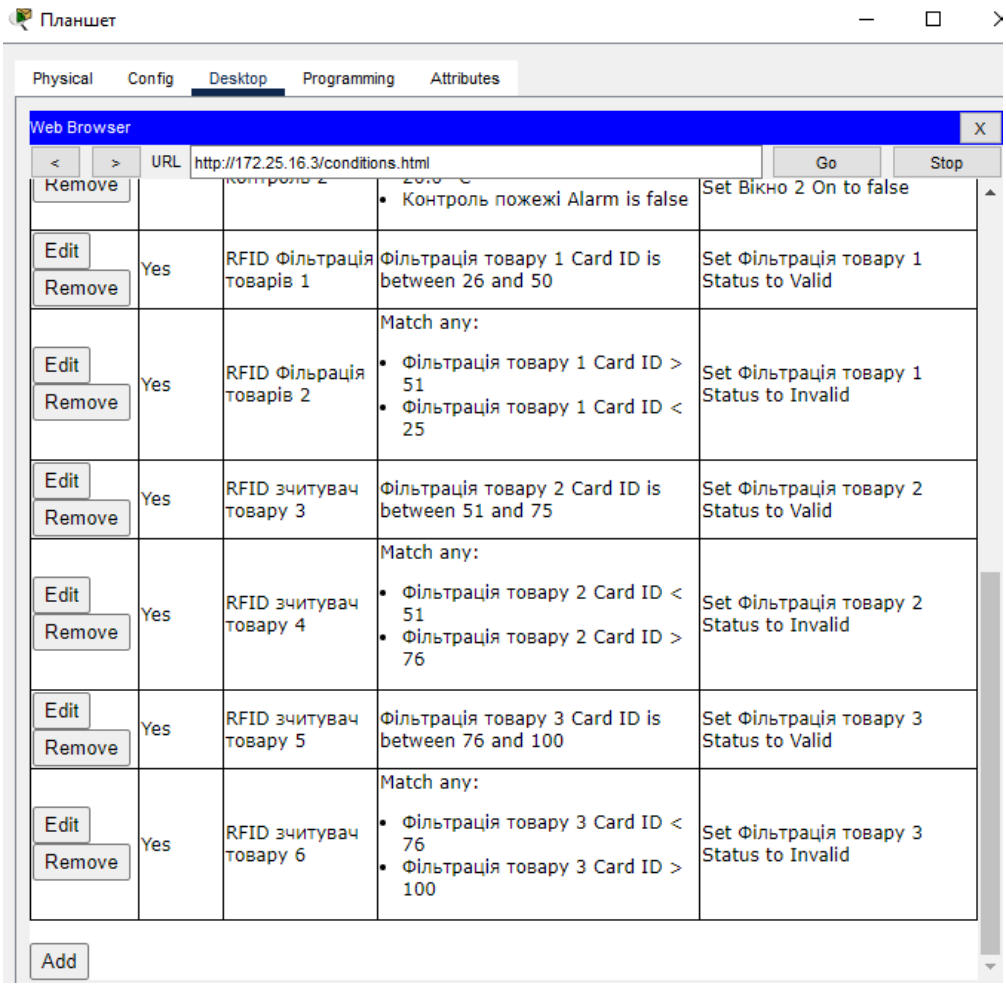


Рисунок 4.18 – Реалізація правил сортування

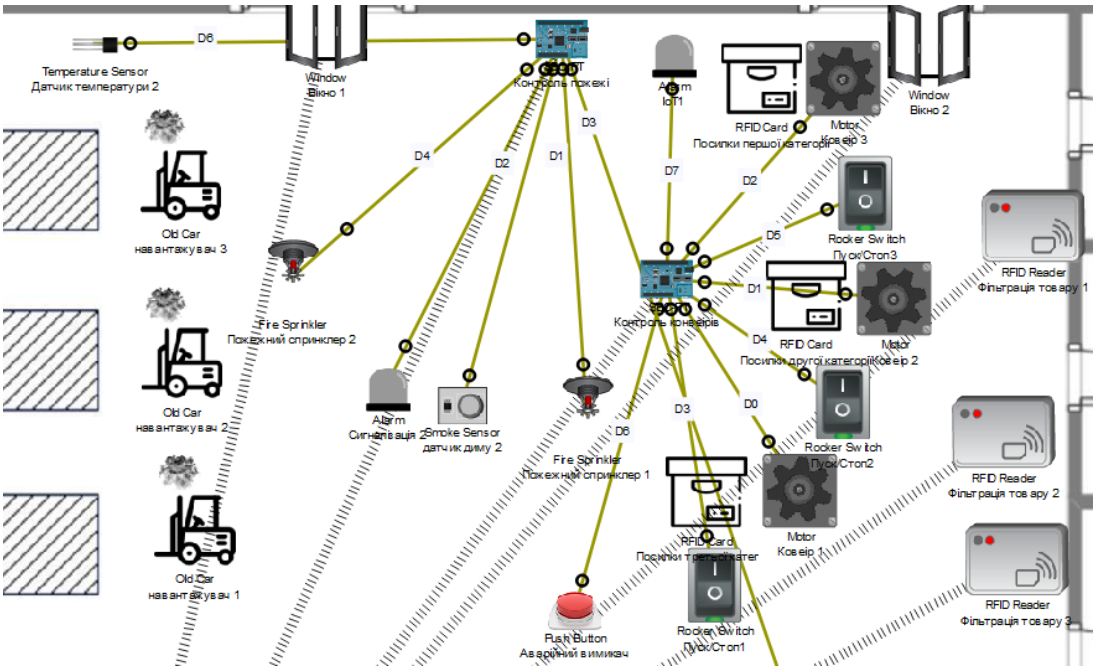


Рисунок 4.19 – Перевірка працездатності – перенесення товарів до ковеерів

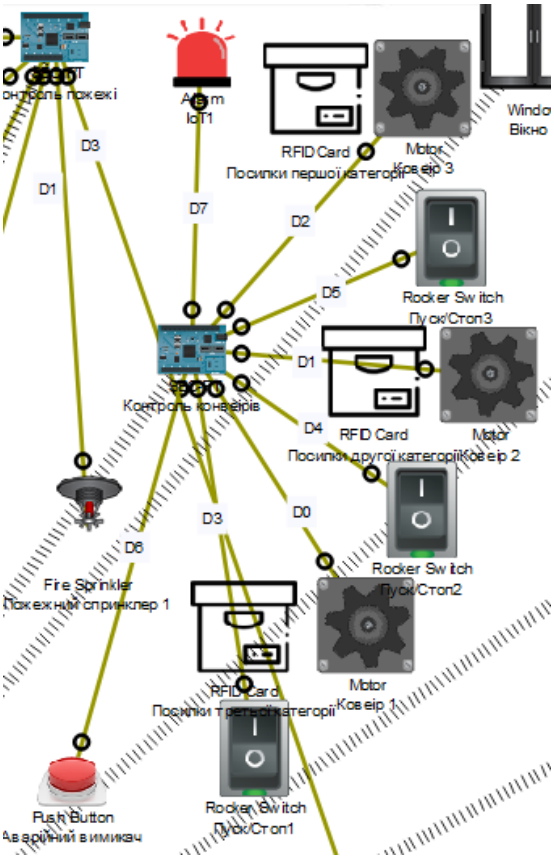


Рисунок 4.20 – Перевірка працездатності, аварійне виключення конвеєрів

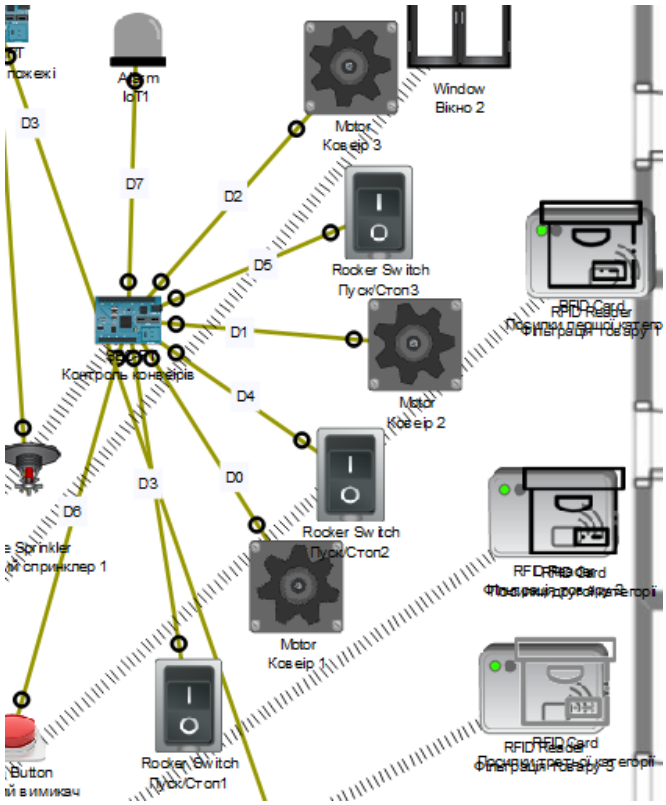


Рисунок 4.21 – Перевірка працездатності, правильне сортування товару.

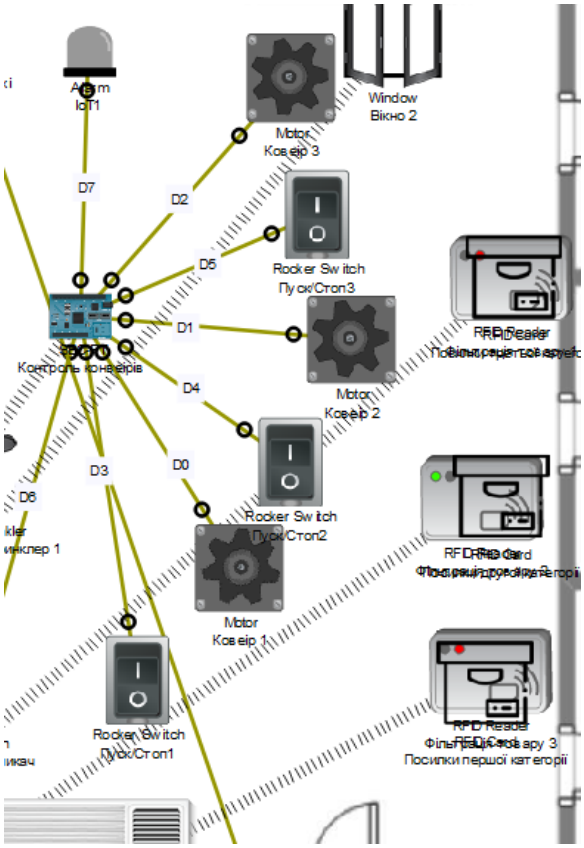


Рисунок 4.22 – Перевірка працездатності, неправильне сортування товару

ВИСНОВКИ

Комп’ютерна мережа логістичної компанії, розроблена в рамках цієї роботи, забезпечує ефективну і безпечну взаємодію між різними підрозділами підприємства, включно зі складським комплексом, відділом логістики, фінансовим та IT-відділами. Завдяки застосуванню сучасних технологій VLAN, маршрутизації та систем безпеки, мережа оптимізує обмін інформацією, прискорює обробку замовлень і контролює доступ до критичних ресурсів.

Маршрутизатори були налаштовані за допомогою протоколів маршрутизації, таких як EIGRP і RIP. Ці протоколи забезпечували ефективний обмін маршрутною інформацією, підтримку масштабованості мережі та стійкість до відмов. NAT і DHCP дозволили автоматизувати процес отримання IP-адрес і забезпечити захист внутрішньої мережі при виході в Інтернет. Крім того, безпека адміністрування покращилася завдяки впровадженню системи аутентифікації AAA, яка контролює доступ до мережевих пристроїв.

Особлива увага була приділена впровадженню IoT-рішень для спрощення виробничих і складських процесів. Датчики температури та диму, пожежні сплінклери, система контролю доступу RFID, клімат-контроль і автоматизоване сортування товарів на конвеєрах є частиною системи.

Загалом, мережа, яка була створена, є масштабованою, надійною та відповідає сучасним стандартам інформаційних технологій. Забезпечуючи стабільність роботи підприємства, вона дозволяє ефективно керувати ресурсами та дозволяє впроваджувати інноваційні технології, які підвищують продуктивність і безпеку. Виконана робота показує комплексний підхід до проектування та налаштування корпоративних мереж, який враховує сучасні технологічні вимоги та особливості діяльності підприємства.

ПЕРЕЛІК ПОСИЛАНЬ

1. Аулін В.В. Формування логістичної інформаційної системи ефективного управління транспортними і виробничими підприємствами / В.В. Аулін // Економіка транспортного комплексу. – 2022. – № 39. – С. 122–129. – [Електронний ресурс]. – Режим доступу: https://surli.cc/diisfw (дата звернення 17.05.2025).

2. Атестація здобувачів вищої освіти. Методичні рекомендації до виконання кваліфікаційної роботи бакалавра здобувачам галузі знань 12 Інформаційні технології спеціальності 124 Комп'ютерна інженерія / Л.І. Цвіркун, С.М. Ткаченко, Я.В. Панферова, Д.О. Бешта, Л.В. Бешта – Д.: НТУ «ДП», 2025. – 65

3. Бублєй В.Ю. Формування логістичної інформаційної системи на підприємстві : дипломна робота на здобуття освітньо-кваліфікаційного рівня магістра: спец. 073 «Менеджмент» / В.Ю. Бублєй. – Харків : ХНЕУ ім. С. Кузнеця, 2019. – [Електронний ресурс]. – Режим доступу: https://surl.li/ldzdln (дата звернення 13.05.2025).

4. Аулін В.В. Формування логістичної інформаційної системи ефективного управління транспортними і виробничими підприємствами / В.В. Аулін // Економіка транспортного комплексу. – 2022. – № 39. – С. 122–129. – [Електронний ресурс]. – Режим доступу:https://surl.lu/zztnis (дата звернення 12.05.2025).

5. Колешня Я.О. Цифрова логістика : навч. посіб. для здобувачів ступеня магістра за освітньою програмою «Логістика» спеціальності 073 Менеджмент / Я.О. Колешня ; М-во освіти і науки України, КПІ ім. Ігоря Сікорського. – Київ : КПІ ім. Ігоря Сікорського, 2022. – 63 с. – [Електронний ресурс]. – Режим доступу: https://surl.li/bimawd (дата звернення 17.05.2025).

ДОДАТОК А

Текст програми налаштування компонентів мережі комп’ютерної системи

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

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ НАЛАШТУВАННЯ МЕРЕЖІ КОМП’ЮТЕРНОЇ СИСТЕМИ

Текст програми

804.02070743.25018-01 12 01

Листів 7

2025

АНОТАЦІЯ

Ця програма містить частини конфігураційного коду, які призначені для налаштування основних компонентів мережевої інфраструктури логістичної компанії. Вона підтримує автоматизацію налаштувань критично важливих мережевих сервісів, таких як DHCP, AAA та NAT, що забезпечує стабільне підключення до IoT-пристроїв, встановлених у складі та на транспорті.

Крім того, програму можна використовувати для створення VPN-з’єднань та захищеного доступу до віддалених логістичних об’єктів. Це необхідно для централізованого моніторингу, відстеження вантажів, контролю температури, руху товарів і забезпечення безпеки на всіх етапах логістичного ланцюга.

ЗМІСТ

Налаштування роутера LAN1_R1_Aleksiichuk

```
hostname LAN1_R1_Aleksiichuk
!
!
!
enable secret 5
$1$mERr$Jp2nTPvFNDw/o9DcIlw891
!
!
ip dhcp excluded-address 172.25.16.1
172.25.16.5
ip dhcp excluded-address 172.25.16.33
172.25.16.38
ip dhcp excluded-address 172.25.16.65
172.25.16.70
ip dhcp excluded-address 172.25.16.129
172.25.16.134
ip dhcp excluded-address 172.25.16.193
172.25.16.198
!
ip dhcp pool SYSADMN
network 172.25.16.0 255.255.255.192
default-router 172.25.16.1
dns-server 172.25.16.5
ip dhcp pool Neteng
network 172.25.16.64 255.255.255.192
default-router 172.25.16.65
dns-server 172.25.16.5
ip dhcp pool SpIoT
network 172.25.16.128 255.255.255.192
default-router 172.25.16.129
dns-server 172.25.16.5
ip dhcp pool Supp1
network 172.25.16.192 255.255.255.240
default-router 172.25.16.193
dns-server 172.25.16.5
!
!
aaa new-model
!
aaa authentication login AAA group radius
!
!
!
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
!
license udi pid CISCO2911/K9 sn
FTX15246877-
!
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface Loopback0
ip address 8.8.8.8 255.255.255.0
!
interface GigabitEthernet0/0
no ip address
duplex auto
speed auto
!
interface GigabitEthernet0/0.10
encapsulation dot1Q 10
ip address 172.25.16.1 255.255.255.192
ip nat inside
!
interface GigabitEthernet0/0.20
encapsulation dot1Q 20
ip address 172.25.16.65 255.255.255.192
ip nat inside
!
interface GigabitEthernet0/0.30
encapsulation dot1Q 30
ip address 172.25.16.129 255.255.255.192
ip nat inside
!
interface GigabitEthernet0/0.40
encapsulation dot1Q 40
ip address 172.25.16.193 255.255.255.240
ip nat inside
!
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
!
```

```
interface GigabitEthernet0/2
no ip address
duplex auto
speed auto
!
interface Serial0/1/0
bandwidth 256
ip address 10.25.16.5 255.255.255.252
ip ospf cost 10
!
interface Serial0/1/1
ip address 10.25.16.29 255.255.255.252
ip ospf cost 5
!
interface Serial0/2/0
ip address 10.25.16.21 255.255.255.252
!
interface Serial0/2/1
no ip address
clock rate 2000000
!
interface Serial0/3/0
no ip address
clock rate 2000000
!
interface Serial0/3/1
no ip address
clock rate 2000000
!
interface Vlan1
no ip address
shutdown
!
router eigrp 100
passive-interface GigabitEthernet0/0
passive-interface GigabitEthernet0/1
passive-interface GigabitEthernet0/2
network 172.0.0.0 0.255.255.255
network 10.0.0.0
network 30.0.0.0
!
ip classless
!
ip flow-export version 9
!
!
ip access-list standard NAT_ACL
permit any
!
!
radius server 172.25.16.2
address ipv4 172.25.16.2 auth-port 1645
key cisco
!
!
!
line con 0
password MarkoAdmin123
!
line aux 0
!
line vty 0 4
password CiscoMarko
login authentication AAA
!
!
!

End
```

Налаштування комутатора LAN1_S1_Aleksiichuk

```
hostname LAN1_S1_Aleksiichuk
!
enable secret 5
$1$mERr$Jp2nTPvFNDw/o9DcIlw891
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
switchport access vlan 30
!
interface FastEthernet0/2
switchport access vlan 30
!
interface FastEthernet0/3
switchport access vlan 30
!
interface FastEthernet0/4
switchport access vlan 30
!
interface FastEthernet0/5
switchport access vlan 30
!
interface FastEthernet0/6
switchport access vlan 30
!
interface FastEthernet0/7
switchport access vlan 30
!
interface FastEthernet0/8
switchport access vlan 30
!
interface FastEthernet0/9
switchport access vlan 30
!
interface FastEthernet0/10
switchport access vlan 30
!
interface FastEthernet0/11
switchport access vlan 40
!
interface FastEthernet0/12
switchport access vlan 40
!
interface FastEthernet0/13
switchport access vlan 40
!
interface FastEthernet0/14
switchport access vlan 40
!
interface FastEthernet0/15
switchport access vlan 40
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
switchport mode trunk
!
interface FastEthernet0/21
switchport mode trunk
!
interface FastEthernet0/22
switchport mode trunk
!
interface FastEthernet0/23
switchport mode trunk
!
interface FastEthernet0/24
switchport mode trunk
!
interface GigabitEthernet0/1
switchport mode trunk
!
interface GigabitEthernet0/2
switchport mode trunk
!
interface Vlan1
no ip address
shutdown
!
!
!
!
line con 0
password MarkoAdmin123
login
!
```

```
line vty 0 4
password CiscoMarko
login
.
```

```
line vty 5 15
login
```