Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Навчально-науковий
інститут електроенергетики
(інститут)

Факультет інформаційних технологій
(факультет)
Кафедра інформаційних технологій та комп'ютерної інженерії
(повна назва)

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня бакалавра

здобувача Литвиненко Діани Сергіївни
(ПІБ)
академічної групи 123-21-1
(шифр)
спеціальності 123 Комп'ютерна інженерія
(код і назва спеціальності)

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

на тему «Комп'ютерна система крамниць музичних інструментів з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі»
(назва за наказом ректора)

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	проф. Цвіркун Л.І.			
Спеціальної частини	проф. Цвіркун Л.І.			
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 Литвиненко Д.С. **академічної групи** 123-21-1
(прізвище та ініціали) (шифр)

спеціальності 123 «Комп'ютерна інженерія»

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

на тему «Комп'ютерна система крамниць музичних інструментів з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі»

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

Розділ	Зміст	Термін виконання
Стан питання і постановка завдання	На основі матеріалів виробничих практик, інших науково-технічних джерел показати актуальність завдання, сформулювати мету та задачі виконання кваліфікаційної роботи	10.02.2025
Розробка апаратної частини	Сформулювати найменування й призначення комп'ютерної системи, висунути технічні вимоги до неї. Виконати технічне проєктування апаратної частини комп'ютерної системи з необхідними інженерними розрахунками	20.04.2025
Розробка корпоративної мережі	Розрахувати й розподілити адреси вузлів комп'ютерної системи, виконати налаштування корпоративної мережі, перевірити роботу системи розробити заходи з обмеження доступу до даних системи	07.05.2025
Розробка компонента системи	Виконати налаштування та керування розумними пристроями КС	31.05.2025

Завдання видано _____ проф. Цвіркун Л.І.
(підпис керівника) (прізвище, ініціали)

Дата видачі 25.02.2025

Дата подання до екзаменаційної комісії _____

Прийнято до виконання _____ Литвиненко Д.С.

РЕФЕРАТ

БЕЗПЕКА, КРАМНИЦЯ, КОМПЛЕКС, КОНТРОЛЬ, КОРПОРАТИВНА МЕРЕЖА, СИСТЕМА

Пояснювальна записка: 72 с., 32 рис., 12 табл., 1 дод., 11 джерел.

Об’єкт вивчення − комп’ютерна система крамниць музичних інструментів з опрацюванням побудови, налаштуванням корпоративної мережі та безпеки корпоративної мережі.

Мета роботи − створення комп’ютерної системи крамниць музичних інструментів.

Здійснено розробку комп’ютерної системи крамниць музичних інструментів з опрацюванням побудови, безпеки та налаштуванням корпоративної мережі. Також у побудові схеми необхідно використати технологію VPN для захисту даних.

Система виконана відкритою і дозволяє здійснювати технічну і програмну модернізацію системи, а так само забезпечує виконання наступних функцій:

− швидкий обмін інформацією;

− збільшення надійності зберігання, обробки та передавання інформації;

− полегшення роботи у системі.

Розробка комп’ютерної мережі виконана відповідно до завдання на дипломну роботу бакалавра.

Розроблена схема мережі реалізована у вигляді моделі на симуляторі Cisco Packet Tracer і перевірена її робота.

Результати перевірки у вигляді таблиць, графіків описані і наводяться у пояснювальній записці або додатку.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

КМ – комп’ютерна мережа;

VPN – мережа VPN;

LAN – локальна обчислювальна мережа, ЛВС;

КС КМІ – комп’ютерна система крамниць музичних інструментів;

Cisco Packet Tracer – це багатофункціональна програма моделювання мереж;

DNS-сервер, Domain name system - додаток, призначений для відповідей на DNS-запити за відповідним протоколом;

VLAN – Virtual Local Area Network — віртуальна локальна комп'ютерна мережа;

TCP/IP – набір протоколів мережі Інтернет;

Ethernet-LocalAreaNetwork – з'єднує кілька різних пристроїв, розташованих поруч;

IP-адреса – унікальний ідентифікатор комп'ютера локальної мережі або мережі Інтернет;

PC – персональний комп’ютер;

DHCP – протокол динамічної настройки вузла;

ВСТУП

Сьогодні комп'ютерні мережі стали невід'ємною частиною діяльності майже кожного підприємства, забезпечуючи зв'язок як між співробітниками в межах одного офісу чи будівлі, так і між командами, розташованими в різних містах і країнах. Ефективне управління сучасним підприємством неможливе без налагодженого контролю за інформаційними потоками та оперативного координування роботи всіх підрозділів і співробітників.

Більшість компаній, незалежно від їхньої сфери діяльності, вже використовують комп'ютерну техніку та офісне обладнання. Однак, якщо процес їхнього придбання та впровадження відбувався без чіткого планування, це може призвести до зниження загальної ефективності та неповноти інформаційної інфраструктури. Крім того, у багатьох існуючих мережах питання захисту інформації не є першочерговим.

Важливо розуміти, що будь-яка організація являє собою систему взаємопов'язаних структурних підрозділів, кожен з яких має свої особливості. Ці підрозділи об'єднані функціональними зв'язками та обміном інформацією, де кожен виконує свою роль у загальному бізнес-процесі. Крім того, ці внутрішні компоненти також взаємодіють із зовнішніми системами, і ця взаємодія може бути як інформаційною, так і функціональною.

Зі ростом і розвитком кожної організації її керівництво прагне створити максимально гнучку та ефективну систему управління мережею всього підприємства та його окремих підрозділів. Особливо важливим є правильне вирішення цих питань для компаній з численними віддаленими філіями та підприємствами, оскільки це сприяє успішному управлінню, скороченню часових і фінансових витрат. Міжнародний досвід великих корпорацій та компаній підтверджує, що оптимальним рішенням є створення єдиної інформаційної системи, яка базується на корпоративній мережі.

У сучасному світі, де обсяги інформації зростають експоненціально, ефективна взаємодія між банківськими установами, торговельними компаніями, державними органами та іншими організаціями практично неможлива без використання сучасних комп'ютерів та швидкісних комп'ютерних мереж. В умовах глобальної економіки навіть хвилинна затримка в передачі критично важливих даних може призвести до серйозних фінансових втрат, тому надійні та швидкі комп'ютерні мережі є життєво необхідними для сучасних організацій.

Сьогодні концепція динамічного адміністрування є особливо актуальною в умовах зростаючої складності інформаційних систем, поширення хмарних технологій та збільшення кількості мобільних пристроїв. Сучасні системи динамічного адміністрування часто включають елементи штучного інтелекту та машинного навчання для більш глибокого аналізу поведінки користувачів та автоматизованого прийняття рішень щодо оптимізації продуктивності та безпеки. Інструменти моніторингу в реальному часі, автоматизовані системи оповіщення та самовідновлення стають ключовими компонентами сучасних рішень динамічного адміністрування, забезпечуючи високий рівень доступності та якості IT-сервісів. В умовах географічно розподілених команд та віддаленої роботи, ефективне динамічне адміністрування є критично важливим для підтримки безперервності бізнесу та продуктивності співробітників.

Метою дослідження є створення комп’ютерної системи крамниць музичних інструментів з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі.

Практичне значення цього дослідження полягає в тому, що розроблена комп'ютерна система для магазинів музичних інструментів, яка включає детальне проектування, налаштування та заходи безпеки корпоративної мережі, є готовим рішенням для впровадження та використання в реальному бізнесі.

1 СТАН ПИТАННЯ І ПОСТАНОВКА ЗАВДАННЯ

1.1 Стисла характеристика галузі та умов застосування системи, що проектується

Ведення бізнесу через розгалужену роздрібну мережу є значно ефективнішим підходом у сфері торгівлі, ніж управління окремими магазинами. Створення такої мережі надає численні переваги, серед яких особливо виділяються оптимізація асортименту та ціноутворення завдяки можливості кращого регулювання товарних запасів та зниження цін за необхідності, що є запорукою успішної торгівлі. Бізнес-план роздрібної мережі завжди включає оптові закупівлі великих партій товарів, що забезпечує значну економію на вартості одиниці продукції та витратах на доставку, а також дає змогу отримувати знижки від постачальників. Мережа магазинів функціонує під єдиним централізованим управлінням, що забезпечує швидке та чітке прийняття рішень на найвищому рівні, а також залучення висококваліфікованих фахівців, що мінімізує операційні проблеми. Зменшення собівартості товарів стає можливим завдяки відсутності необхідності постійного пошуку місць збуту та зниженню витрат на рекламу, що, своєю чергою, дозволяє пропонувати конкурентніші ціни та залучати більше покупців. Важливою перевагою є можливість адаптації асортименту кожного окремого магазину до місцевого попиту, що підвищує загальну ефективність мережі.

Роздрібна торговельна мережа зі значною кількістю магазинів (за деякими оцінками, понад 19-21) розглядається як торговельна ланка, що свідчить про вищий рівень її розвитку та потенційну рентабельність.

У сучасному світі розвиток роздрібних мереж характеризується такими тенденціями, як омніканальність, що поєднує онлайн та офлайн канали продажів; активна цифровізація для оптимізації управління та персоналізації пропозицій; розширення через електронну комерцію; зростання значення персоналізації та сталого розвитку; а також посилення конкуренції з боку e-commerce гігантів. Розуміння цих переваг та сучасних

тенденцій є ключовим для успішного розвитку роздрібних мереж в умовах динамічного ринку.

Робота мережі магазинів музичної техніки охоплює завдання, пов'язані з купівлею та продажем товарів, а також ведення бухгалтерського обліку. Для ефективної діяльності необхідно оперативно отримувати інформацію про клієнтів та співробітників.

Крім того, важливим є забезпечення можливості для відвідувачів переглядати асортимент онлайн, замовляти продукцію через інтернет та надсилати заявки електронною поштою.

Таким чином, для злагодженого функціонування всі елементи мережі магазинів повинні оперативно взаємодіяти.

Оскільки інформація про наявну продукцію в магазинах, на складах та її електронний каталог зберігатиметься в базі даних, для забезпечення максимальної оперативності та злагодженості роботи мережі необхідно об'єднати комп'ютери кожної філії локальною обчислювальною мережею, які, своєю чергою, будуть пов'язані між собою.

1.2 Характеристика і структура об’єкта впровадження

Для ефективного функціонування бізнесу, що займається продажем музичних інструментів, ключовим є створення, впровадження та налагодження комплексної комп'ютерної системи. Розробка мережевого проєкту вимагає ретельного аналізу структурних підрозділів підприємства, які будуть інтегровані в єдину мережу. Такі підприємства характеризуються широким спектром функціональних завдань, що охоплюють різні аспекти їхньої діяльності, а також потребують організації автоматизованих сховищ та архівів інформації. В сучасних умовах ефективне управління підприємством неможливе без впровадження комп'ютерної системи, що базується на сучасних мережевих технологіях та обладнанні. Побудова логічної топології мережі передбачає детальне ознайомлення з організаційною структурою підприємства та визначення підрозділів, яким необхідний доступ до мережевих ресурсів. Загальна організаційна

структура магазинів з продажу музичних інструментів визначається взаємозв'язками та підпорядкованістю між її структурними одиницями.

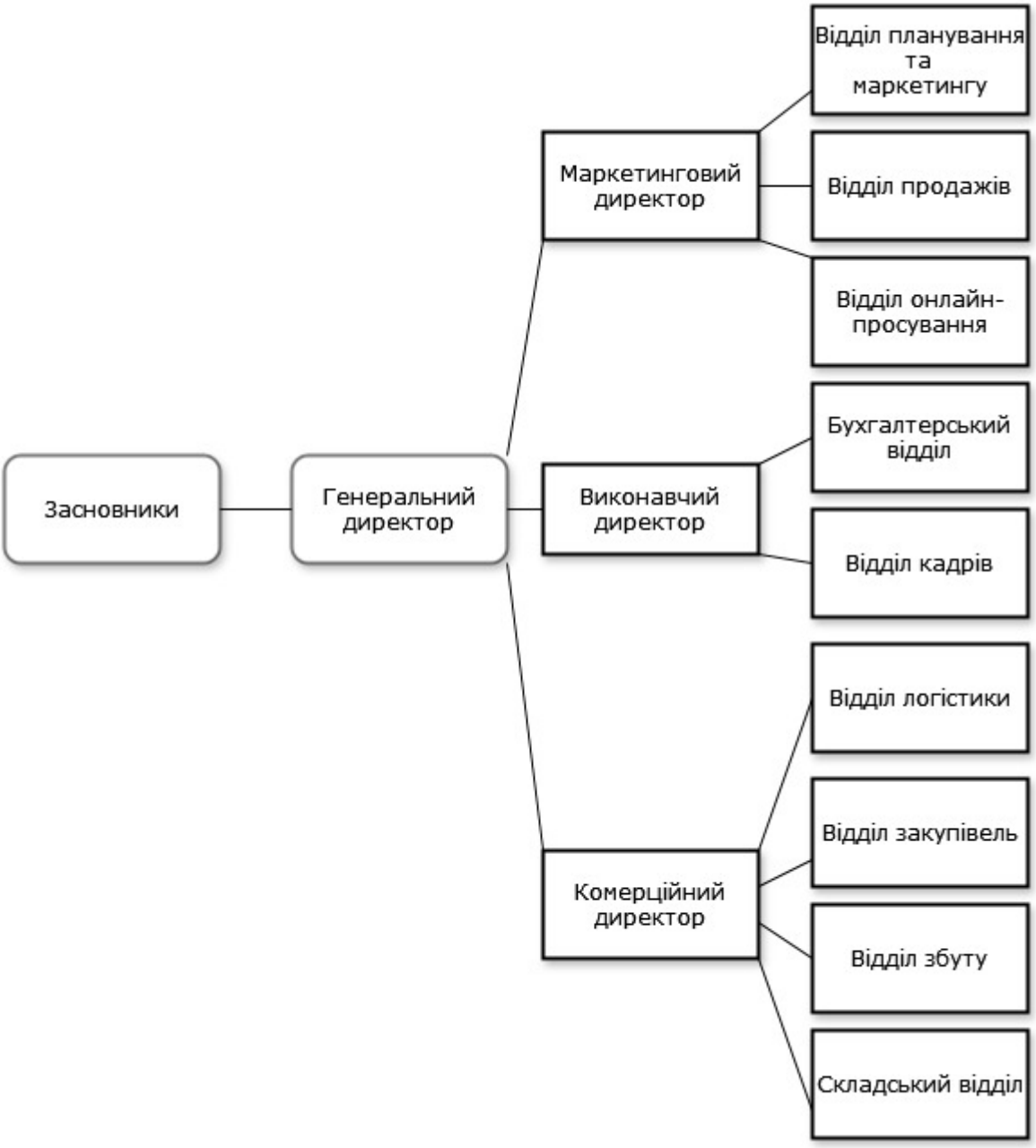


Рисунок 1.1 – Організаційна структура крамниць музичних інструментів

Вищим рівнем корпоративного управління є загальні збори учасників, які можуть проводитися як планово, так і за необхідності. Контроль за фінансово-господарською діяльністю підприємства здійснює ревізійна комісія. Поточне управління діяльністю покладається на дирекцію, очолювану директором, який несе відповідальність за роботу підприємства

в цілому. Директор, будучи єдиним виконавчим органом, представляє інтереси компанії, здійснює операції, видає ліцензії працівникам, керує справами та надає обов'язкові для виконання вказівки всім співробітникам, проте самостійно приймати рішення та діяти від імені корпорації не уповноважений.

У кожному магазині ведеться ретельний облік усіх товарів, прийнятих замовлень та клієнтів.

Доступ до бази даних магазинів музичних інструментів мають різні групи користувачів, кожна з яких має певні права та обов'язки. Директори володіють повним доступом до всієї інформації про діяльність усіх підрозділів. Бухгалтерський відділ може переглядати всю фінансову документацію та інформацію щодо касових операцій. Маркетологи та менеджери мають можливість переглядати та додавати інформацію про чеки, редагувати або додавати дані про замовлення, а також переглядати будь-яку іншу інформацію в базі даних. Адміністратори-консультанти можуть вносити зміни до особистих даних клієнтів та працівників, додавати або видаляти інформацію про товари, редагувати або додавати дані про замовлення, а також переглядати всю наявну інформацію. Продавці-касири мають доступ до перегляду інформації про замовлення та наявність товарів на складі. Клієнти ж можуть переглядати інформацію про свої замовлення та отримувати відомості про товари, які їх цікавлять.

1.3 Огляд існуючих аналогів КС, технологій, архітектур та програмних рішень

На даний момент існує кілька підстандартів технології Fast Ethernet (100 Мбіт/с), які відрізняються фізичним рівнем передачі даних, тобто типом кабелю та способом кодування сигналу. Ось основні з них:

100BASE-TX. Це найпоширеніший підстандарт Fast Ethernet. Він використовує неекрановану кручену пару (UTP) категорії 5 або вище, а також екрановану кручену пару (STP). Для передачі даних використовуються дві пари проводів: одна для передачі та одна для

прийому. Максимальна довжина сегмента становить 100 метрів. В 100BASE-TX застосовується метод кодування 4B5B з подальшим кодуванням MLT-3 (Multi-Level Transmit-3).

100BASE-FX. Цей підстандарт призначений для передачі даних по оптоволоконному кабелю. Він використовує два волокна (одне для передачі та одне для прийому) і працює на довжині хвилі 1300 нм. Максимальна довжина сегмента може досягати кількох кілометрів (залежно від типу оптоволокна та використовуваних трансиверів), що робить його придатним для з'єднання між будівлями або на великих відстанях.

100BASE-T4. Цей підстандарт використовує чотири пари проводів неекранованої крученої пари (UTP) категорії 3 або вище. На відміну від 100BASE-TX, він використовує всі чотири пари одночасно як для передачі, так і для прийому даних. Максимальна довжина сегмента також становить 100 метрів. В 100BASE-T4 застосовується складніший метод кодування, який дозволяє досягти швидкості 100 Мбіт/с, використовуючи менш вимогливу категорію кабелю. Однак, цей підстандарт був менш популярним, ніж 100BASE-TX, через складність реалізації та вимоги до обладнання.

Існують також інші, менш поширені підстандарти, такі як 100BASE-T2, який використовував дві пари категорії 3 UTP для повнодуплексного зв'язку, але він не набув широкого поширення.

Отже, основні підстандарти Fast Ethernet відрізняються типом використовуваного кабелю (кручена пара чи оптоволокно) та кількістю пар проводів (для крученої пари), а також методами кодування сигналу, що впливає на максимальну довжину сегмента та вимоги до кабелю. 100BASE-TX залишається найпоширенішим варіантом для локальних мереж на основі мідної крученої пари, тоді як 100BASE-FX використовується для з'єднань на більших відстанях з використанням оптоволокна. 100BASE-T4 хоч і був стандартом, але не отримав значної популярності.

Також існує кілька підстандартів технології Gigabit Ethernet (1000 Мбіт/с), які відрізняються фізичним рівнем передачі даних, тобто типом кабелю та способом кодування сигналу. Ось основні з них:

1000BASE-T. Це найпоширеніший підстандарт Gigabit Ethernet, що працює по неекранованій крученій парі (UTP) категорії 5e або вище. Він використовує всі чотири пари проводів для одночасної передачі та прийому даних у повнодуплексному режимі. Максимальна довжина сегмента становить 100 метрів. В 1000BASE-T використовується складний метод кодування сигналу, такий як PAM5 (Pulse Amplitude Modulation with 5 levels).

1000BASE-TX. Цей підстандарт також використовує неекрановану кручену пару (UTP) категорії 6 або вище. Він, як і 100BASE-TX, використовує дві пари проводів для передачі та дві пари для прийому. Максимальна довжина сегмента також становить 100 метрів. Хоча він і був розроблений як альтернатива 1000BASE-T, він не набув такої широкої популярності через вищі вимоги до кабелю (категорія 6) та меншу сумісність з існуючою інфраструктурою.

1000BASE-SX. Цей підстандарт призначений для роботи по багатомодовому оптоволоконному кабелю (MMF). Він використовує короткохвильове лазерне випромінювання (850 нм). Максимальна довжина сегмента залежить від типу багатомодового волокна і може варіюватися від 220 до 550 метрів. 1000BASE-SX є економічно вигідним рішенням для з'єднання обладнання на відносно невеликих відстанях у межах будівлі або кампусу.

1000BASE-LX. Цей підстандарт призначений для роботи як по багатомодовому (MMF), так і по одномодовому оптоволоконному кабелю (SMF). Він використовує довгохвильове лазерне випромінювання (1300 нм). При використанні багатомодового волокна максимальна довжина сегмента може досягати 550 метрів, а при використанні одномодового волокна - до 5 кілометрів і більше (залежно від якості волокна та трансиверів). 1000BASE-

LX використовується для з'єднання обладнання на більших відстанях, включаючи з'єднання між будівлями.

Існують також інші, менш поширені підстандарти Gigabit Ethernet, призначені для специфічних застосувань, наприклад, 1000BASE-CX (працював на коротких відстанях по коаксіальному кабелю, але застарів) та різні варіанти для пасивних оптичних мереж (PON).

Отже, основні підстандарти Gigabit Ethernet відрізняються типом використовуваного кабелю (кручена пара чи оптоволокно), категорією крученої пари (для мідних з'єднань), типом оптоволокна (багатомодове чи одномодове) та довжиною хвилі лазерного випромінювання (для оптичних з'єднань). Ці відмінності визначають максимальну довжину сегмента, вартість обладнання та придатність для різних сценаріїв використання. 1000BASE-T є найбільш поширеним варіантом для локальних мереж на основі мідної крученої пари, тоді як оптичні підстандарти використовуються для з'єднань на більших відстанях.

Технологія 10 Gigabit Ethernet (10GbE) – це технологія передачі даних в локальних мережах (LAN) зі швидкістю 10 гігабіт на секунду (10 Gbps або 10 000 Мбіт/с). Вона є значним кроком вперед у порівнянні з Gigabit Ethernet (1 Gbps) і стала ключовою технологією для високошвидкісних мереж, центрів обробки даних, корпоративних мереж та інших застосувань, що вимагають великої пропускної здатності.

Існує кілька підстандартів 10 Gigabit Ethernet, які відрізняються фізичним рівнем передачі даних, тобто типом кабелю та способом кодування сигналу. Ось основні з них:

Для мідної крученої пари:

10GBASE-T. Це найпоширеніший підстандарт 10GbE для мідної інфраструктури. Він використовує неекрановану кручену пару (UTP) категорії 6a або вище, а в деяких випадках може працювати на коротших відстанях з кабелем категорії 6. Всі чотири пари проводів використовуються для одночасної передачі та прийому даних у повнодуплексному режимі. Максимальна довжина сегмента становить 100 метрів для категорії 6a та 55

метрів для категорії 6. В 10GBASE-T застосовується складний метод кодування сигналу, такий як PAM16 (Pulse Amplitude Modulation with 16 levels).

Оптоволоконний кабель.

10GBASE-SR (Short Range). Призначений для роботи по багатомодовому оптоволоконному кабелю (MMF). Використовує короткохвильове лазерне випромінювання (850 нм). Максимальна довжина сегмента залежить від типу багатомодового волокна і може варіюватися від 26 до 400 метрів. Це економічно вигідне рішення для з'єднання обладнання на невеликих відстанях у межах центру обробки даних або будівлі.

10GBASE-LR (Long Range). Призначений для роботи по одномодовому оптоволоконному кабелю (SMF). Використовує довгохвильове лазерне випромінювання (1310 нм). Максимальна довжина сегмента може досягати 10 кілометрів. Використовується для з'єднання між будівлями або на значних відстанях.

10GBASE-ER (Extended Range). Призначений для роботи по одномодовому оптоволоконному кабелю (SMF). Використовує довгохвильове лазерне випромінювання (1550 нм). Максимальна довжина сегмента може досягати 40 кілометрів. Використовується для з'єднань на дуже великих відстанях.

10GBASE-LRM (Long Reach Multimode). Розроблений для роботи по існуючому багатомодовому оптоволоконному кабелю (MMF), який може бути старішим (наприклад, OM1 або OM2). Використовує довгохвильове лазерне випромінювання (1310 нм) та спеціальні методи кодування для компенсації дисперсії. Максимальна довжина сегмента становить до 300 метрів, залежно від типу волокна.

Існують також інші підстандарти 10GbE, призначені для специфічних застосувань, такі як варіанти для пасивних оптичних мереж (PON) та для з'єднань по коаксіальному кабелю (хоча останні менш поширені).

Основні відмінності між підстандартами.

Тип кабелю. Мідна кручена пара (UTP) або оптоволокно (MMF або SMF).

Категорія мідного кабелю. Для мідних підстандартів потрібні різні категорії кабелю для забезпечення необхідної пропускної здатності та довжини сегмента.

Довжина хвилі лазера (для оптики): Визначає тип оптоволокна та максимальну відстань передачі.

Максимальна довжина сегмента: Значно варіюється залежно від підстандарту та типу кабелю.

Вартість. Вартість обладнання (трансиверів, комутаторів) та кабельної інфраструктури може суттєво відрізнятися між різними підстандартами.

Вибір конкретного підстандарту 10 Gigabit Ethernet залежить від конкретних потреб мережі, відстаней між обладнанням, існуючої інфраструктури та бюджету. 10GBASE-T є зручним варіантом для оновлення існуючих мідних мереж, тоді як оптичні підстандарти забезпечують більшу відстань передачі та кращу стійкість до електромагнітних завад.

Технології WLAN (Wireless Local Area Network) або бездротові локальні мережі дозволяють пристроям підключатися до мережі Інтернет або один до одного без використання фізичних кабелів. Вони стали надзвичайно поширеними завдяки своїй зручності, гнучкості та здатності забезпечувати мобільність користувачів.

Основні аспекти технологій WLAN.

1. Стандарти IEEE 802.11 (Wi-Fi).

Більшість сучасних WLAN базуються на стандартах, розроблених Інститутом інженерів з електротехніки та електроніки (IEEE) і відомих як сімейство 802.11, або більш комерційно – Wi-Fi. Кожен новий стандарт вводить покращення в швидкості передачі даних, ефективності, надійності та інших характеристиках. Основні стандарти включають:

802.11b (Wi-Fi 1). Один з перших широко поширених стандартів. Забезпечує максимальну швидкість передачі даних до 11 Мбіт/с. Працює в діапазоні 2.4 ГГц.

802.11a (Wi-Fi 2). Забезпечує вищу швидкість передачі даних до 54 Мбіт/с, але працює в діапазоні 5 ГГц, що може мати менший радіус дії та гірше проникнення через стіни порівняно з 2.4 ГГц.

802.11g (Wi-Fi 3). Комбінує переваги 802.11b (діапазон 2.4 ГГц) та 802.11a (швидкість до 54 Мбіт/с). Став дуже популярним.

802.11n (Wi-Fi 4). Впровадив технологію MIMO (Multiple-Input Multiple-Output), що дозволило значно збільшити швидкість передачі даних (до 600 Мбіт/с теоретично, зазвичай менше в реальних умовах) та радіус дії. Працює в діапазонах 2.4 ГГц та 5 ГГц.

802.11ac (Wi-Fi 5). Подальше значне збільшення швидкості (до кількох гігабіт на секунду теоретично) завдяки ширшим каналам, вищій щільності модуляції та технології MU-MIMO (Multi-User MIMO). Працює переважно в діапазоні 5 ГГц.

802.11ax (Wi-Fi 6). Впровадив технологію OFDMA (Orthogonal Frequency-Division Multiple Access) для більш ефективного використання спектра та покращення продуктивності в умовах великої кількості підключених пристроїв. Збільшена швидкість та енергоефективність. Працює в діапазонах 2.4 ГГц та 5 ГГц, а також у нових діапазонах (6 ГГц).

802.11be (Wi-Fi 7): Найновіший стандарт, який обіцяє ще вищі швидкості, нижчу затримку та кращу ефективність завдяки ширшим каналам (до 320 МГц), технології MLO (Multi-Link Operation) та покращеній модуляції.

2. Діапазони частот.

WLAN використовують неліцензовані радіочастотні діапазони.

2.4 ГГц. Має краще проникнення через стіни та більший радіус дії, але більш завантажений через використання іншими пристроями (Bluetooth, мікрохвильові печі тощо).

5 ГГц. Менш завантажений, забезпечує вищі швидкості, але має менший радіус дії та гірше проникнення через перешкоди.

6 ГГц. Новий діапазон, доступний для Wi-Fi 6E та Wi-Fi 7, забезпечує значну кількість додаткових каналів, що сприяє вищим швидкостям та меншій кількості перешкод.

3. Компоненти WLAN. Точка доступу (Access Point - AP): Пристрій, який створює WLAN. Зазвичай підключається до дротової мережі (наприклад, до маршрутизатора) і транслює бездротовий сигнал, до якого підключаються клієнтські пристрої.

Клієнтські пристрої. Комп'ютери, смартфони, планшети, принтери та інші пристрої з вбудованими або зовнішніми бездротовими мережевими адаптерами, які можуть підключатися до WLAN.

Маршрутизатор (Router). Часто поєднує в собі функції точки доступу, маршрутизатора (для керування трафіком між мережами) та іноді модема (для підключення до Інтернет-провайдера).

4. Режими роботи WLAN. Найпоширеніший режим, де клієнтські пристрої підключаються до точки доступу, яка, в свою чергу, підключена до дротової мережі.

Ad-hoc режим (Peer-to-peer): Клієнтські пристрої безпосередньо підключаються один до одного без використання точки доступу. Менш поширений для підключення до Інтернету, але може використовуватися для обміну файлами між пристроями.

5. Безпека WLAN. Безпека є критично важливим аспектом WLAN. Існують різні протоколи шифрування для захисту бездротової мережі від несанкціонованого доступу:

WEP (Wired Equivalent Privacy): Застарілий та вразливий протокол. Не рекомендується до використання.

WPA (Wi-Fi Protected Access): Покращений протокол, але також має відомі вразливості.

WPA2 (Wi-Fi Protected Access 2): Більш безпечний протокол, який використовує алгоритм шифрування AES. Довгий час був стандартом.

WPA3 (Wi-Fi Protected Access 3): Найновіший та найбезпечніший протокол, який пропонує покращене шифрування, захист від атак методом підбору пароля та спрощений процес підключення IoT-пристроїв.

6. Застосування WLAN. WLAN використовуються в широкому спектрі сценаріїв:

– домашні мережі для підключення персональних пристроїв до Інтернету.
– офісні мережі для забезпечення бездротового доступу співробітників до мережевих ресурсів.
– публічні Wi-Fi мережі в кафе, аеропортах, готелях тощо.
– промислові мережі для підключення обладнання та датчиків.
– освітні заклади для забезпечення доступу до навчальних ресурсів.

7. Тенденції розвитку WLAN. Постійне збільшення швидкості передачі даних з появою нових стандартів (Wi-Fi 6, Wi-Fi 7).

Покращення ефективності використання радіочастотного спектра.

Збільшення щільності підключення пристроїв без втрати продуктивності.

Розширення використання нових частотних діапазонів (6 ГГц).

Покращення безпеки та зручності використання.

Інтеграція з іншими бездротовими технологіями (наприклад, Bluetooth).

Підсумовуючи, технології WLAN є ключовою складовою сучасного цифрового світу, забезпечуючи зручний та гнучкий бездротовий доступ до мережі для широкого спектра пристроїв та застосувань. Постійний розвиток стандартів Wi-Fi продовжує покращувати їхні можливості та розширювати сфери використання.

Технології доступу до Інтернету. У сучасному світі існує велика різноманітність конкурентоспроможних технологій доступу до Інтернету, кожна з яких має свої переваги та недоліки, що робить їх придатними для різних потреб та умов. Однією з найпоширеніших є дротове підключення

через Ethernet, яке забезпечує стабільне та швидке з'єднання, особливо в локальних мережах, але обмежує мобільність. DSL (Digital Subscriber Line) технології, такі як ADSL та VDSL, використовують існуючу телефонну інфраструктуру для передачі даних, пропонуючи широкосмуговий доступ, хоча швидкість може залежати від відстані до провайдера. Кабельне телебачення (DOCSIS) також є популярним варіантом, використовуючи коаксіальні кабелі для забезпечення високих швидкостей завантаження та вивантаження.

Значну конкуренцію дротовим технологіям складають бездротові технології, серед яких лідером є Wi-Fi (IEEE 802.11). Завдяки стандартам, що постійно розвиваються (Wi-Fi 6, Wi-Fi 7), WLAN забезпечують високі швидкості та зручність підключення в межах зони дії точки доступу, що робить їх незамінними вдома, в офісах та громадських місцях. Мобільний інтернет (3G, 4G LTE, 5G) є ще однією важливою бездротовою технологією, яка забезпечує доступ до Інтернету в будь-якій точці покриття мережі оператора, пропонуючи зростаючі швидкості та низьку затримку, особливо з впровадженням 5G.

Окрім вищезазначених, існують і інші технології, такі як супутниковий інтернет, який забезпечує доступ у віддалених та важкодоступних регіонах, хоча може мати вищу затримку та вартість. Оптоволоконний інтернет (FTTx) вважається однією з найперспективніших технологій завдяки надзвичайно високій швидкості та стабільності з'єднання, але його розгортання потребує значних інвестицій в інфраструктуру. Також варто згадати про новітні рішення, такі як Starlink та інші системи супутникового широкосмугового доступу нового покоління, які прагнуть забезпечити високошвидкісний інтернет у глобальному масштабі.

Конкуренція між цими технологіями стимулює провайдерів постійно вдосконалювати свої послуги, підвищувати швидкості, знижувати ціни та розширювати покриття, що зрештою йде на користь кінцевим користувачам, забезпечуючи їм широкий вибір варіантів доступу до

Інтернету, що відповідають їхнім індивідуальним потребам та можливостям.

1.4 Обґрунтування вибраного напрямку вирішення задачі

Ефективне функціонування сучасної компанії з розгалуженою клієнтською базою та широким асортиментом товарів вимагає комплексної модернізації, ключовим елементом якої є впровадження гнучкої системи розрахунків, налагодженого контролю оплати, постійного моніторингу складських запасів та автоматизованого формування необхідної документації. В умовах інтенсивного обміну даними між різними підрозділами, забезпечення оперативного доступу до інформації для всіх зацікавлених сторін є критично важливим. Тому для оптимізації інформаційних потоків та підвищення ефективності управління необхідна єдина інформаційна система, що базується на сучасній комп'ютерній мережі.

Корпоративна мережа підприємства призначена виключно для внутрішнього використання персоналом. Складність, структура та ієрархія цієї мережі безпосередньо залежать від масштабу підприємства та специфіки завдань, які воно виконує. У контексті сучасних технологій, програмно-апаратні рішення від лідерів галузі, таких як Cisco Systems, забезпечують комплексний підхід до побудови та управління мережевими комунікаціями, охоплюючи всі аспекти їхнього використання.

Cisco Systems, як провідний постачальник мережевих рішень, пропонує широкий спектр інноваційних технологій та обладнання, що охоплюють не лише традиційну маршрутизацію та комутацію, але й передові рішення в галузі кібербезпеки, бездротових мереж (Wi-Fi 6, Wi-Fi 7), хмарних технологій, Інтернету речей (IoT), штучного інтелекту (AI) для управління мережею, а також програмно-визначених мереж (SDN) та мережевих функцій віртуалізації (NFV), що забезпечують гнучкість, масштабованість та автоматизацію мережевої інфраструктури. Використання таких сучасних рішень дозволяє компаніям будувати

високопродуктивні, надійні та безпечні мережі, що є фундаментом для успішного ведення бізнесу в цифрову епоху.

Сьогодні портфель рішень Cisco продовжує розвиватися, включаючи інтеграцію штучного інтелекту та машинного навчання для автоматизації мережевого управління та підвищення безпеки (наприклад, Cisco DNA Center з SD-Access та AI Network Analytics). Також зростає значення хмарних рішень для управління мережевою інфраструктурою та безпекою (наприклад, Cisco SecureX). Cisco активно розвиває напрямок Secure Access Service Edge (SASE), що об'єднує мережеві функції та функції безпеки в єдину хмарну службу. У сфері бездротових мереж особлива увага приділяється розгортанню Wi-Fi 6 та Wi-Fi 6E для забезпечення ще вищих швидкостей та кращої продуктивності в умовах високої щільності клієнтів, а також готується до впровадження стандарту Wi-Fi 7. Для IoT Cisco пропонує розширені можливості для промислового IoT, включаючи кіберфізичну безпеку та аналітику даних в реальному часі, [1].

1.5 Мета і задачі роботи

Основна мета цієї роботи – полягає у створенні комп'ютерної системи для магазинів музичних інструментів, яка детально охоплює процеси побудови, налаштування та забезпечення безпеки корпоративної мережі.

Ключовою вимогою до таких мереж є надання користувачам безперешкодного доступу до ресурсів усіх комп'ютерів, об'єднаних в єдину систему.

Всі інші важливі характеристики, такі як продуктивність, надійність, сумісність, керованість, прозорість, розширюваність та масштабованість, є похідними від цієї основної мети та визначають якість її реалізації.

Для ефективної роботи більшості сучасних програм критично важлива висока продуктивність комп'ютерної мережі. Ця продуктивність визначається кількома ключовими технічними показниками. Час реакції є інтегральною характеристикою мережі з точки зору користувача,

відображаючи проміжок часу між його запитом до мережевого ресурсу та отриманням відповіді [2, 3].

Пропускна здатність визначає максимальну потужність обробки трафіку, встановлену стандартом використовуваної технології, і являє собою максимальний обсяг даних, який мережа або її компонент може передати за одиницю часу.

Час затримки – це інтервал часу між надходженням даних на вхід компонента або всієї мережі та їхнім виходом. Важливим аспектом є також варіація затримки, тобто випадкові зміни часу затримки, які можуть істотно погіршити якість мережевих сервісів [3].

Однією з фундаментальних цілей створення розподілених систем, включаючи комп'ютерні мережі, була забезпечення вищого рівня надійності порівняно з окремими комп'ютерами. Для оцінки надійності складних систем використовуються такі атрибути: готовність або коефіцієнт готовності, що відображає час, протягом якого система доступна для використання; збереження даних та їх захист від спотворень; узгодженість даних, особливо важлива у випадку резервування даних на кількох серверах, де необхідно забезпечувати їхню ідентичність через постійну синхронізацію; а також можливість доставки даних.

Ключовою вимогою до сучасних мереж є безпека – здатність системи захищати дані від несанкціонованого доступу.

Відмовостійкість – це здатність системи приховувати від користувачів відмови окремих компонентів, забезпечуючи безперервність роботи сервісів.

Сумісність або інтегрованість означає здатність мережі підтримувати різноманітне програмне та апаратне забезпечення, включаючи різні операційні системи, комунікаційні протоколи та обладнання від різних виробників.

Керованість передбачає можливість централізованого управління станом компонентів мережі, виявлення та вирішення проблем, а також віддалене конфігурування для задоволення мінливих потреб організації.

Прозорість – це здатність мережі приховувати свою внутрішню складність від користувача, представляючись як єдиний інтегрований ресурс. Розширюваність означає можливість легкого додавання нових компонентів (користувачів, комп'ютерів, програм, служб) та збільшення довжини мережевих сегментів.

Нарешті, масштабованість – це здатність мережі збільшувати кількість учасників та довжину з'єднань, зберігаючи при цьому високий рівень продуктивності.

Також варто враховувати, що у сучасному контексті до цих вимог додаються такі важливі аспекти, як енергоефективність, особливо важлива для великих мереж та центрів обробки даних; якість обслуговування (QoS) для пріоритезації певного типу трафіку (наприклад, голосового або відео); гнучкість та адаптивність до швидкозмінних технологічних вимог; а також автоматизація багатьох процесів управління та моніторингу мережі за допомогою програмно-визначених мереж (SDN) та мережевих функцій віртуалізації (NFV).

Також зростає важливість кіберстійкості, що включає не лише захист від несанкціонованого доступу, але й здатність мережі відновлюватися після кібератак та інших збоїв.

2 РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ КОМП'ЮТЕРНОЇ СИСТЕМИ ПІДПРИЄМСТВА

2.1 Технічні вимоги до КС

2.1.1 Вимоги до системи в цілому

2.1.1.1 Вимоги до структури і функціонуванню системи

Комп'ютерна система сучасної мережі магазинів музичних інструментів є критично важливою інфраструктурою, що забезпечує операційну ефективність, безпеку даних та безперебійний доступ до ресурсів. Її функціональність можна умовно розділити на дві ключові, тісно інтегровані області.

1. Система моніторингу та управління продуктивністю мережевої інфраструктури.

Цей напрямок охоплює централізований збір даних про стан, продуктивність та доступність усіх активних компонентів мережі (серверів, маршрутизаторів, комутаторів, точок доступу Wi-Fi, робочих станцій, POS-терміналів, а також, за потреби, інтегрованих "розумних" музичних інструментів - IoT-пристроїв).

Функції системи моніторингу:

– моніторинг доступності. Безперервна перевірка працездатності пристроїв та сервісів;

– моніторинг продуктивності. Відстеження завантаження процесорів, використання пам'яті, дискового простору, мережевого трафіку, затримок та інших метрик;

– журналювання та оповіщення. Збір системних логів (журналів подій) для аудиту та негайне сповіщення адміністраторів про критичні події, аномалії чи збої (перевищення порогів використання ресурсів, відмова пристрою, спроба несанкціонованого доступу).

– моніторинг безпеки. Інтеграція з системами SIEM для виявлення та аналізу подій, що стосуються кібербезпеки.

2. Система керування ідентифікацією та доступом до ресурсів.

Даний напрямок фокусується на визначенні, автентифікації та авторизації користувачів (співробітників) та пристроїв для контрольованого доступу до мережевих ресурсів, даних та програмного забезпечення.

Функції системи керування ідентифікацією та доступом:

– централізована автентифікація. Використання єдиних облікових записів (Active Directory) для доступу до різних систем та сервісів (ПК, сервери, мережеві диски, корпоративні додатки);

– управління авторизацією (правами доступу). Детальне визначення прав користувачів та груп до файлів, папок, баз даних, функцій у корпоративних системах (CRM) на основі ролей (RBAC);

– управління пристроями. Контроль за підключенням пристроїв до мережі (NAC – Network Access Control), централізоване розгортання програмного забезпечення, оновлень безпеки та політик конфігурації.

Вимоги до узгодженості та функціонування пристроїв у мережі.

Для ефективної роботи цих систем і всієї мережі необхідно дотримуватися наступних принципів:

– повсюдний мережевий зв'язок. Кожен пристрій у мережі (від сервера в центральному ЦОД до POS-терміналу чи інтерактивного музичного інструменту в магазині) повинен мати гарантовану можливість встановлювати зв'язок та взаємодіяти з іншими необхідними пристроями та сервісами. Це забезпечується правильною конфігурацією маршрутизації, фаєрволів, VLAN-сегментації та надійним фізичним з'єднанням;

– забезпечення рівноправного доступу до фізичного середовища для всіх пристроїв, що колективно використовують його. Це досягається за рахунок використання сучасних мережевих протоколів (CSMA/CD для дротових мереж, CSMA/CA для Wi-Fi), ефективного дизайну мережі (наприклад, відсутність петель, правильна сегментація).

2.1.1.2 Показники призначення

Комп'ютерна система мережі магазинів музичних інструментів має бути спроектована для забезпечення високої продуктивності та ефективної роботи користувачів, а також підтримки ключових бізнес-процесів.

1. Вимоги до масштабованості користувачів.

Підсистема оперативної діяльності (POS, складський облік). Система повинна бути здатною одночасно обслуговувати до 500 активних користувачів. Це включає персонал магазинів (касири, продавці-консультанти, менеджери), співробітників центрального офісу (відділи закупівель, логістики, продажів, бухгалтерії) та зовнішніх партнерів, які взаємодіють із системою.

Підсистеми (CRM, файлові сервіси). Для цих підсистем має бути забезпечена підтримка не менше 100 одночасних користувачів. Це дозволить ефективно працювати відділам по роботі з клієнтами, кадровим службам, аналітикам та іншим підрозділам, що використовують спеціалізовані додатки.

2. Вимоги до часу відгуку системи.

Час відгуку системи є критично важливим для продуктивності співробітників та якості обслуговування клієнтів. Ці показники повинні бути досягнуті для всього ланцюга (від клієнтського пристрою, через мережу, до серверу та назад), що вимагає оптимізації як апаратного, так і програмного забезпечення, а також мережевої інфраструктури.

Для операцій навігації за екранними формами системи час відгуку системи повинен становити не більше 2 секунд.

Для операцій формування доступу/запитів (проведення продажу на касі, збереження нового замовлення, оновлення статусу товару, автентифікація користувача). Час відгуку системи повинен становити не більше 5 секунд.

3. Вимоги до часу генерації аналітичних звітів.

Період часу, виділений на аналітичні звіти, залежить від їх складності та обсягу даних. Прості, операційні звіти (наприклад, продажі за день)

повинні генеруватися протягом декількох секунд. Складні аналітичні звіти, що вимагають агрегації великих обсягів даних за тривалий період (наприклад, аналіз продажів за рік по всіх філіалах, прогнозування попиту), можуть займати від декількох секунд до декількох хвилин.

2.1.1.3 Вимоги до експлуатації, технічного обслуговування, ремонту і збереженню

Комп'ютерна система мережі магазинів музичних інструментів має бути спроектована та впроваджена з урахуванням найвищих стандартів надійності, достовірності даних та комплексного захисту.

Основною вимогою є забезпечення мінімального часу простою системи. Навіть повна відсутність зовнішнього електроживлення не повинна призводити до повного збою, а лише викликати тимчасове, перехідне порушення функціонування (наприклад, короткочасний перехід на резервне живлення без втрати даних та автоматичне відновлення роботи). Загальний час, протягом якого комп'ютерна система перебуває в непрацездатному стані (недоступна або функціонує некоректно) протягом року, не повинен перевищувати 0,02% від загального часу роботи, що еквівалентно приблизно 20 хвилинам на рік. Для досягнення цього показника, для типової безперебійної роботи системи необхідно гарантувати безперебійне джерело живлення для всіх критично важливих компонентів (наприклад, через ДБЖ з достатнім часом автономної роботи та/або дизель-генератори).

Усі технічні рішення, обрані для побудови та функціонування системи, а також визначення апаратного забезпечення, мусять відповідати чинним нормам і правилам щодо техніки безпеки, пожежної безпеки та захисту навколишнього середовища. Це охоплює вимоги до електроустановок, вентиляції, систем пожежогасіння, утилізації відходів тощо.

Система має бути органічно інтегрована як складова частина загального комплексу програмно-технічної інфраструктури мережі

магазинів музичних інструментів. Крім того, для забезпечення безпеки та керованості, IT-інфраструктура магазинів музичних інструментів повинна бути чітко розділена на внутрішню та зовнішню мережі. Внутрішня мережа призначена для доступу співробітників та внутрішніх ресурсів, тоді як зовнішня – для публічних сервісів (веб-сайт, онлайн-магазин) та взаємодії із зовнішнім світом.

Технічний та фізичний захист апаратних компонентів системи (серверів, мережевого обладнання, робочих станцій), зберігання даних, забезпечення надійного джерела живлення, а також резервування ресурсів (дублювання ключових елементів) є завданням IT-департаменту підприємства. Цей департамент також відповідає за поточне обслуговування системи.

2.1.2 Вимоги до функцій, які виконує КС

Комп'ютерна система мережі магазинів музичних інструментів повинна забезпечувати надійний та багаторівневий захист від несанкціонованого доступу (НСД) до інформаційних ресурсів. Цей захист має відповідати високим стандартам безпеки, зокрема, рівню не нижче "категорії 1Д" згідно з класифікацією чинного керівного документа НД ТЗІ 1.4-001-2000 "Загальні положення щодо побудови та функціонування комплексної системи захисту інформації в автоматизованих системах". Ця категорія передбачає комплексну систему захисту інформації, що охоплює технічні та організаційні заходи.

Ключові принципи та складові підсистеми захисту від НСД:

Побудована система повинна гарантувати суворе обмеження доступу як на рівні окремих програмних компонентів, так і на рівні структур даних. Це означає, що доступ до інформації та функціоналу надається виключно на основі визначених прав та ролей користувачів.

Основні складові підсистеми захисту від НСД включають:

– ідентифікація користувача. Система повинна однозначно ідентифікувати кожного користувача перед наданням доступу до будь-яких

ресурсів або початку роботи. Це передбачає використання унікальних логінів та автентифікаторів;

– автентифікація та перевірка повноважень. Включає перевірку пароля, використання багатофакторної автентифікації (MFA), біометричних даних або токенів;

– "Сліпі" паролі. При введенні пароля символи на екрані не повинні відображатися (або замінюватися зірочками/точками), а також, для додаткового захисту від підглядання, кількість відображуваних символів може не відповідати фактичній довжині пароля;

– система має забезпечувати детальне розмежування доступу користувачів до ресурсів, що базується на їхніх ролях та потребах. Реалізується на двох основних рівнях: на рівні завдань/функцій (касир має право оформлювати продаж, але не має доступу до звіту про прибутки компанії) та на рівні інформаційних масивів/даних.

– політики паролів з вимогою до створення складних паролів (довжина, комбінація символів), регулярна зміна паролів, блокування облікового запису після кількох невдалих спроб входу;

– шифрування конфіденційних даних як при зберіганні (at rest), так і при передачі (in transit) мережею;

– онтроль доступу до приміщень, де розміщені сервери та мережеве обладнання.

2.1.3 Вимоги до видів забезпечення КС

2.1.3.1 Вимоги до інформаційного забезпечення

Комп'ютерна система мережі магазинів музичних інструментів повинна забезпечувати високу ефективність, стабільність та прозорість обробки інформації, гарантуючи при цьому безперебійну та швидку передачу даних.

1. Прозорий режим обслуговування. Будь-які технічні аспекти роботи мережі, сервісів чи баз даних мають бути максимально приховані від

кінцевого користувача. Це забезпечує безшовний та комфортний досвід, дозволяючи зосередитися на бізнес-завданнях або процесі купівлі.

2. Стійкість до навантажень та відсутність блокувань. Навіть за умов повного або пікового завантаження мережі та систем, не повинно відбуватися блокування передачі даних. Це означає, що критично важливі операції (наприклад, проведення продажу, запит наявних товарів, доступ до ERP/CRM) повинні завжди мати пріоритет та виконуватися без затримок, незалежно від загального обсягу трафіку або кількості одночасних користувачів. Мережева інфраструктура та сервери повинні бути спроектовані з достатнім запасом пропускної здатності та обчислювальних ресурсів для запобігання "вузьким місцям" та колізіям, що можуть призвести до блокування.

3. Вимоги до швидкості передачі даних. Для забезпечення ефективної роботи та мінімального часу відгуку, мінімальна швидкість передачі даних на кожному робочому місці та між ключовими компонентами мережі повинна становити не менше 100 Мбіт/с. Для підключення серверів та магістральних з'єднань ця швидкість повинна бути значно вищою, згідно з розрахунками інтенсивності трафіку, і може сягати 1 Гбіт/с, 10 Гбіт/с або навіть 40/100 Гбіт/с для забезпечення безперебійної роботи критично важливих сервісів та швидкої обробки великих обсягів інформації.

2.1.3.2 Вимоги до програмного забезпечення

Розроблена система повинна відповідати вимогам передових світових технологій у сфері телекомунікацій та автоматизації управління, [2]:

– система повинна підтримувати можливість зберігання значних обсягів інформації в єдиній логічній базі даних, гарантуючи її комплексність та цілісність, а також забезпечувати широкі можливості функціонального розширення та нарощування потужності у міру зростання бізнесу, що визначає її розширюваність та масштабованість;

– підтримка розподіленої обробки інформації, дозволяє ефективний доступ до ресурсів системи як у локальній мережі, так і через мережу

Інтернет. Це забезпечить гнучкість роботи співробітників та доступність сервісів незалежно від їхнього фізичного розташування;

– для уніфікації процесів та даних, система має використовувати єдину систему класифікації та кодування інформації, що сприятиме її уніфікованості;

– система має бути здатною функціонувати в гетерогенних середовищах та на різних апаратних платформах, що підкреслює її багатоплатформність та гнучкість розгортання. Для мінімізації витрат та забезпечення безперебійної роботи необхідно забезпечувати взаємодію та повну сумісність з різними програмними продуктами, які вже використовуються на підприємстві, що підкреслює її відкритість та інтегрованість через використання стандартизованих інтерфейсів та API.

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

Структурна схема технічних засобів комп'ютерної системи мережі крамниць музичних інструментів являє собою трирівневу архітектуру, розроблену для забезпечення ефективної та безпечної роботи всієї інфраструктури.

Рівень ядра корпоративної мережі. Цей рівень є основою всієї мережі, де розташовані 5 роутерів, що виконують ключову роль у сегментуванні мережі та маршрутизації трафіку. Ці роутери не лише розділяють мережу на логічні частини, але й забезпечують оптимальний шлях передачі даних між різними підмережами. Таке сегментування підвищує безпеку, зменшує перевантаження мережі та спрощує управління трафіком. Роутери, використовуючи складні алгоритми маршрутизації, динамічно визначають оптимальний шлях для кожного пакету даних, враховуючи завантаженість мережі, пропускну здатність каналів зв'язку та інші фактори.

До складу корпоративної мережі входять шість підмереж, кожна з яких обслуговує конкретний підрозділ.

LAN_1 – Маркетинговий підрозділ. Забезпечує мережеве з'єднання для співробітників, відповідальних за маркетингові стратегії та комунікації.

LAN_2 – Виконавчий підрозділ. Підтримує мережеві потреби керівництва компанії.

LAN_3 – Крамниця 1. Обслуговує першу торгову точку, забезпечуючи з'єднання для касових апаратів, систем інвентаризації та інших пристроїв.

LAN_4 – Комерційний підрозділ. Забезпечує мережеві з'єднання для співробітників, відповідальних за продажі та комерційну діяльність.

LAN_5 – Крамниця 2. Обслуговує другу торгову точку, аналогічно до LAN_3.

LAN_6 – IT-відділ. Забезпечує мережеву інфраструктуру для технічних спеціалістів, відповідальних за підтримку та розвиток всієї комп'ютерної системи.

Рівень доступу. На цьому рівні розташовані комутатори підмереж, які організовують локальні мережі (LAN). У підмережах крамниць використовуються по два комутатори з підтримкою технології VLAN (Virtual LAN). VLAN дозволяє розділити фізичну мережу на декілька логічних мереж, що забезпечує ізоляцію трафіку між різними групами пристроїв та підвищує безпеку. У підмережах крамниць також розташовані системи Інтернету речей (IoT). Для доступу цих пристроїв до мережі використовуються спеціалізовані роутери з підтримкою бездротової технології, які виступають у ролі шлюзу (Gateway) для "розумних" речей.

Рівень хостів. На цьому рівні розташовані кінцеві мережеві пристрої комп'ютерної системи крамниць музичних інструментів. До їх складу входять комп'ютери, сервери, касові апарати та IP-камери в підмережах крамниць, а також сервери в підмережі LAN_6. У LAN_6 розташовані сервери IoT, FTTP, DNS та HTTP. Сервери IoT забезпечують керування та обробку даних від IoT-пристроїв, FTTP – доступ до Інтернету, DNS – перетворення доменних імен на IP-адреси, а HTTP – обслуговування веб-трафіку.

Канали зв'язку. Тип кабелів, що використовуються для з'єднання різних пристроїв, залежить від відстані та необхідної пропускної здатності. Між роутерами головного офісу і роутерами крамниць застосований оптоволоконний кабель, що забезпечує високу швидкість передачі даних на великі відстані. Між роутерами головного офісу застосовані кабелі Serial, які підходять для менших відстаней. Між роутерами і комутаторами використовуються кабелі Gigabit Ethernet, які забезпечують швидкість передачі даних до 1 гігабіта на секунду. Між комутаторами і хостами застосовуються кабелі Fast Ethernet, які забезпечують швидкість передачі даних до 100 мегабіт на секунду. Розумні речі в підмережах крамниць використовують бездротовий зв'язок WiFi, що забезпечує зручність та гнучкість у розгортанні мережі.

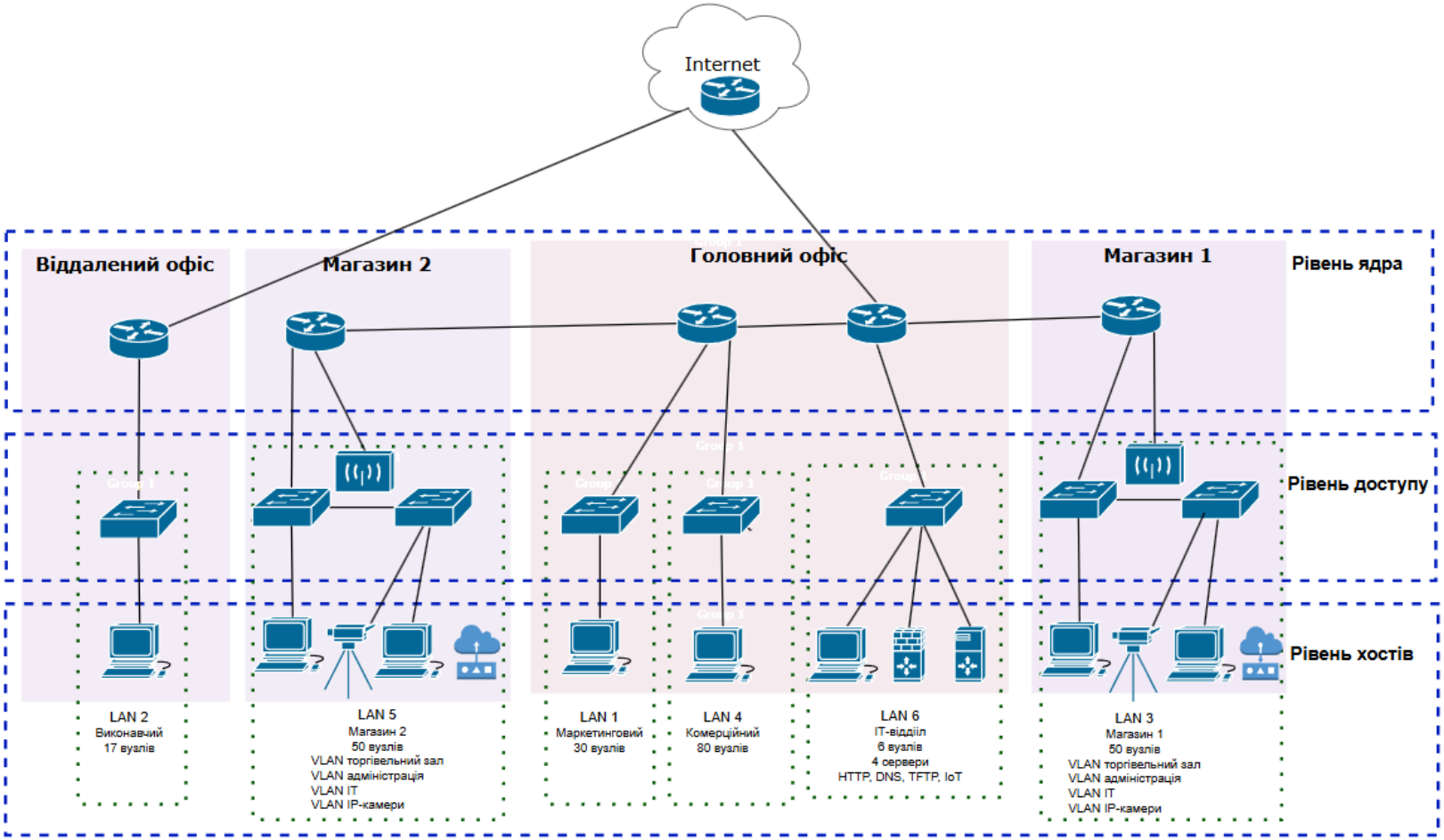


Рисунок 2.1 – Структурна схема технічних засобів комп’ютерної системи крамниць музичних інструментів

2.3 Розробка специфікації апаратних засобів КС

Рівень хостів.

1. Сервери.

Відповідно до технічних вимог щодо серверного обладнання КС КМІ (використання компонентів корпоративного класу, що характеризуються тривалим терміном служби, можливістю дублювання ключових елементів, гарантоване зберігання даних (RAID-масиви), масштабованість) після порівняння технічних характеристик серверів, було обрано сервер Dell PowerEdge R760 (Rack Server, 2U).

Технічні характеристики: розширена масштабованість – до 32 слотів DIMM DDR5, що дозволяє встановити до 8 ТБ оперативної пам'яті, до 24 NVMe/SAS/SATA 2.5" накопичувачів або до 12 NVMe/SAS/SATA 3.5" накопичувачів; оптимізований для високої продуктивності за рахунок NVMe; вбудовані 1GbE/10GbE LAN-порти, слоти PCIe Gen5 для високошвидкісних мережевих карт (25GbE, 40GbE, 100GbE); Підтримка до двох процесорів Intel Xeon Scalable 4-го або 5-го покоління (до 60 ядер на процесор).

2. Робочі місця користувачів.

2.1. Робочі місця для загальних офісних та адміністративних завдань.

Виконавши порівняння технічних характеристик робочих станцій було обрано Dell OptiPlex 5000/7000 Series (SFF/Mini PC), який має наступні характеристики:

– процесор: Intel Core i5 (12-го покоління або новіше) / AMD Ryzen 5 (5000-ї серії або новіше);

– оперативна пам'ять (RAM): 16 ГБ DDR4/DDR5. Це забезпечить плавну роботу кількох додатків одночасно;

– накопичувач: 256 ГБ - 512 ГБ NVMe SSD. NVMe значно прискорює завантаження ОС та додатків.

– операційна система: Windows 10 Pro / Windows 11 Pro (для корпоративного середовища та підтримки доменних політик).

– мережеві можливості: Gigabit Ethernet (1 Гбіт/с), Wi-Fi 5 (802.11ac) або Wi-Fi 6 (802.11ax), Bluetooth 5.0.

2.2. Робочі місця для магазинів (Каси / POS-термінали).

Після проведенного аналізу були вибрані компактні ПК - модифіковані Dell OptiPlex Micro, які мають наступні характеристики:

– процесор: Intel Core i3 (10-го покоління або новіше) / AMD Ryzen 3 (4000-ї серії або новіше). Достатньо для виконання транзакційних операцій;

– оперативна пам'ять (RAM): 8 ГБ DDR4;

– накопичувач: 128 ГБ - 256 ГБ SSD (SATA або NVMe). Об'єм менший, оскільки основні дані зберігаються централізовано.

– операційна система: Windows 10 IoT Enterprise LTSC (для спеціалізованих POS) або Windows 10 Pro;

– мережеві можливості: Gigabit Ethernet (пріоритет для стабільності), Wi-Fi (як резервний канал або для мобільних пристроїв).

Вибір «розумних речей».

1. IP-камери.

IP-камери є невід'ємною частиною сучасної системи безпеки та моніторингу в роздрібній торгівлі. Вони забезпечують візуальний контроль, запис подій, а також можуть надавати цінні дані для бізнес-аналітики. Для магазинів музичних інструментів важливо обирати камери, що забезпечують чітке зображення, надійну роботу в різних

умовах освітлення та інтеграцію з мережевою інфраструктурою. Після проведенного аналізу були вибрані IP-камери Dahua DH-IPC-HFW2831TP-ZS-S2 (Lite Series 8MP Vari-focal Bullet Network Camera), які мають наступні характеристики:

– тип: циліндрична (Bullet) IP-камера. Частіше використовується для зовнішнього спостереження, моніторингу периметру, коридорів або входів, де потрібна більша дальність;

– роздільна здатність: 8 мегапікселів (4K UHD, 3840 × 2160). Надає надзвичайно високу деталізацію, що важливо для розпізнавання дрібних деталей або збільшення частини зображення;

– об'єктив: моторизований варіфокальний (наприклад, 2.7 мм – 13.5 мм), що дозволяє дистанційно регулювати фокусну відстань та кут огляду, а також виконувати оптичний зум;

– нічне бачення: вбудоване ІЧ-підсвічування (до 60 м) та технологія Starlight для відмінного кольорового зображення в умовах надзвичайно низького освітлення;

– підключення: Ethernet (RJ45) з підтримкою PoE (802.3af);

– відеокомпресія: H.265+/H.265/H.264+/H.264.

2. Система пожежогасіння.

Датчики диму. Для системи пожежогасіння в мережі магазинів музичних інструментів вибір датчиків диму є критично важливим для раннього виявлення пожежі, захисту цінних активів та забезпечення безпеки персоналу. При аналізі датчиків диму, був зроблений вибір на користь датчиків Bosch Security Systems (серія FPA-5000, AVENAR detector 4000).

Датчик вогню. Для повноцінної системи пожежовиявлення критично важливими є датчики вогню, які зазвичай поділяються на теплові датчики

та датчики полум'я. При аналізі датчиків вогню, був зроблений вибір на користь датчиків Bosch AVENAR heat detector 4000 (серія AVENAR detector 4000).

Сповіщувач пожежний звуковий. Їхнє основне призначення – ефективно та швидко сповістити людей про виникнення пожежі та необхідність негайної евакуації. При аналізі оповіщувачів, був зроблений вибір на користь Bosch FAP-425-O Series (частина лінійки FPA-5000) та аналогічні моделі.

Автоматичні спринклерні системи пожежогасіння. Спринклерна система призначена для гасіння пожежі на ранніх стадіях або її локалізації шляхом розпилення води безпосередньо в зоні загоряння. При аналізі спринклерних розпилювачів, був зроблений вибір на користь Viking Mirage® Series Concealed Pendent Sprinkler.

Рівень доступу. Вибір комутаторів.

Для даного проекту були розглянуті та обрані комутатори виробника D-Link. Вибір D-Link базується на їхній репутації щодо надійності, співвідношенні ціни та якості, а також здатності підтримувати ключові мережеві функції, такі як VLAN-сегментація.

Після проведенного аналізу були вибрані комутатори D-Link DGS-1250-28X (Smart Managed 10 Gigabit Stackable Switch), які мають характеристики:

– тип: керований комутатор рівня 2 (L2 Smart Managed 10 Gigabit Stackable Switch);

– порти: 24 x 10/100/1000Base-T Gigabit Ethernet порти; 4 x 10 Gigabit SFP+ порти.

– підтримка PoE (DGS-1250-28XMP);

– розширені функції VLAN, включаючи Multiple VLANs, Asymmetric VLAN, GVRP.

–функції безпеки, включаючи IPv6 ACL, IP-MAC-Port Binding (IMPB) для прив'язки пристроїв до портів, D-Link Safeguard Engine (захист від DDoS-атак);

– висока комутаційна матриця до 128 Гбіт/с;

– стекування (Stackable): можливість об'єднання кількох комутаторів цієї серії в один логічний пристрій для спрощення управління та підвищення відмовостійкості.

Рівень ядра.

В якості роутерів КС КМІ обрані Cisco 2911/K9.

Маршрутизатор Cisco 2911/K9, відноситься до покоління ISR G2. Він може бути використаний для корпоративних мереж, підтримує можливість інтеграції додаткових слотів розширення з оптоволокном та serial-з'єднання.

Cisco 2911/K9 підтримує протоколи IPv4, IPv6, VPN, QoS, NAT, ACL тощо. Має особливості:

– модульний дизайн, що дозволяє додавати розширювальні модулі та WAN-інтерфейси;
– підтримка CISCO IOS – стабільна та багатофункціональна операційна система;
– підтримує криптографічні функції (шифрування з використанням SSL, IPsec).

Використовується для побудови корпоративних шлюзів, мережевого маршрутизування, VPN-з'єднань, мережевого безпечного доступу.

Таблиця 2.1 − Специфікація обладнання

Позиція	Найменування і технічна характеристика	Одиниці виміру	Кількість
1	2	3	4
1	Dell PowerEdge R760 (Rack Server, 2U)	шт.	4
2	Dell OptiPlex 5000/7000 Series (SFF/Mini PC)	шт.	30
3	Dell OptiPlex Micro	шт.	2
4	Dahua DH-IPC-HFW2831TP-ZS-S2 (Lite Series 8MP Vari-focal Bullet Network Camera)	шт.	12
5	Bosch Security Systems (наприклад, серії FPA-5000, AVENAR detector 4000)	шт.	4
6	Bosch AVENAR heat detector 4000 (Серія AVENAR detector 4000)	шт.	3
7	Bosch FAP-425-O Series	шт.	2
8	Viking Mirage® Series Concealed Pendent Sprinkler	шт.	4
9	D-Link DGS-1250-28X (Smart Managed 10 Gigabit Stackable Switch)	шт.	6
10	Cisco2911-V/K9 (SFP-роз'єми та слоти розширення EHWIC)	шт.	5
11	Cisco DLC-100 (спеціалізований маршрутизатор з підтримкою IoT)	шт	2

3 РОЗРОБКА КОРПОРАТИВНОЇ МЕРЕЖІ

3.1 Розрахунок схеми адресації корпоративної мережі

Побудова ефективної та масштабованої корпоративної мережі для мережі крамниць музичних інструментів є важливим кроком для забезпечення стабільної роботи бізнесу, централізованого управління даними та підтримки комунікації між різними локаціями. Важливо при виконанні проєкту мережі детально документувати структуру мережі, включаючи розподіл IP-адрес, налаштування мережевого обладнання та інші важливі деталі.

Побудова корпоративної мережі крамниць музичних інструментів виконується враховуючи вихідний блок адрес 17.24.144.0/21, і методи поділу його на 6 підмереж за технічними вимогами, з урахуванням особливостей цього процесу.

При роботі з адресним простором корпоративної мережі застосовуються методи CIDR (Classless Inter-Domain Routing) та VLSM (Variable Length Subnet Mask), які є ключовими компонентами сучасних мереж. CIDR забезпечує гнучке керування IP-адресами, а VLSM дозволяє ефективно використовувати IP-адресний простір шляхом розділення мереж на підмережі різного розміру. VLSM часто використовується для внутрішніх мереж, оптимізуючи розподіл адрес, тоді як CIDR революціонізував виділення адрес у глобальному масштабі. Вони взаємодіють у безкласовій маршрутизації.

Таблиця 3.1 – Блок адрес мережі та кількість вузлів в кожній з підмереж

№	Блок адрес	LAN_1	LAN_2	LAN_3	LAN_4	LAN_5
17	172.24.144.0/21	45	39	240	249	168

Щоб розділити мережу за організаційними підрозділами магазинів музичних інструментів, слід враховувати логіку функціонального або

структурного поділу підмереж (див. розділ 1). Мережі підприємства ділять за відділами або підрозділами.

LAN_1 – підрозділ маркетинговий.

LAN_2 – підрозділ виконавчий.

LAN_3 – крамниця 1.

LAN_4 – підрозділ комерційний.

LAN_5 – крамниця 2.

LAN_6 – IT-відділ.

Перш за все, необхідно визначити оптимальний розмір кожної підмережі. Для цього потрібно враховувати кількість пристроїв, які будуть підключені до кожної крамниці, а також майбутнє розширення мережі. Для 6 підмереж використаний підхід VLSM.

Спочатку визначається необхідна кількість бітів для ідентифікації підмереж: Для 6 підмереж потрібно щонайменше 3 біти (2^3 = 8, що дозволяє мати до 8 підмереж).

Виконується розрахунок нової маски підмережі. Вихідна маска /21 означає, що для адрес хоста доступно 11 бітів (32 - 21 = 11). Для створення 6 підмереж ми "позичаються" 3 біти з цих 11, залишаючи 8 бітів для адрес хостів. Отже, нова маска підмережі буде /24 (21 + 3 = 24).

Таким чином, кожна підмережа матиме маску /24, що дозволить мати 254 хости (2^8 - 2 = 254) в кожній підмережі (враховуючи, що адреси мережі та broadcast не можуть бути використані для хостів).

Розподіл адресного простору наведено в таблиці 3.2.

Таблиця 3.2 – Схема адресації підмереж підприємства

Назва мережі	Необхідна кількість вузлів	Виділена кількість вузлів	Адреса підмережі	Префікс	Діапазон допустимих IP-адрес вузлів
LAN_4	249	254	172.24.144.0 255.255.255.0	/24	172.24.144.1 - 172.24.144.254
LAN_3	240	254	172.24.145.0 255.255.255.0	/24	172.24.145.1 - 172.24.145.254
LAN_5	168	254	172.24.146.0 255.255.255.0	/24	172.24.146.1 - 172.24.146.254
LAN_1	45	62	172.24.147.0 255.255.255.192	/26	172.24.147.1 - 172.24.147.62
LAN_2	39	62	172.24.147.64 255.255.255.192	/26	172.24.147.65 - 172.24.147.126
LAN_6	27	30	172.24.147.128 255.255.255.224	/27	17.24.147.129 - 17.24.147.158

Підмережі двох крамниць музичних інструментів мають бути поділені на окремі сегменти для обмеження трафіку. В кожній крамниці такими сегментами є: торгівельний зал, адміністрація магазину, IT-підрозділ, сегмент для IP-камер відеонагляду в крамниці.

Віртуальні мережі (VLAN) є ефективним рішенням для сегментування мережевого трафіку, що особливо актуально для організацій з декількома підрозділами або філіями. У випадку двох крамниць музичних інструментів, поділ їхніх підмереж на окремі сегменти за допомогою VLAN є обґрунтованим та стратегічно вигідним.

Основна мета впровадження VLAN – це обмеження broadcast-трафіку та покращення загальної продуктивності мережі. В музичних крамницях, де може бути розгорнуто декілька касових апаратів, систем обліку товарів, а також мережеве обладнання для демонстрації інструментів (наприклад, цифрових піаніно або гітар з підсилювачами), broadcast-трафік може значно збільшуватися. Розділення цих пристроїв на окремі VLAN дозволяє ізолювати трафік кожної крамниці, запобігаючи перевантаженню мережі та підвищуючи її стабільність.

Крім того, VLAN забезпечують підвищену безпеку. Розділяючи мережу на логічні сегменти, можна обмежити доступ між різними частинами мережі. Наприклад, можна встановити правила, які дозволяють касовим апаратам мати доступ лише до серверів обліку, але не до інших пристроїв в мережі. Це зменшує ризик поширення шкідливого програмного забезпечення або несанкціонованого доступу до конфіденційних даних.

Впровадження VLAN вимагає ретельного планування та налаштування мережевого обладнання. Необхідно визначити, які пристрої будуть належати до кожного VLAN, та налаштувати маршрутизацію між цими мережами. Проте, початкові інвестиції у правильне налаштування VLAN повністю виправдовуються за рахунок покращеної продуктивності, безпеки та керованості мережі музичних крамниць.

Таблиця 3.3 – Схема адресації мереж VLAN крамниці №2

Назва	Розмір	Адреса	Префікс мережі	Діапазон адрес
Trading_area	62	172.24.145.0 255.255.255.192	/26	172.24.145.1 - 172.24.145.62
Office	62	172.24.145.64 255.255.255.192	/26	172.24.145.65 - 172.24.145.126
Cameras	62	172.24.145.128 255.255.255.192	/26	172.24.145.129 - 172.24.145.190
Managment	14	172.24.145.192 255.255.255.240	/28	172.24.145.193 - 172.24.145.206

Таблиця 3.4 – Схема адресації мереж VLAN крамниці №1

Назва	Розмір	Адреса	Префікс мережі	Діапазон адрес
Trading_area	62	172.24.146.0 255.255.255.192	/26	172.24.146.1 - 172.24.146.62
Office	62	172.24.146.64 255.255.255.192	/26	172.24.146.65 - 172.24.146.126
Cameras	62	172.24.146.128 255.255.255.192	/26	172.24.146.129 - 172.24.146.190
Managment	14	172.24.146.192 255.255.255.240	/28	172.24.146.193 - 172.24.146.206

Для каналів між роутерами рівня ядра корпоративної мережі крамниць музичних інструментів використовується блок адрес 10.1.17.0/24. Поділ на підмережі здійснюється за допомогою методу VLSM. Щоб підтримувати сегмент мережі, що складається з 2 вузлів, потрібна підмережа з маскою /30 (оскільки 2^2 - 2 = 2). Для цього позбавляємо 2 біти справа. В результаті отримуємо 64 підмережі по 2 вузли кожна. У таблиці 3.5 наведено схему адресації каналів між маршрутизаторами.

Таблиця 3.5 – Схема адресації каналів між маршрутизаторами

Назва підмережі	Адреса підмережі	Префікс	Діапазон допустимих IP-адрес вузлів	Широкомовна адреса
WAN_1	10.1.17.0	/30	10.1.17.1-10.1.17.2	10.1.17.3
WAN_2	10.1.17.4	/30	10.1.17.5-10.1.17.6	10.1.17.7
WAN_3	10.1.17.8	/30	10.1.17.9-10.1.17.10	10.1.17.11
WAN_4	10.1.17.12	/30	10.1.17.13-10.1.17.14	10.1.17.15

При розділі адресного простору важливо врахувати резервування адрес в кожній підмережі для майбутніх потреб, таких як додавання нових пристроїв або розширення функціональності.

Для ефективного управління IP-адресами в кожній підмережі необхідно за технічними вимогами використовувати DHCP-сервер, який автоматично призначає IP-адреси пристроям.

Розрахунок схеми адресації активних мережних пристроїв у корпоративній мережі крамниць музичних інструментів виконується відповідно до схеми структурної комплексу технічних засобів КС КМІ з врахуванням інтерфейсів підключення каналів WAN та локальних мереж LAN до маршрутизаторів.

Таблиця 3.6 – Схема адресації маршрутизаторів КС КМІ

Пристрій	Інтерфейс	IP-адрес	Маска мережі	Префікс
Litvunenko_R1	Gig3/0	172.24.147.1	255.255.255.0	/24
	Gig4/0	172.24.144.1	255.255.255.0	/24
	Serial1/0	10.1.17.1	255.255.255.252	/30
	Serial2/0	10.1.17.5	255.255.255.252	/30
	Gig0/0	10.1.17.9	255.255.255.252	/30
Litvunenko_R2	Gig0/0	10.1.17.14	255.255.255.252	/30
	Gig3/0	172.24.145.1	255.255.255.0	/24
	Gig4/0	172.24.145.2	255.255.255.0	/24
Litvunenko_R3	Serial1/0	10.1.17.2	255.255.255.252	/30
	Serial2/0	10.1.17.6	255.255.255.252	/30
	Gig3/0	209.165.202.1	255.255.255.252	/30
	Gig4/0	172.24.147.129	255.255.255.224	/27
Litvunenko_R4	Gig0/0	10.1.17.10	255.255.255.252	/30
	Gig3/0	172.24.146.1	255.255.255.0	/24
	Gig4/0	172.24.146.2	255.255.255.0	/24
Litvunenko_R5	Gig3/0	172.24.147.65	255.255.255.192	/26
	Gig4/0	64.100.13.1	255.255.255.252	/30
Rout_ISP	Gig4/0	209.165.201.1	255.255.255.252	Налаштовані відповідно
	Gig0/0	209.165.202.1	255.255.255.252	/30
	Gig6/0	64.100.13.2	255.255.255.252	/30

Адреси SVI-інтерфейсів комутаторів налаштовано відповідно до схеми сегментації мережі КС КМІ.

Таблиця 3.7 – Схема адресації SVI-інтерфейсів комутаторів

Підмережа	Пристрій	IP-адрес	Маска мережі	Адреса шлюзу
LAN_1	Litvunenko_Sw1	172.24.147.2	255.255.255.192	172.24.147.1
LAN_2	Litvunenko_Sw2	172.24.147.66	255.255.255.192	172.24.147.65
LAN_3	Litvunenko_Sw3.1	172.24.145.130	255.255.255.240	172.24.145.129
	Litvunenko_Sw3.2	172.24.145.131	255.255.255.240	172.24.145.129
LAN_4	Litvunenko_Sw4	172.24.144.2	255.255.255.0	172.24.144.1
LAN_5	Litvunenko_Sw5.1	172.24.146.194	255.255.255.240	172.24.186.193
	Litvunenko_Sw5.2	172.24.146.195	255.255.255.240	172.24.186.193

Отримана топологічна схеми корпоративної мережі наведена на рисунку 3.1

Топологічна схема КС КМІ, що складається з мережі офісного приміщення, двох мереж крамниць, віддаленої мережі офісу виконавчої служби та мережі провайдера послуг Інтернету, представляє собою складну систему, яка потребує ретельного планування, впровадження та управління.

Особливої уваги потребують мережі крамниць, які, окрім стандартного обладнання, включають в себе IP-камери та пристрої Інтернету речей (IoT). Впровадження цих технологій дозволяє покращити безпеку, здійснювати моніторинг товарів та оптимізувати операційні процеси. Проте, використання IP-камер та пристроїв IoT також створює додаткові вимоги до мережевої інфраструктури, зокрема щодо пропускної здатності та безпеки. Необхідно забезпечити достатню пропускну здатність для передачі відеопотоку з IP-камер та даних з пристроїв IoT, а також захистити мережу від потенційних кіберзагроз, які можуть бути спрямовані на ці пристрої.

Значна відстань між мережами крамниць (3 км та 9 км) зумовила використання оптоволоконного кабелю для з'єднання. Оптоволокно є оптимальним рішенням для передачі даних на великі відстані, оскільки воно забезпечує високу пропускну здатність, низький рівень затримки та стійкість до електромагнітних перешкод.

Надійне з'єднання з мережею провайдера послуг Інтернету (ISP) є ключовим для забезпечення безперебійної роботи всієї мережі. Необхідно обрати провайдера з надійною інфраструктурою та високим рівнем обслуговування.

Віддалена мережа офісу виконавчої служби потребує безпечного та стабільного з'єднання з основною мережею офісного приміщення. Для цього необхідно використовувати віртуальну приватну мережу (VPN), яка забезпечує шифроване з'єднання між двома мережами.

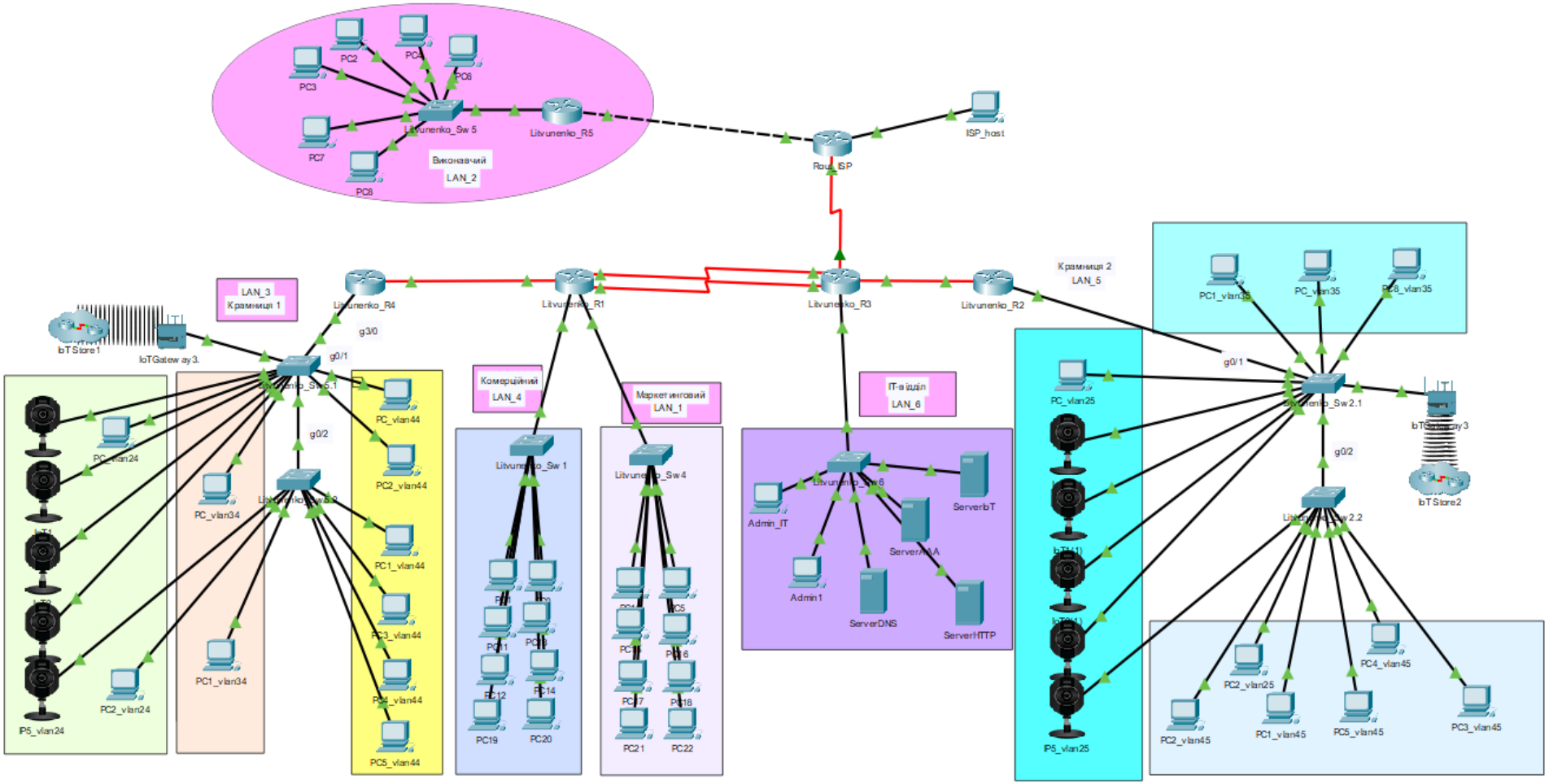


Рисунок 3.1 – Топологічна схема корпоративної мережі КМІ

3.2 Налаштування моделі комп’ютерної мережі

3.2.1 Налаштування маршрутизаторів КС КМІ

Налаштування маршрутизаторів КС КМІ виконується за технічними вимогами до розробки. Для мережі підприємства передбачає кілька ключових етапів, включаючи базову конфігурацію, налаштування IP-адрес та доменних імен, настройку маршрутизації, та налаштування безпеки.

Базова конфігурація є важливим етапом налаштувань, що передбачає налаштування:

– вхід в систему: доступ до конфігураційного інтерфейсу маршрутизатора за протоколом SSH або консольний порт;

– налаштування параметрів користувача: створення облікового запису користувача із зазначенням відповідних прав доступу.;

– призначення паролів входу до ОС маршрутизатора та ліній VTY, а також для консольного доступу на пристрій;

– встановлення унікального імені роутера для легшої ідентифікації у мережі;

– є необхідність налаштування часового поясу для коректного ведення журналів та інших процесів.

– надання IP-адрес та масок мережі для фізичних та віртуальних інтерфейсів маршрутизатора;

– зазначення DNS-серверів для перетворення доменних імен в IP-адреси;

– підключається сервіс шифрування паролів, що зберігаються у відкритому вигляді;

– створення ключа RSA для шифрування;

– налаштування доменного імені для ідентифікації роутеру в мережі, використовується замість IP-адреси (складно запам'ятати) для доступу до роутера.

Приклад базового налаштування маршрутизатору Litvunenko_R4 наведено на рисунку 3.2.

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname Litvunenko_R4
Litvunenko_R4(config)#no ip domain-lookup
Litvunenko_R4(config)#service password-encryption
Litvunenko_R4(config)#enable secret cisco
Litvunenko_R4(config)#line console 0
Litvunenko_R4(config-line)#password cisco
Litvunenko_R4(config-line)#login
Litvunenko_R4(config-line)#exit
Litvunenko_R4(config)#line vty 0 15
Litvunenko_R4(config-line)#password cisco
Litvunenko_R4(config-line)#login local
Litvunenko_R4(config-line)#trans inp ssh
Litvunenko_R4(config-line)#exit
Litvunenko_R4(config)#banner motd #123-21 Litvunenko. Login for authorized users only#
Litvunenko_R4(config)#username 12321litv password cisco
Litvunenko_R4(config)#ip domain-name Litvunenko_R4.com
Litvunenko_R4(config)#cryp key g r
The name for the keys will be: Litvunenko_R4.Litvunenko_R4.com
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

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

Рисунок 3.2 – Налаштування маршрутизатору Litvunenko_R4

При налаштуванні послідовного інтерфейсу (serial interface) маршрутизатора, необхідно встановити певні параметри для забезпечення коректної роботи та зв'язку з іншими пристроями. Ці параметри включають:

– налаштування пропускної здатності (bandwidth) Важливо, щоб djyf була однаковою на обох кінцях послідовного з'єднання, інакше зв'язок буде неможливий або нестабільний. Використане стандартне значення 128 Mbps;

–інформацію про clock rate, особливо на стороні DCE (Data Communications Equipment), в даному випадку 128000;

– вибір DCE-інтерфейсу, якому необхідно задати clock rate;

– підключити живлення інтерфейсу.

```
Litvunenko_R1(config)#int s2/0
Litvunenko_R1(config-if)#description to R3
Litvunenko_R1(config-if)#ip add 10.1.17.5 255.255.255.252
Litvunenko_R1(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial2/0, changed state to down
Litvunenko_R1(config-if)#clock rate 128000
Litvunenko_R1(config-if)#bandwidth 128
Litvunenko_R1(config-if)#exit
```

Рисунок 3.3 – Налаштування маршрутизатору Litvunenko_R4

Наступним важливим кроком налаштування роутера є налаштування маршрутизації. Маршрутизація – це процес визначення найкращого шляху для пересилання пакетів даних між мережами. Маршрутизатори КС КМІ налаштовані на застосування протоколу маршрутизації EIGRP для визначення найкращого шляху.

Застосування EIGRP зумовлено його перевагами та технічними вимогами. До переваг можна віднести: використання алгоритму Diffusing Update Algorithm (DUAL) для швидкого визначення альтернативних шляхів у разі збою основного маршруту; підтримку VLSM; використання комплексної метрики (bandwidth + delay + load + reliability) каналу та автоматичне оновлення маршрутів.

```
Litvunenko_R1(config)#router eigrp 14
Litvunenko_R1(config-router)#redistribute static
Litvunenko_R1(config-router)#network 10.1.17.4 0.0.0.3
Litvunenko_R1(config-router)#network 10.1.17.4 0.0.0.3
Litvunenko_R1(config-router)#network 10.1.17.8 0.0.0.3
Litvunenko_R1(config-router)#network 172.24.147.0 0.0.0.63
Litvunenko_R1(config-router)#network 172.24.144.0 0.0.0.255
Litvunenko_R1(config-router)#pas g3/0
Litvunenko_R1(config-router)#pas g4/0
Litvunenko_R1(config-router)#exit
Litvunenko_R1(config)#ip route 0.0.0.0 0.0.0.0 209.165.202.1
%DUAL-5-NBRCHANGE: IP-EIGRP 14: Neighbor 10.1.17.10 (GigabitEthernet0/0) is up: new
adjacency
```

Рисунок 3.4 – Приклад налаштування протоколу на Litvunenko_R1

При налаштуванні EIGRP необхідно визначити:

– авторизовану зону (в прикладі 14);

– розповсюдження статичних маршрутів;

– мережі маршрутизації;

–маршрут за замовчування до маршрутизатору ISP (обладнання провайдера);

– поширення оновлень тупікових LAN.

Результатом належного налаштування маршрутизації мережі – є таблиці маршрутизації на роутерах.

```
Litvunenko_R1#show ip route
Codes: C - connected, S - static, I - IGRP, 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 209.165.202.1 to network 0.0.0.0

     10.0.0.0/30 is subnetted, 4 subnets
C       10.1.17.0 is directly connected, Serial1/0
C       10.1.17.4 is directly connected, Serial2/0
D       10.1.17.12 [90/20512256] via 10.1.17.2, 02:15:45, Serial1/0
                   [90/20512256] via 10.1.17.6, 02:15:45, Serial2/0
C       10.1.17.16 is directly connected, GigabitEthernet5/0
     172.24.0.0/16 is variably subnetted, 9 subnets, 6 masks
D       172.24.0.0/16 [90/20514816] via 10.1.17.2, 02:15:45, Serial1/0
                      [90/20514816] via 10.1.17.6, 02:15:45, Serial2/0
D EX    172.24.144.0/21 [170/25632000] via 10.1.17.2, 01:27:12, Serial1/0
                        [170/25632000] via 10.1.17.6, 01:27:12, Serial2/0
C       172.24.144.0/24 is directly connected, GigabitEthernet4/0
D       172.24.146.0/26 [90/28416] via 10.1.17.18, 02:15:16, GigabitEthernet5/0
D       172.24.146.64/26 [90/28416] via 10.1.17.18, 02:15:16, GigabitEthernet5/0
D       172.24.146.128/26 [90/28416] via 10.1.17.18, 02:15:16, GigabitEthernet5/0
D       172.24.146.192/28 [90/28416] via 10.1.17.18, 02:15:16, GigabitEthernet5/0
C       172.24.147.0/26 is directly connected, GigabitEthernet3/0
D       172.24.147.128/27 [90/20512256] via 10.1.17.2, 02:15:45, Serial1/0
                          [90/20512256] via 10.1.17.6, 02:15:45, Serial2/0
D    209.165.201.0/24 [90/21026560] via 10.1.17.6, 01:22:01, Serial2/0
                      [90/21026560] via 10.1.17.2, 01:22:00, Serial1/0
     209.165.202.0/30 is subnetted, 1 subnets
D       209.165.202.0 [90/21024000] via 10.1.17.6, 01:22:01, Serial2/0
                      [90/21024000] via 10.1.17.2, 01:22:01, Serial1/0
S*   0.0.0.0/0 [1/0] via 209.165.202.1
```

Рисунок 3.5 – Приклад таблиці маршрутизації на Litvunenko_R1

Працездатність мережі підприємства КМІ означає здатність мережі функціонувати належним чином, забезпечуючи передачу даних між пристроями. Перевірка працездатності мережі включає в себе тестування зв'язку між комп'ютерами та оцінку роботи маршрутизаторів та комутаторів. Перевірку можна здійснити надсиланням тестових пакетів даних. Важливо переконатися у коректності маршрутизації та відсутності помилок в передачі даних.

Fire	Last Status	Source	Destination	Type	Color
	Successful	ServerAAA	PC1	ICMP	
	Successful	IP5_vlan24	ServerAAA	ICMP	
	Successful	PC_vlan44	PC1	ICMP	
	Successful	PC10	PC1	ICMP	
	Successful	PC2_vlan25	PC1_vlan35	ICMP	

Рисунок 3.6 – Пінгування хостів в різних підмережах КС КМІ

Протокол DHCP виконує автоматичну та динамічну адресацію пристроїв в мережі. Це дозволяє зменшити ручну роботу адміністраторів та ефективніше використовувати IP-адреси, а також забезпечує простоту в налаштуванні пристроїв. Також DHCP забезпечує легке переміщення пристроїв по мережі без зміни їх IP-адрес. На роутерах Cisco налаштування DHCP включає створення DHCP-сервера, визначення пулу адрес, мережі для якої призначається пул та додаткових параметрів (шлюз, DNS, excluded-address).

```
Litvunenko_R4(config)#ip dhc ex 172.24.146.1 172.24.146.10
Litvunenko_R4(config)#ip dhc ex 172.24.146.65 172.24.146.75
Litvunenko_R4(config)#ip dhc ex 172.24.146.129 172.24.146.139
Litvunenko_R4(config)#ip dhc pool POOL_VLAN24
Litvunenko_R4(dhcp-config)#net 172.24.146.0 255.255.255.192
Litvunenko_R4(dhcp-config)#def 172.24.146.1
Litvunenko_R4(dhcp-config)#dns 172.24.147.132
Litvunenko_R4(dhcp-config)#ip dhc pool POOL_VLAN34
Litvunenko_R4(dhcp-config)#net 172.24.146.64 255.255.255.192
Litvunenko_R4(dhcp-config)#def 172.24.146.65
Litvunenko_R4(dhcp-config)#dns 172.24.147.132
Litvunenko_R4(dhcp-config)#ip dhc pool POOL_VLAN44
Litvunenko_R4(dhcp-config)#net 172.24.146.128 255.255.255.192
Litvunenko_R4(dhcp-config)#def 172.24.146.129
Litvunenko_R4(dhcp-config)#dns 172.24.147.132
Litvunenko_R4(dhcp-config)#
```

Рисунок 3.7 – Приклад налаштування DHCP на маршрутизаторі Litvunenko_R4

Перевірити результат можна застосувавши команду show ip dhcp binding.

```
Litvunenko_R4#show ip dhcp binding
IP address       Client-ID/              Lease expiration        Type
                 Hardware address
172.24.146.11    000A.F351.C9C0          --                      Automatic
172.24.146.13    0004.9A82.358D          --                      Automatic
172.24.146.14    00D0.D3A5.AD93          --                      Automatic
172.24.146.17    0002.4A58.9586          --                      Automatic
172.24.146.16    0002.4A12.DCBC          --                      Automatic
172.24.146.15    000A.4129.D001          --                      Automatic
172.24.146.12    0005.5E40.09E7          --                      Automatic
172.24.146.76    0060.5CDD.3D24          --                      Automatic
172.24.146.77    00D0.D386.AAEE          --                      Automatic
172.24.146.142   00D0.BA69.A5E4          --                      Automatic
172.24.146.141   0030.A3B4.31D1          --                      Automatic
172.24.146.143   0001.6381.7863          --                      Automatic
172.24.146.144   0050.0FDA.2A35          --                      Automatic
172.24.146.140   0002.16E2.4C39          --                      Automatic
172.24.146.145   0090.2BAD.7B0E          --                      Automatic
```

Рисунок 3.8 – Результат застосування DHCP на Litvunenko_R4

Для підтримки технології DHCP також відповідним чином повинен бути налаштований хост даної мережі.

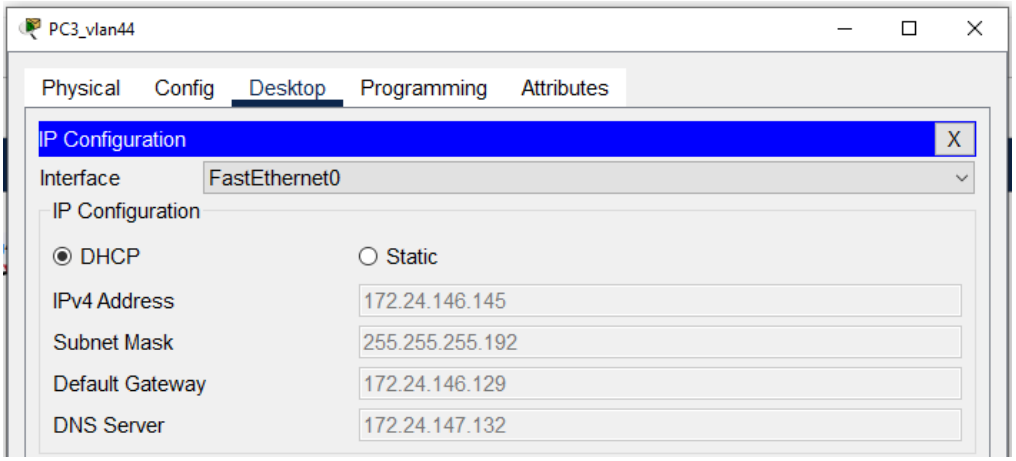


Рисунок 3.9 – Результат застосування DHCP на PC3_vlan44

Відповідно до логічної топології корпоративної мережі КМІ, підмережа крамниць сегментована з використанням технології віртуальних мереж (VLAN). Отже, конфігурація маршрутизаторів Litvunenko_R4 та Litvunenko_R2 потребує налаштування для підтримки відповідного протоколу міжвіртуальної маршрутизації (наприклад, 802.1Q trunking, inter-VLAN routing на основі router-on-a-stick або використання Layer 3 switch). Це дозволить забезпечити коректну комунікацію між сегментами мережі та гарантувати ефективну передачу даних між крамницями та центральним офісом КМІ.

Підмережа крамниці розподілена на три підмережі VLAN. Номери та назви мереж VLAN представлено в 3.8.

Таблиця 3.8 – Мережі VLAN

Номер VLAN	Ім’я VLAN	Примітка
1	Default	Не використовується
24	Trading_area	Для зани продажу
34	Office	Для адміністрації крамниці
44	Cameras	Для IP-камер
99	Managment	Для управління пристроями
100	Native	Власна мережі

```
Litvunenko_Sw5.1(config)#vlan 24
Litvunenko_Sw5.1(config-vlan)#name Trading_area
Litvunenko_Sw5.1(config-vlan)#vlan 34
Litvunenko_Sw5.1(config-vlan)#name Office
Litvunenko_Sw5.1(config-vlan)#vlan 44
Litvunenko_Sw5.1(config-vlan)#name Cameras
Litvunenko_Sw5.1(config-vlan)#vlan 99
Litvunenko_Sw5.1(config-vlan)#name Management
Litvunenko_Sw5.1(config-vlan)#vlan 100
Litvunenko_Sw5.1(config-vlan)#name Native
Litvunenko_Sw5.1(config-vlan)#exit
```

Рисунок 3.10 – Номери та назви мереж VLAN крамниці

Розподіл портів для окремих мереж VLAN є важливим етапом у побудові та підтримці ефективної та безпечної мережевої інфраструктури.

Ізоляція трафіку між різними VLAN зменшує широкомовний домен, що, в свою чергу, мінімізує мережеві затримки та збільшує загальну продуктивність. Розподіляючи порти між VLAN, адміністратори можуть контролювати, які пристрої мають доступ до певних мережевих ресурсів, тим самим обмежуючи поширення шкідливого програмного забезпечення або несанкціонованого доступу.

Таблиця 3.9 – Розподіл портів для окремих мереж VLAN

Назва	VLAN	Порти
Trading_area	24	f0/6-f0/11
Office	34	f0/13-f0/17
Cameras	44	f0/18-f0/23

Адресація пристроїв в підмережі крамниці 1 КС КМІ представлена в таблиці 3.10.

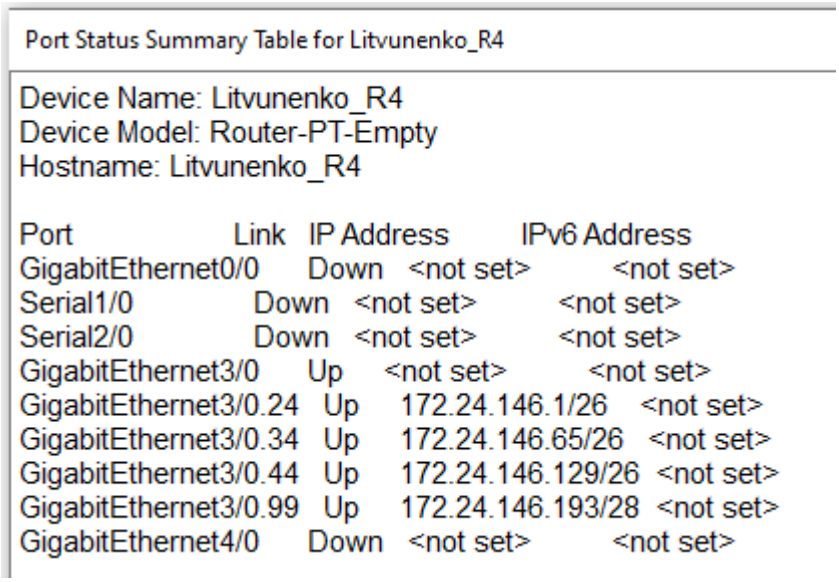
Таблиця 3.10 – Адресація пристроїв в підмережі крамниці 1 КС КМІ

Пристрій	Інтерфейс	Адреса	Маска мережі	Шлюз	VLAN
Litvunenko_Sw4.1	SVI	172.24.145.194	255.255.255.240	172.24.145.193	99
Litvunenko_Sw4.2	SVI	172.24.145.195	255.255.255.240	172.24.145.193	99
Litvunenko_R4	G0/0.24	172.24.145.1	255.255.255.192	-	24
	G0/0.34	172.24.145.65	255.255.255.192	-	34
	G0/0.44	172.24.145.129	255.255.255.192	-	44
	G0/0.99	172.24.145.193	255.255.255.240	-	99

Приклад налаштування протоколу , 802.1Q trunking в мережах VLAN маршрутизатору Litvunenko_R4 наведено на рисунку 3.11. Фізичний інтерфейс G3/0 поділений на чотири віртуальні. Кожному призначено IP-адресу за таблицею 3.10 та застосовано протокол 802.1Q.

```
Litvunenko_R4(config-if)#int g3/0.24
Litvunenko_R4(config-subif)#enc d 24
Litvunenko_R4(config-subif)#ip add 172.24.146.1 255.255.255.192
Litvunenko_R4(config-subif)#no shut
Litvunenko_R4(config-subif)#exit
Litvunenko_R4(config)#int g3/0.34
Litvunenko_R4(config-subif)#enc d 34
Litvunenko_R4(config-subif)#ip add 172.24.146.65 255.255.255.192
Litvunenko_R4(config-subif)#no shut
Litvunenko_R4(config-subif)#exit
Litvunenko_R4(config)#int g3/0.44
Litvunenko_R4(config-subif)#enc d 44
Litvunenko_R4(config-subif)#ip add 172.24.146.129 255.255.255.192
Litvunenko_R4(config-subif)#no shut
Litvunenko_R4(config-subif)#exit
Litvunenko_R4(config)#int g3/0.99
Litvunenko_R4(config-subif)#enc d 99
Litvunenko_R4(config-subif)#ip add 172.24.146.193 255.255.255.240
Litvunenko_R4(config-subif)#no shut
Litvunenko_R4(config-subif)#exit
%LINK-5-CHANGED: Interface GigabitEthernet3/0, changed state to up
```

Рисунок 3.10 – Налаштування протоколу 802.1Q trunking



Port Status Summary Table for Litvunenko_R4

Device Name: Litvunenko_R4
Device Model: Router-PT-Empty
Hostname: Litvunenko_R4

Port	Link	IP Address	IPv6 Address
GigabitEthernet0/0	Down	<not set>	<not set>
Serial1/0	Down	<not set>	<not set>
Serial2/0	Down	<not set>	<not set>
GigabitEthernet3/0	Up	<not set>	<not set>
GigabitEthernet3/0.24	Up	172.24.146.1/26	<not set>
GigabitEthernet3/0.34	Up	172.24.146.65/26	<not set>
GigabitEthernet3/0.44	Up	172.24.146.129/26	<not set>
GigabitEthernet3/0.99	Up	172.24.146.193/28	<not set>
GigabitEthernet4/0	Down	<not set>	<not set>

Рисунок 3.11 – Результат перевірки налаштування 802.1Q

Налаштування VLAN на комутаторі Litvunenko_Sw4.1 вимагає декількох ключових кроків та компонентів. Основні етапи налаштування включають:

– створення VLAN командою vlan [ідентифікатор VLAN] створюється віртуальна мережа. Ідентифікатор VLAN – це число від 1 до 4094. Далі, за допомогою команди name [назва VLAN] можна присвоїти VLAN зрозуміле ім'я;

– призначення портів VLAN для цього потрібно вибраний інтерфейс комутатора налаштувати для роботи з певним VLAN. Це робиться за допомогою команд switchport mode access та switchport access vlan [ідентифікатор VLAN]. switchport mode access вказує, що порт працює в режимі доступу (access mode), при якому він може передавати трафік лише одного VLAN.

```
Litvunenko_Sw5.1(config-if-range)#int r f0/6-11
Litvunenko_Sw5.1(config-if-range)#sw m a
Litvunenko_Sw5.1(config-if-range)#no shut

%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to down

%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to down

%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to down

%LINK-5-CHANGED: Interface FastEthernet0/9, changed state to down

%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to down

Litvunenko_Sw5.1(config-if-range)#sw a v 24
Litvunenko_Sw5.1(config-if-range)#int r f0/12-16
Litvunenko_Sw5.1(config-if-range)#sw m a
Litvunenko_Sw5.1(config-if-range)#no shut
```

Рисунок 3.12 – Призначення портів VLAN

В підмережі крамниці КС КМІ необхідно передавати трафік трьох VLAN між двома комутаторами. В такому випадку потрібно налаштувати Trunk порт. Це робиться за допомогою команд switchport mode trunk та switchport trunk encapsulation dot1q (для протоколу 802.1Q). Далі, команда switchport trunk allowed vlan [список VLAN] дозволяє визначити, які VLAN будуть передаватися через Trunk.

```
Litvunenko_Sw5.1(config)#int g0/1
Litvunenko_Sw5.1(config-if)#switchport mode trunk
Litvunenko_Sw5.1(config-if)#switchport trunk native vlan 100
Litvunenko_Sw5.1(config-if)#switchport trunk allowed vlan 24,34,44,99-100
Litvunenko_Sw5.1(config-if)#no shutdown
Litvunenko_Sw5.1(config-if)#exit
```

Рисунок 3.13 – Налаштування Trunk порт

VLAN 99 використовується як VLAN управління. Призначення IP-адрес виконане відповідно до таблиці 3.10. З цієї мережі призначаються адреси для роутера Litvunenko_R4 та комутаторів.

```
Litvunenko_Sw5.1(config)#int vlan 99
Litvunenko_Sw5.1(config-if)#description LAN Vnutr_99
Litvunenko_Sw5.1(config-if)#ip add 172.24.146.194 255.255.255.240
Litvunenko_Sw5.1(config-if)#no shut
Litvunenko_Sw5.1(config-if)#ip default-gateway 172.24.146.194
Litvunenko_Sw5.1(config)#exit
%LINK-5-CHANGED: Interface Vlan99, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up
```

Рисунок 3.14 – Налаштування VLAN 99

Перевірка налаштувань VLAN виконується командами show vlan brief та show interface [інтерфейс] switchport, що дозволяють перевірити поточні налаштування VLAN та інтерфейсів.

```
Litvunenko_Sw5.1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/17, Fa0/18, Fa0/24
24   Trading_area                     active    Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/11
34   Office                           active    Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                Fa0/16
44   Cameras                          active    Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23
99   Management                       active
100  Native                           active
```

Рисунок 3.15 – Результат перевірки налаштувань VLAN

Fire	Last Status	Source	Destination	Type	Color
	Successful	PC1_vlan44	PC2_vlan24	ICMP	
	Successful	PC_vlan44	PC1_vlan34	ICMP	
	Successful	PC1_vlan34	PC_vlan24	ICMP	
	Successful	PC_vlan24	PC_vlan44	ICMP	

Рисунок 3.17 – Результат перевірки пінгування між хостами трьох VLAN крамниці КС КМІ

3.2.2 Налаштування роботи з Інтернет

Для доступу хостів КС КМІ до мережі Інтернет використовується технологія NAT (Network Address Translation). [13]

Маршрутизатор Litvunenko_R3 є пограничним і виконуватиме трансляцію мережевих адрес. Litvunenko_R3 підтримує NAT та має внутрішній (LAN) і зовнішній (WAN) інтерфейси.

Необхідна глобальна IP-адреса, надана інтернет-провайдером (ISP), яка буде використовуватися для зв'язку з Інтернетом. Ця адреса присвоюється WAN-інтерфейсу маршрутизатора.

Налаштування технології NAT граничного маршрутизатору Litvunenko_R3: створюються пул NAT IP-адрес для підміни, зазначається IP-адреси NAT для серверу, зазначаються інтерфейси inside та outside.

```
Litvunenko_R3(config)#access-list 14 permit 172.24.144.0 0.0.7.255
Litvunenko_R3(config)#ip nat pool Internet 209.165.202.5 209.165.202.30 netmask
255.255.255.224
Litvunenko_R3(config)#ip nat inside source list 14 pool Internet
Litvunenko_R3(config)#ip nat inside source static 172.24.144.138 209.165.202.3
Litvunenko_R3(config)#ip route 0.0.0.0 0.0.0.0 209.165.202.1
Litvunenko_R3(config)#ip route 172.24.144.0 255.255.248.0 s5/0
Litvunenko_R3(config)#interface s5/0
Litvunenko_R3(config-if)#ip nat outside
Litvunenko_R3(config-if)#interface s2/0
Litvunenko_R3(config-if)#ip nat inside
Litvunenko_R3(config-if)#interface s1/0
Litvunenko_R3(config-if)#ip nat inside
Litvunenko_R3(config-if)#interface g4/0
Litvunenko_R3(config-if)#ip nat inside
Litvunenko_R3(config-if)#exit
```

Рисунок 3.18 – Налаштування NAT Litvunenko_R3

```
Litvunenko_R3#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 209.165.202.7:8   172.24.144.250:8   203.0.0.10:8       203.0.0.10:8
icmp 209.165.202.8:3   172.24.145.200:3   203.0.0.10:3       203.0.0.10:3
icmp 209.165.202.9:3   172.24.147.126:3   203.0.0.10:3       203.0.0.10:3
---  209.165.202.3     172.24.147.138     ---                ---
```

Рисунок 3.19 – Результат перевірки налаштувань NAT

3.2.3 Захист інформації в комп'ютерній системі

Для безпеки контролю доступу до мережевих ресурсів в КС КМІ застосована технологія AAA. AAA дозволяє адміністраторам централізовано управляти ідентифікацією користувачів, їхніми правами доступу та обліком їхньої активності.

При налаштуванні AAA застосований метод аутентифікації протоколом RADIUS, що дозволяює перенести процес аутентифікації на зовнішні сервери. Це забезпечує більш гнучке та централізоване управління користувачами.

Важливою складовою є налаштування авторизації, яка визначає, які ресурси та команди доступні користувачам після успішної аутентифікації. Адміністратори можуть визначати різні рівні привілеїв для різних груп користувачів, забезпечуючи таким чином відповідний рівень доступу до мережевого обладнання.

Облік (accounting) дозволяє реєструвати дії користувачів, такі як команди, які вони виконують, та час, протягом якого вони працюють в мережі. Ця інформація може бути використана для моніторингу активності, виявлення проблем та забезпечення відповідності політикам безпеки.

```
Litvunenko_R3(config)#aaa new-model
Litvunenko_R3(config)#aaa authentication login default local
Litvunenko_R3(config)#aaa authentication login Login group radius local
Litvunenko_R3(config)#line vty 0 4
Litvunenko_R3(config-line)#login authentication default
Litvunenko_R3(config-line)#radius-server host 172.24.147.138 auth-port 1645
Litvunenko_R3(config)#radius-server key radius123
Litvunenko_R3(config)#exit
Litvunenko_R3#
Litvunenko_R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Litvunenko_R3(config)#aaa authentication login SSH-LOGIN local
Litvunenko_R3(config)#line vty 0 4
Litvunenko_R3(config-line)#login authentication SSH-LOGIN
Litvunenko_R3(config-line)#transport input ssh
Litvunenko_R3(config-line)#exit
%SYS-5-CONFIG_I: Configured from console by console

Litvunenko_R3(config)#radius-server host 172.24.147.138
Litvunenko_R3(config)#radius-server key radius123
Litvunenko_R3(config)#aaa authentication login default group radius local
```

Рисунок 3.20 – Налаштування служби AAA на роутері

В ході роботи з службою виконано: налаштування аутентифікації для консольного доступу до мережевого пристрою з використанням серверу Radius, налаштування серверу Radius, оголошення ключа аутентифікації, встановлено метод аутентифікації для доступу до консольного порту та віртуальних ліній.

На сервері, що підтримуватиме AAA, необхідно налаштувати мережну конфігурацію з зазначенням імен роутерів, IP та параль. І налаштувати параметри для користувачів.

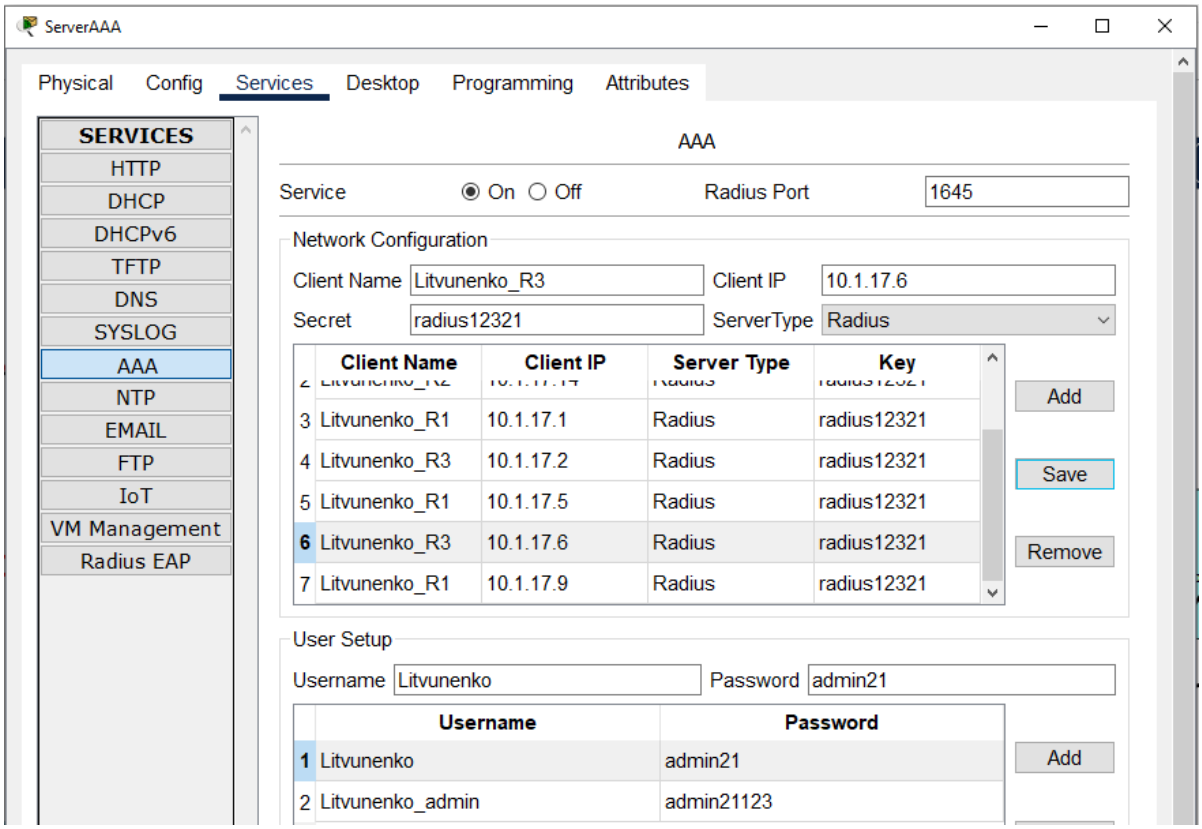


Рисунок 3.20 – Налаштування серверу AAA

```
123-21 Litvunenko. There is protection

User Access Verification

Username: Litvunenko_R2
Password:
Litvunenko_R2>en
Litvunenko_R2>enable
Password:
Litvunenko_R2#sh ver
Cisco IOS Software, C2900 Software (C2900-UNIVERSALK9-M), Version 15.1(4)M4,
```

Рисунок 3.21 – Перевірка служби AAA

В підмережі LAN_6 КС КМІ розташовані сервери підприємства. На комутаторі цієї LAN Litvunenko_Sw6 необхідно впровадити заходи безпеки для портів, де підключені сервери. В процесі необхіжно: обрати порт Swich, ввімкнути режим доступу, командою switchport port-security застосувати захисту порту, зазначити для порту кількості пристроїв, яким наданий доступ дл цього порту, ввімкнути розпізнавання MAC-адресу пристрою, що під'єднаний до порту Swich, зазначені дії комутатору на випадок неспівпадіння адрес.

switchport port-security mac-address sticky // налаштування автоматичного розпізнавання MAC-адресу з додаванням його в поточну конфігурацію

switchport port-security violation restrict // налаштування

Перевірка налаштувань безпеки порту комутатору з'єднаного з сервером IoT на прикладі Litvunenko_Sw6. Перевірка здійснюється за допомогою команди show port-security.

```
Litvunenko_Sw6#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)         (Count)
-------------------------------------------------------------------------
       Fa0/20        2           0                0          Restrict
       Fa0/21        2           0                0          Restrict
       Fa0/22        2           0                0          Restrict
       Fa0/24        2           0                0          Restrict
-------------------------------------------------------------------------
```

Рисунок 3.21 – Перевірка безпеки порту

На роутерах КС КМІ для безпеки віддаленого доступу до ліній VTY налаштований протокол SSH v2.

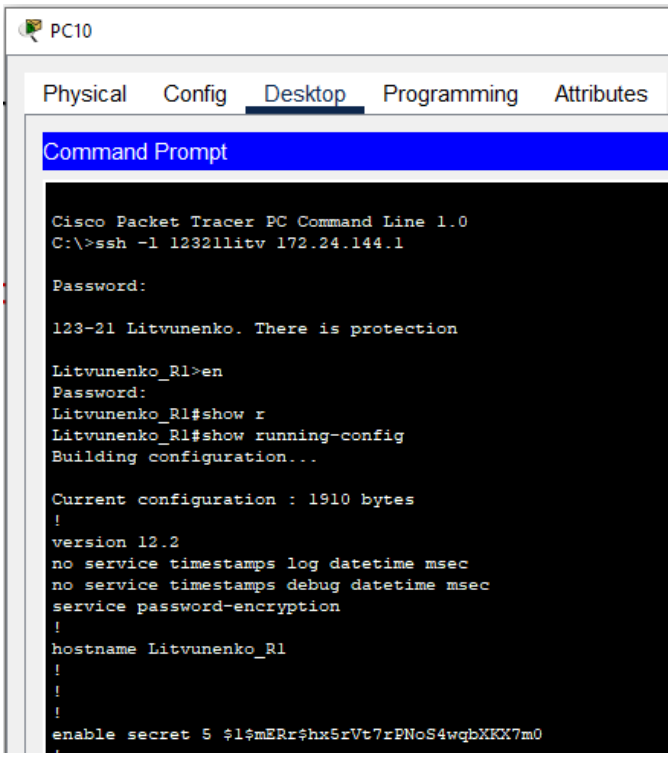


Рисунок 3.22 – Перевірка доступу а протоколом SSH

3.2.4 Налаштування віртуальної приватної мережі VPN

VPN (Virtual Private Network) в КС КМІ забезпечує захищений канал зв'язку між двома підмережами: "LAN6 Відділ ІТ" (з шлюзом Litvunenko_R3) та "LAN_1 Виконавчий підрозділ" (з шлюзом Litvunenko_R0). VPN створює віртуальну приватну мережу поверх існуючої інфраструктури, наприклад, Інтернету. Її ключові функції включають автентифікацію учасників мережі, щоб розмежувати її трафік від загального, та шифрування даних, що передаються між серверами фірми у відділі ІТ та виконавчим підрозділом, забезпечуючи конфіденційність та цілісність інформації. Таким чином, VPN гарантує безпечну передачу критично важливих даних між віддаленими підрозділами організації.

При налаштуванні тунелю обов’язково зазначаються такі кроки: зазначити мережі тунелю, обрати криптографічну політику, зазначити метод аутентифікації, група обміну ключами, виконати набор перетворень, зазначити адресу піру VPN з’єднання та інтерфейсу, зіставити кріпто МАР з вихідним інтерфейсом.

Для оцінки працездатності VPN на маршрутизаторі Litvunenko_R0 було проведено тестування. Процес включав відправку двох пакетів даних з комп'ютера PC21, розташованого у віддаленій мережі LAN_3, до комп'ютера PC14 в офісній мережі LAN_6 (згідно зі схемою на рис. 3.23). Подальший аналіз стану VPN-з'єднання здійснювався за допомогою команди show crypto ipsec sa, що дозволило оцінити параметри безпеки та переконатися у коректній роботі встановленого IPsec тунелю. Цей метод забезпечує практичну перевірку ефективності VPN-рішення.

```
Litvunenko_R5#show crypto ipsec sa

interface: Serial0/0/0
    Crypto map tag: VPN-MAP, local addr 209.165.202.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (172.24.146.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (172.24.147.128/255.255.255.224/0/0)
   current_peer 64.100.13.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 1, #pkts encrypt: 1, #pkts digest: 0
   #pkts decaps: 2, #pkts decrypt: 2, #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.: 209.165.202.1, remote crypto endpt.:64.100.13.2
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
     current outbound spi: 0x0(0)
```

Рисунок 3.27 – Перевірка технології VPN

4 РОЗРОБКА КОМПОНЕНТА СИСТЕМИ

Музичні крамниці, як і багато інших підприємств роздрібної торгівлі, все частіше інтегрують технології Інтернету речей (IoT) для оптимізації процесів, підвищення безпеки та покращення загального клієнтського досвіду. Розглянемо типову реалізацію IoT у музичній крамниці, зосереджуючись на системах виявлення та гасіння пожеж.

В основі мережі IoT у крамниці лежить бездротовий маршрутизатор (Wireless Router), який служить шлюзом для підключення розумних пристроїв до корпоративної мережі. Цей маршрутизатор отримує TCP/IP налаштування для свого інтерфейсу Internet від головного маршрутизатора мережі крамниці з діапазону адрес 172.24.145.0/24. Це гарантує інтеграцію мережі IoT з існуючою інфраструктурою крамниці, дозволяючи обмін даними та централізоване управління.

За допомогою бездротової технології WiFi, роутер мережі IoT призначає мережні налаштування "розумним речам" у крамниці.

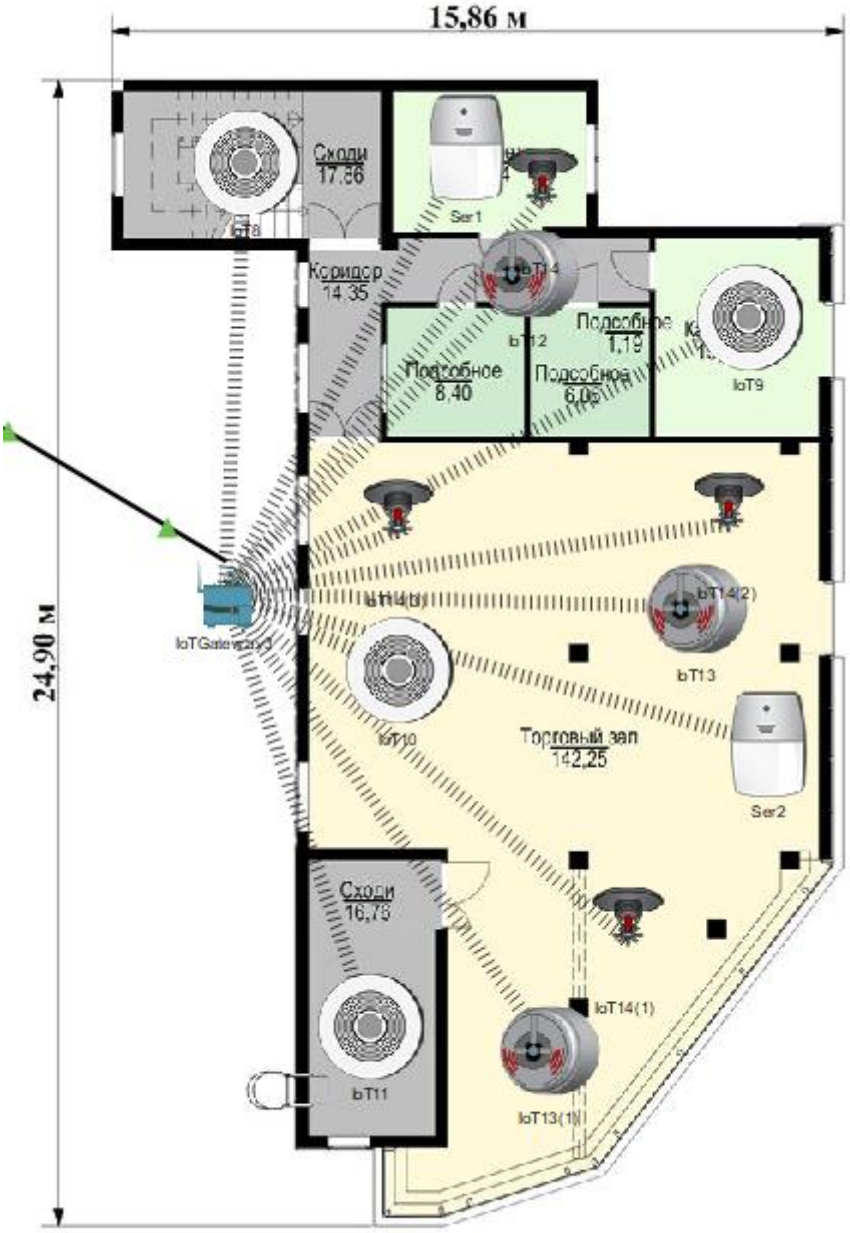


Рисунок 4.1 – Архітектура IoT Store1

Таблиця 4.1 – Мережні налаштування IoT-шлюзу

Параметр	Значення
IP-адреса інтерфейсу Internet	172.24.146.15
Маска домашньої підмережі	255.255.255.0
SSID бездротової домашньої мережі	MusicStore1
Метод автентифікації	WPA2-PSK AES
Ключ автентифікації (*пароль*)	Litvunenko

"Розумні речі" виконують задачі виявлення задимленості і сповіщення про перевищення, а також виявлення пожежі та пожежогасіння. Датчики диму стратегічно розташовані по всій крамниці для раннього виявлення задимленості, дозволяючи вживати превентивні заходи до того, як ситуація переросте в повномасштабну пожежу. Датчики тепла реагують на різке підвищення температури, що є ознакою відкритого вогню.

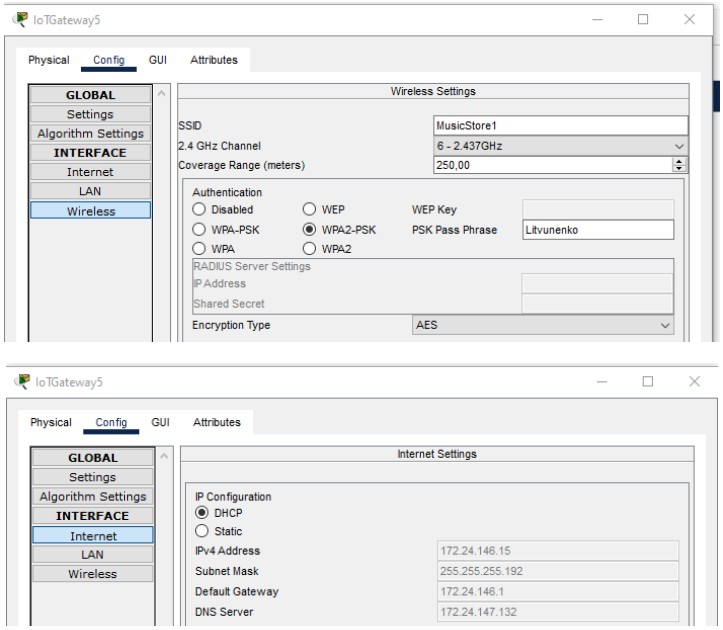


Рисунок 4.2 – Перевірка налаштувань шлюза

Ключовим елементом IoT-системи є те, що дані, зібрані "розумними речами", передаються на IoT-сервер, який розташований у підмережі "Відділ-IoT" компанії. Цей сервер виконує роль центрального хабу для обробки, аналізу та зберігання даних. Саме тут відбуваються критичні функції, такі як моніторинг стану датчиків, виявлення аномалій та ініціювання автоматичних реакцій.

IoT-сервер надає веб-інтерфейс, що дозволяє користувачам (наприклад, персоналу крамниці або службі безпеки) проглядати стан "розумних речей" в реальному часі. Це забезпечує видимість та контроль над системою пожежної безпеки. Можна побачити, які датчики активні, які рівні задимленості або температури фіксуються, і який стан відповідних пристроїв пожежогасіння (наприклад, готовність до активації).

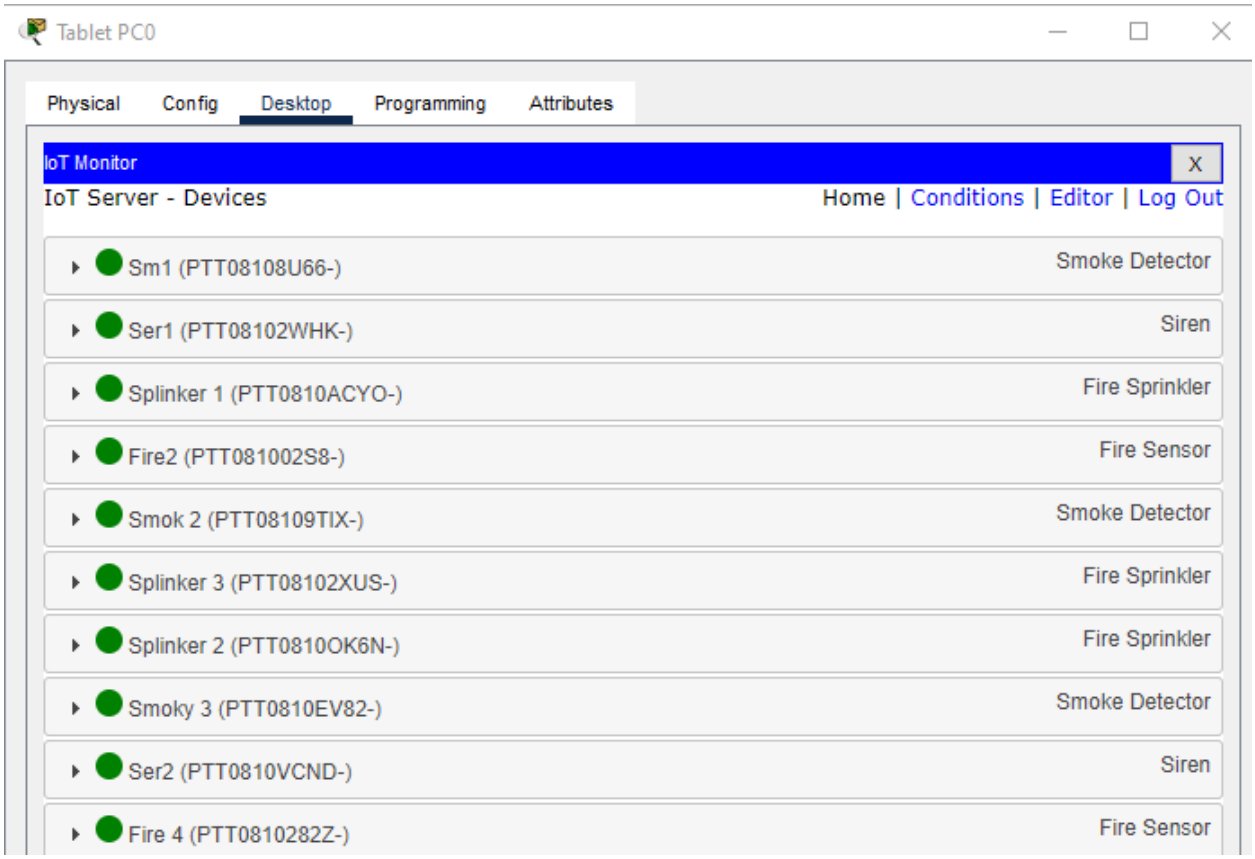


Рисунок 4.3 – Перевірка підключення речей до серверу IoT

На додаток до моніторингу, сервіси IoT-серверу надають можливість створення сценаріїв керування "розумними речами". Це означає, що можна налаштувати автоматичні дії у відповідь на певні події. Наприклад, якщо датчик диму фіксує перевищення встановленого порогу задимленості, система може автоматично:

– надіслати сповіщення на мобільні пристрої персоналу крамниці;
– активувати звукову та світлову сигналізацію;
– активувати систему пожежогасіння в зоні задимленості.

Раннє виявлення, швидке реагування, централізований моніторинг та автоматизоване управління значно підвищують безпеку крамниці, захищають майно та, найголовніше, зберігають життя. Аналіз даних, зібраних системою IoT, може надати цінні відомості про потенційні ризики та дозволити вживати профілактичні заходи для мінімізації ризику пожеж у майбутньому.

ВИСНОВКИ

Виконана кваліфікаційна робота була присвячена розробці комп'ютерної системи для крамниць музичних інструментів, з акцентом на побудову, налаштування та безпеку корпоративної мережі. В ході дослідження було підтверджено актуальність розробки подібної системи, враховуючи сучасні потреби музичного бізнесу в автоматизації та оптимізації процесів.

Розроблена апаратна частина системи, базується на сформульованих технічних вимогах, враховує специфіку розташування крамниць на великих відстанях від головного офісу. Використання оптоволоконних роутерів дозволило забезпечити стабільне та швидкісне з'єднання, необхідне для ефективної роботи системи.

Особлива увага була приділена розробці корпоративної мережі. Було успішно виконано сегментування IP-адрес, налаштовано мережеве обладнання та впроваджено необхідні заходи безпеки, що мінімізують ризики несанкціонованого доступу та кіберзагроз.

Додатково, в рамках роботи було розроблено компонент системи з налаштування IoT технологій, з акцентом на інтеграцію систем пожежної та димової безпеки. Це дозволить забезпечити безпеку персоналу та майна крамниць, а також оперативно реагувати на виникнення небезпечних ситуацій.

В цілому, розроблена комп'ютерна система з детально опрацьованою корпоративною мережею представляє собою комплексну та надійну платформу для автоматизації бізнес-процесів крамниць музичних інструментів. Результати роботи можуть бути використані для практичного впровадження у реальних умовах, що сприятиме підвищенню ефективності та конкурентоспроможності підприємства.

ПЕРЕЛІК ПОСИЛАНЬ

1. Атестація здобувачів вищої освіти. Методичні рекомендації до виконання кваліфікаційної роботи бакалавра студентами галузі знань 12 Інформаційні технології спеціальності 123 Комп'ютерна інженерія / Л.І. Цвіркун, С.М. Ткаченко, Я.В. Панферова, Д.О. Бешта, Л.В. Бешта. – Д.: НТУ «ДП», 2024. – 63 с.

2. Б.Ю. Жураковський, І.О. Зенів. Комп'ютерні мережі : навч. посібник/ за ред. Батрак Є.В – Міністерство освіти і науки України, Київ: КПІ ім. Ігоря Сікорського, 2020. – 328 с.

3. ANSI/TIA-568.1-D, Commercial Building Telecommunications Infrastructure Standard, 2015

4. Oleksiy Nedashkivskyy. Estimation of quality of Internet services in Ukraine // Modern Problems of Radio Engineering, Telecommunications and Computer Science, Slavske in Lviv region, 23 February, 2016 – 26 February, 2016, p.31.

5. Налаштування NAT – Education [Електронний ресурс] – Режим доступу до ресурсу: http://surl.li/ufwxg.

6. Налаштування VLAN – Education [Електронний ресурс] – Режим доступу до ресурсу: http://surl.li/ufwxs.

7. Налаштування VPN – Education [Електронний ресурс] – Режим доступу до ресурсу: http://surl.li/ufwyf.

8. Сервер Dell PowerEdge T40 (PET40-ST#1-08) – https://rozetka.com.ua/ua/dell_pet40_st_1_08/p204083497/

9. Моноблок Artline Business M62 v03 White – https://hard.rozetka.com.ua/ua/artline_m62_v03/p146179070/

10. Вита пара FinMark UTP Cat.5e 4P 24AWG PVC W Pull Box 305 м (DS049449) – https://rozetka.com.ua/ua/finmark_ds049449/p38945768/

11. Вита пара зовнішня FinMark UTP Cat.5e 4P 24AWG PE-M B Drum – https://rozetka.com.ua/finmark_ds054624/p38945696/

ДОДАТОК А

Текст програми налаштування мережі

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

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ НАЛАШТУВАННЯ МЕРЕЖІ КОМП’ЮТЕРНОЇ СИСТЕМИ

Текст програми

804.02070743.24013-01 12 01

Листів 9

2025

АНОТАЦІЯ

Дана програма містить в собі частину програмного коду для програмування налаштування компонентів корпоративної мережі комп’ютерної системи. Програма призначена для забезпечення налаштування DHCP, AAA, інтерфейсів, протоколу маршрутизації NAT, консольних і vty ліній та створення мереж VPN, домену и ssh комп’ютерної системи.

ЗМІСТ

Стор.

1. Налаштування маршрутизатора Litvunenko_R4

```
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Litvunenko_R4
!
!
!
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
!
ip dhcp excluded-address 172.24.146.1 172.24.146.10
ip dhcp excluded-address 172.24.146.65 172.24.146.75
ip dhcp excluded-address 172.24.146.129 172.24.146.139
!
ip dhcp pool POOL_VLAN24
 network 172.24.146.0 255.255.255.192
 default-router 172.24.146.1
 dns-server 172.24.147.132
ip dhcp pool POOL_VLAN34
 network 172.24.146.64 255.255.255.192
 default-router 172.24.146.65
 dns-server 172.24.147.132
ip dhcp pool POOL_VLAN44
 network 172.24.146.128 255.255.255.192
 default-router 172.24.146.129
 dns-server 172.24.147.132
!
aaa new-model
!
aaa authentication login Login group radius local
aaa authentication login SSH-LOGIN local
aaa authentication login default group radius local
!
username 12321litv password 7 0822455D0A16
!
license udi pid CISCO2911/K9 sn FTX1524M7I7-
!
no ip domain-lookup
ip domain-name Litvunenko_R4.com
!
spanning-tree mode pvst
!
interface GigabitEthernet0/0
 no ip address
!
interface Serial1/0
 no ip address
 clock rate 2000000
 shutdown
!
interface Serial2/0
 no ip address
 clock rate 2000000
 shutdown
!
interface GigabitEthernet3/0
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet3/0.24
 encapsulation dot1Q 24
 ip address 172.24.146.1 255.255.255.192
!
interface GigabitEthernet3/0.34
 encapsulation dot1Q 34
 ip address 172.24.146.65 255.255.255.192
!
interface GigabitEthernet3/0.44
```

```
 encapsulation dot1Q 44
 ip address 172.24.146.129
255.255.255.192
!
interface GigabitEthernet3/0.99
 encapsulation dot1Q 99
 ip address 172.24.146.193
255.255.255.240
!
interface GigabitEthernet4/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface GigabitEthernet5/0
 description TO wan 5
 ip address 10.1.17.18
255.255.255.252
 duplex auto
 speed auto
!
router eigrp 14
 redistribute static
 passive-interface
GigabitEthernet3/0.24
 passive-interface
GigabitEthernet3/0.34
 passive-interface
GigabitEthernet3/0.44
 passive-interface
GigabitEthernet3/0.99
 network 10.1.17.8 0.0.0.3
 network 172.24.146.0 0.0.0.63
 network 172.24.146.64 0.0.0.63
 network 172.24.146.128 0.0.0.63
 network 172.24.146.192 0.0.0.15
 network 10.1.17.16 0.0.0.3
 no auto-summary!
!
ip classless
ip route 0.0.0.0 0.0.0.0 209.165.202.1
!
ip flow-export version 9
!
banner motd #123-21 Litvunenko.
Login for authorized users only#
!
radius server 172.24.147.10
 address ipv4 172.24.147.10 auth-port
1645
!
line con 0
 password 7 0822455D0A16
!
line aux 0
!
line vty 0 4
 password 7 0822455D0A16
 login authentication SSH-LOGIN
 transport input ssh
line vty 5 15
 password 7 0822455D0A16
 transport input ssh
!
end
```

2. Налаштування комутатора Litvunenko_Sw5.1

```
!
!
version 15.0
no service timestamps log datetime
msec
no service timestamps debug datetime
msec
service password-encryption
!
```

```
hostname Litvunenko_Sw5.1
!
!
!
ip domain-name
Litvunenko_Sw5.com
!
username 12321_Lit privilege 1
password 7 0822455D0A16
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 shutdown
!
interface FastEthernet0/2
 shutdown
!
interface FastEthernet0/3
 shutdown
!
interface FastEthernet0/4
 shutdown
!
interface FastEthernet0/5
 shutdown
!
interface FastEthernet0/6
 switchport access vlan 24
 switchport mode access
!
interface FastEthernet0/7
 switchport access vlan 24
 switchport mode access
!
interface FastEthernet0/8
 switchport access vlan 24
 switchport mode access
!
interface FastEthernet0/9
 switchport access vlan 24
 switchport mode access
!
interface FastEthernet0/10
 switchport access vlan 24
 switchport mode access
!
interface FastEthernet0/11
 switchport access vlan 24
 switchport mode access
!
interface FastEthernet0/12
 switchport access vlan 34
 switchport mode access
!
interface FastEthernet0/13
 switchport access vlan 34
 switchport mode access
!
interface FastEthernet0/14
 switchport access vlan 34
 switchport mode access
!
interface FastEthernet0/15
 switchport access vlan 34
 switchport mode access
!
interface FastEthernet0/16
 switchport access vlan 34
 switchport mode access
!
interface FastEthernet0/17
 shutdown
!
interface FastEthernet0/18
 shutdown
!
interface FastEthernet0/19
 switchport access vlan 44
 switchport mode access
!
interface FastEthernet0/20
 switchport access vlan 44
 switchport mode access
!
interface FastEthernet0/21
 switchport access vlan 44
```

```
 switchport mode access
!
interface FastEthernet0/22
 switchport access vlan 44
 switchport mode access
!
interface FastEthernet0/23
 switchport access vlan 44
 switchport mode access
!
interface FastEthernet0/24
 shutdown
!
interface GigabitEthernet0/1
 switchport trunk native vlan 100
 switchport trunk allowed vlan
24,34,44,99-100
 switchport mode trunk
!
interface GigabitEthernet0/2
 switchport trunk native vlan 100
 switchport trunk allowed vlan
24,34,44,99-100
 switchport mode trunk
!
interface Vlan1
 description Litvunenko_Sw5.1 LAN5
 no ip address
!
interface Vlan99
 description LAN Vnutr_99
 ip address 172.24.146.194
255.255.255.240
!
ip default-gateway 172.24.146.194
!
banner motd #123-21 Litvunenko.
There is protection#
!
!
!
line con 0
 password 7 0822455D0A16
 login
!
line vty 0 4
 password 7 0822455D0A16
 login local
 transport input ssh
line vty 5 15
 password 7 0822455D0A16
 login local
 transport input ssh
!
!
!
!
end
```