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 Моторного Олександра Миколайовича
(ПІБ)

академічної групи 123-21-2
(шифр)

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

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

на тему «Комп'ютерна система юридичної фірми з детальним опрацюванням побудови та налаштування корпоративної мережі»
(назва за наказом ректора)

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	доц. Кожевніков А.В.			
спеціальної частини	доц. Кожевніков А.В.			
розділу розробка корпоративної мережі	ас. Панферова Я.В.			

Рецензент				

Нормоконтролер	проф. Цвіркун Л.І.			

Дніпро
2025

ЗАТВЕРДЖЕНО:

завідувач кафедри
інформаційних технологій
та комп'ютерної інженерії
(повна назва)

_____ Гнатушенко В.В.
(підпис) (прізвище, ініціали)

« » _____ 2025 року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавр

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

спеціальності 123 Комп'ютерна інженерія

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

на тему «Комп'ютерна система юридичної фірми з детальним опрацюванням побудови та налаштування корпоративної мережі»

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

Розділ	Зміст	Термін виконання
Стан питання та постановка завдання	На основі матеріалів виробничих практик, інших науково-технічних джерел розглянути комп'ютерну систему юридичної фірми та виконати постановку завдання	10.02.2025
Розробка апаратної частини	Сформулювати найменування й призначення комп'ютерної системи, висунути технічні вимоги до неї	15.03.2025
	Виконати технічну розробку апаратної частини комп'ютерної системи	20.04.2025
Розробка корпоративної мережі	Виконати розрахунок налаштувань корпоративної мережі та перевірити роботу системи, розробити методи та налаштування обладнання для захисту інформації в системі	07.05.2025
Розробка компонента системи	Виконати розробку системи контролю доступу на основі RFID-карт	31.05.2025

Завдання видано _____ проф. Кожевніков А.В.
(підпис керівника) (прізвище, ініціали)

Дата видачі 25.02.2025

Дата подання до екзаменаційної комісії 16.06.2025

Прийнято до виконання _____ Моторний О. М.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 66 с., 33 рис., 4 табл., 1 додаток, 12 джерел.

КОМП’ЮТЕРНА МЕРЕЖА, ЮРИДИЧНА ФІРМА, IP-ТЕЛЕФОНІЯ VLAN, DHCP; СИСТЕМА КОНТРОЛЮ ДОСТУПУ; СМАРТ-КАРТА; RFID.

Об’єкт професійної діяльності – комп’ютерна система юридичної фірми, а саме її інфраструктура, яка включає в себе побудову корпоративної мережі, налаштування засобів безпеки та систему контролю доступу.

Мета роботи − розробка та налаштування комп'ютерної системи для юридичної фірми, яка включає в себе побудову корпоративної мережі з урахуванням усіх сучасних вимог з безпеки та доступності, а також фізичний контроль доступу. Основними завданнями є аналіз існуючих рішень, проектування архітектури мережі, а також налаштування необхідних програмних і апаратних засобів.

Окрему увагу в межах даної кваліфікаційної роботи приділено розробці системи контролю доступу на основі RFID-карт, що дозволяє реалізувати автоматичну ідентифікацію персоналу на вході до приміщень та обмежити доступ до певних зон або серверних кімнат.

Актуальність теми зумовлена необхідністю дотримання високих стандартів інформаційної безпеки та безперервності діяльності в юридичному секторі. У сучасних умовах цифровізації, юридичні компанії обробляють великі обсяги конфіденційних даних, що вимагає впровадження захищених комп’ютерних мереж, засобів ідентифікації персоналу, а також інтеграції інформаційних та фізичних систем безпеки.

У результаті виконання роботи було спроєктовано та змодельовано безпечну мережу юридичної фірми з урахуванням сегментації трафіку, контролю доступу, а також з впровадженням базових механізмів захисту другого рівня. Запропонована модель сприяє підвищенню стійкості мережі до внутрішніх атак та забезпечує стабільне надання IP-адрес клієнтам.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАК, ОДИНИЦЬ І ТЕРМІНІВ

КС – комп’ютерна система;

СКД – система контролю доступу;

СКС – структурована кабельна система;

DAI – англ. Dynamic ARP Inspection;

DHCP – англ. Dynamic Host Configuration Protocol;

DMZ англ. Demilitarized Zone;

HSRP – англ. Hot Standby Router Protocol

IP – англ. Internet Protocol;

MAC – англ. Media Access Control;

RFID – англ. Radio Frequency Identification

VLAN – англ. Virtual Local Area Network;

VoIP – англ. Voice over Internet Protocol.

ВСТУП

У сучасному інформаційному суспільстві надання якісних юридичних послуг є неможливим без використання ефективних комп'ютерних систем, які забезпечують надійну обробку, зберігання та захист великого обсягу конфіденційної інформації.

Створення корпоративної мережі для юридичної установи є комплексним завданням, яке охоплює не лише технічне проектування та підбір обладнання, але й глибоке розуміння особливостей галузі, зокрема вимог до збереження правової таємниці, контролю доступу до даних, взаємодії з державними електронними сервісами. У цьому контексті комп'ютерна система виконує роль основи цифрової трансформації юридичної фірми, забезпечуючи автоматизацію робочих процесів, захист правових даних, мобільність та ефективне управління інформаційними потоками.

Актуальність теми обумовлюється потребою юридичних фірм в адаптації до сучасних умов роботи – дистанційної взаємодії з клієнтами, цифрового документообігу, електронного судочинства. Розробка надійної комп'ютерної мережі з урахуванням принципів безпеки, масштабованості та централізованого адміністрування дозволяє досягти нової якості надання юридичних послуг та підвищити конкурентоспроможність організації.

Метою кваліфікаційної роботи є розробка комп'ютерної системи юридичної фірми з акцентом на створення корпоративної мережі, яка забезпечує надійне, безпечне та ефективне функціонування усіх підрозділів організації. В рамках роботи проведено аналіз організаційної структури, сформульовано технічні вимоги, спроєктовано фізичну і логічну топології мережі, обґрунтовано вибір обладнання, реалізовано налаштування маршрутизаторів і серверних служб, а також впроваджено систему контролю доступу на основі смарт-карт.

Практичне значення роботи полягає у формуванні типового рішення, що може бути адаптоване для впровадження у реальних умовах юридичних установ з різним масштабом діяльності. Отримані результати сприяють підвищенню інформаційної безпеки, покращенню документообігу та загальній оптимізації функціонування IT-інфраструктури юридичних фірм.

1 СТАН ПИТАННЯ ТА ПОСТАНОВКА ЗАВДАННЯ

1.1 Характеристика юридичної галузі та умов застосування комп’ютерної системи

Юридична галузь є однією з основних складових правової системи держави, яка регулює права та обов'язки фізичних осіб і організацій у різних сферах суспільного життя. Вона охоплює численні підгалузі права, серед яких цивільне, кримінальне, адміністративне, сімейне та комерційне право. Кожна з цих підгалузей має свої характерні риси, методи вирішення правових питань та особливості застосування норм.

Юридична сфера відіграє важливу роль у забезпеченні стабільності і правопорядку в суспільстві, гарантуючи захист прав і свобод громадян, а також регулюючи відносини між державними органами, фізичними та юридичними особами. Вона створює правові засади для розвитку бізнесу, регулюючи комерційні та господарські взаємовідносини, що є необхідним для сталого економічного розвитку.

Основними принципами, на яких базується юридична галузь, є законність, правова держава та правова відповідальність. Законність забезпечує виконання встановлених норм та правил, що є основою функціонування правової системи. Принцип правової держави передбачає рівність усіх громадян перед законом і забезпечення належного захисту їхніх прав. Правова відповідальність визначає покарання за порушення встановлених норм.

Юридична галузь є надзвичайно динамічною та адаптується до соціально-економічних змін. Вона охоплює різні професії: адвокатів, юристів, суддів, прокурорів, нотаріусів та інших фахівців, кожен з яких відіграє свою роль у забезпеченні правосуддя та дотриманні законів.

Особливістю юридичної діяльності є велика кількість документів і даних, які потребують ефективного зберігання, обробки та обміну. У цьому контексті використання інформаційних технологій, зокрема комп’ютерних

мереж та спеціалізованого програмного забезпечення, є важливим для оптимізації робочих процесів. Ці технології дозволяють значно покращити доступ до необхідної інформації, забезпечити надійність обміну даними та автоматизувати багато аспектів роботи юридичних фірм.

В Україні реформа правової системи активно набирає обертів [1]. Одним із важливих напрямів є вдосконалення законодавства, модернізація судових процедур і підвищення ефективності захисту прав громадян. Інтеграція сучасних технологій у правову діяльність, зокрема впровадження комп’ютерних мереж і програмного забезпечення, дозволяє оптимізувати процеси, знизити людський фактор та підвищити ефективність роботи юридичних фірм. Це також дає змогу юридичним організаціям обробляти великі обсяги даних, здійснювати швидкий доступ до документів та забезпечити високий рівень безпеки для клієнтів.

Таким чином, юридична галузь в Україні знаходиться в процесі трансформації, активно адаптуючись до змін у технологіях і потребах суспільства. Впровадження сучасних інформаційних систем є важливим кроком для підвищення ефективності та якості правових послуг, що сприяє розвитку правопорядку і стабільності в країні.

Впровадження комп'ютерної системи є стратегічно важливим кроком для сучасної юридичної фірми. Правильно підібрана та налаштована система дозволяє оптимізувати робочі процеси, підвищити ефективність роботи, покращити якість послуг, що надаються клієнтам, та забезпечити конкурентоздатність на ринку юридичних послуг. При виборі системи необхідно враховувати специфіку діяльності фірми, її розмір, бюджет та майбутні потреби. Ефективне використання комп'ютерної системи дозволить юридичній фірмі зосередитися на головному – наданні якісної правової допомоги своїм клієнтам.

1.2 Характеристика і особливості комп’ютеризації юридичної діяльності

Об'єктом впровадження комп’ютерної системи є юридична фірма, що спеціалізується на наданні широкого спектра правових послуг для бізнесу та приватних клієнтів. Фірма має досвід у сфері юридичного консалтингу, зарекомендувавши себе як надійний партнер для вітчизняних та міжнародних організацій, державних установ, неприбуткових організацій і фізичних осіб.

Основні напрями діяльності компанії охоплюють такі правові галузі:

– корпоративне право та бізнес-структуризація – надання послуг з реєстрації підприємств, консультування щодо корпоративного управління, реструктуризації бізнесу та ліквідації компаній;

– податкове право – розробка стратегій податкової оптимізації, супровід перевірок та представництво інтересів клієнтів у податкових органах;

– трудове право – правовий супровід з питань трудових договорів, кадрових спорів, соціального захисту та питань зайнятості;

– міжнародне право – юридична підтримка зовнішньоекономічної діяльності, захист прав інтелектуальної власності, супровід міжнародних контрактів;

– судова та арбітражна практика – представництво інтересів клієнтів у судах усіх інстанцій та в арбітражах;

– право нерухомості – супровід угод з купівлі, продажу, оренди, а також юридичне оформлення прав власності;

– фінансове та банківське право – консультування з питань кредитування, інвестування, лізингу та взаємодії з банківськими установами.

Фірма дотримується високих етичних стандартів, принципів конфіденційності та професійної відповідальності. Юристи компанії надають клієнтам індивідуальний підхід до вирішення кожної справи, виходячи з потреб конкретного запиту.

Крім основної діяльності, фірма активно реалізує соціальні ініціативи: співпрацює з благодійними фондами, надає безоплатну правову допомогу, підтримує мистецькі та культурні заходи.

Завдяки впровадженню сучасних інформаційних технологій, фірма ефективно обслуговує клієнтів як в Україні, так і за її межами, використовуючи онлайн-зв’язок, електронний документообіг та хмарні сервіси.

Комп’ютерна система фірми включає в себе кілька складових: серверну частину для зберігання даних та забезпечення доступу, мережеву інфраструктуру для швидкої та безпечної передачі даних, а також систему безпеки для захисту конфіденційної інформації. Основною складовою є корпоративна мережа фірми, що з’єднує робочі місця співробітників, сервери, засоби зберігання даних, а також інші компоненти, що необхідні для ефективної роботи юридичної фірми. Структура цієї мережі повинна бути гнучкою та масштабованою, з можливістю інтеграції нових технологій та пристроїв без шкоди для безпеки.

1.3 Організаційна структура юридичної фірми

Організаційна структура юридичної фірми є фундаментом її ефективного функціонування та успішного надання послуг клієнтам. В умовах сучасного українського ринку юридичних послуг, що характеризується динамічністю та конкуренцією, оптимальна організаційна модель набуває особливого значення. Типова юридична фірма в Україні, незалежно від її розміру та спеціалізації, як правило, будується за принципами, що забезпечують чітке розподілення функцій, відповідальності та сприяють координації діяльності.

Юридична фірма має чітку організаційну структуру, яка включає керівництво, юридичних консультантів, асистентів, а також адміністративний персонал, що відповідає за документообіг та інші важливі аспекти діяльності. Схема організаційної структури на рисунку 1.1 відображає роль кожного підрозділу та взаємодію між ними. Оскільки більшість робочих процесів фірми

передбачає взаємодію з конфіденційними документами, важливо створити схему доступу до інформації, де кожен співробітник має доступ лише до тих ресурсів, що необхідні для виконання його службових обов’язків.

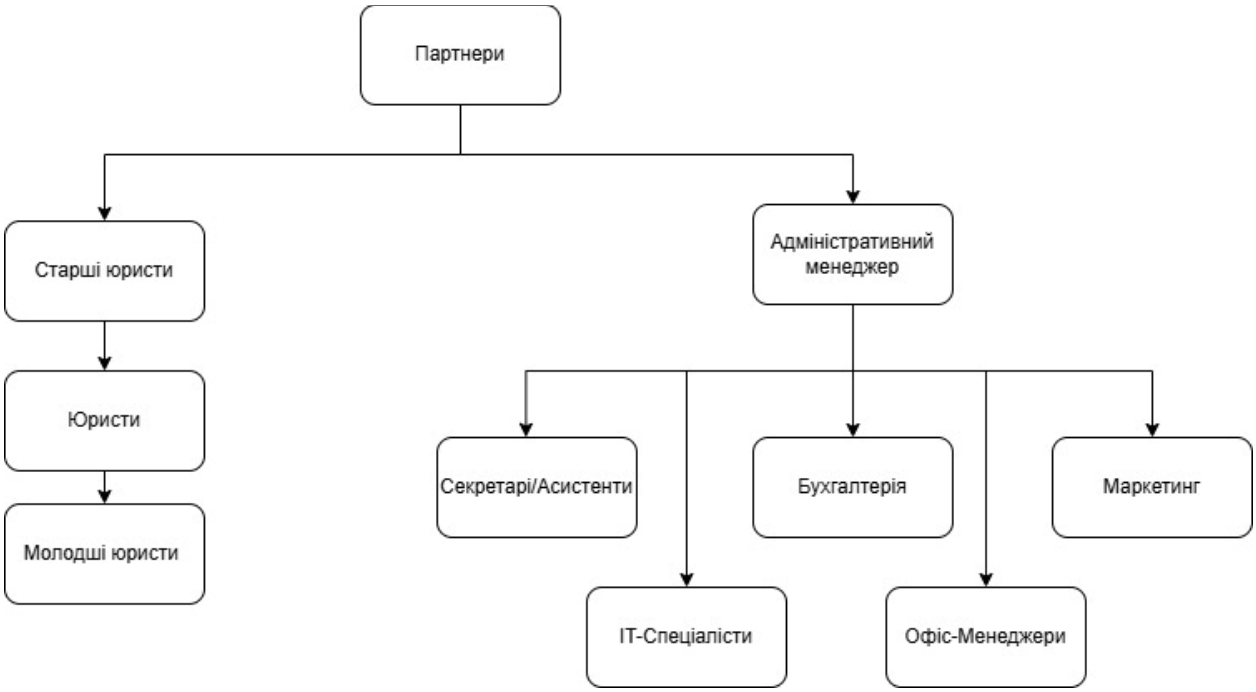

Рисунок 1.1 – Організаційна структура юридичної фірми

Центральною ланкою будь-якої юридичної фірми є її юридичний склад. Це ядро організації, що об'єднує юристів різних рівнів кваліфікації. На вершині ієрархії стоять партнери – власники або співвласники фірми, які, як правило, мають значний досвід, високу репутацію та несуть відповідальність за стратегічний розвиток бізнесу. Партнери можуть спеціалізуватися на певних галузях права, керувати окремими практиками або відділами, а також активно займатися залученням нових клієнтів.

Під керівництвом партнерів працюють старші юристи (senior associates) та юристи (associates). Старші юристи, як правило, мають кількарічний досвід роботи, самостійно ведуть складні справи, керують молодшими колегами та беруть участь у розвитку клієнтських відносин. Юристи – це фахівці, які здобувають досвід, працюючи під керівництвом старших колег та партнерів. Вони виконують значний обсяг роботи з підготовки документів, аналізу законодавства та участі в судових процесах. На початкових етапах кар'єри в

юридичній фірмі часто перебувають молодші юристи (junior associates) або стажери, які виконують допоміжні функції та отримують базові навички.

Важливою складовою організаційної структури є практики або відділи. Це спеціалізовані групи юристів, які фокусуються на певних галузях права (наприклад, корпоративне право, судова практика, нерухомість, інтелектуальна власність, податкове право тощо). Такий поділ дозволяє фірмі накопичувати експертизу в конкретних сферах та надавати високоякісні послуги в рамках цих спеціалізацій. Керівниками практик часто є партнери або досвідчені старші юристи.

Окрім юридичного складу, функціонування юридичної фірми неможливе без адміністративного та допоміжного персоналу. Ця частина структури забезпечує безперебійну роботу офісу та підтримку юридичної діяльності. До нього належать:

– адміністративний директор/менеджер: відповідає за загальне управління офісом, ресурсами, персоналом (окрім юридичного складу);

– секретарі/асистенти: надають адміністративну підтримку юристам, відповідають за документообіг, комунікації, організацію зустрічей;

– спеціалісти з фінансів та бухгалтерії: ведуть фінансовий облік, виставляють рахунки, контролюють витрати;

– спеціалісти з маркетингу та розвитку бізнесу: займаються просуванням фірми, залученням клієнтів, організацією заходів;

– IT-спеціалісти: забезпечують технічну підтримку, функціонування інформаційних систем;

– офіс-менеджери: відповідають за матеріально-технічне забезпечення офісу.

Структура адміністративного та допоміжного персоналу може варіюватися залежно від розміру фірми. У невеликих фірмах ці функції можуть бути об'єднані, тоді як у великих – представлені окремими відділами.

Загалом, організаційна структура типової юридичної фірми в Україні є комбінацією лінійної та функціональної структури. Юристи

підпорядковуються старшим колегам та партнерам (лінійна ієрархія), але одночасно працюють в рамках функціональних практик. Адміністративний персонал підпорядковується адміністративному керівництву, але надає підтримку всім функціональним підрозділам.

1.4 Технології збору, передачі та захисту інформації в юридичній фірмі

У діяльності юридичної фірми надзвичайно важливо забезпечити оперативний доступ до правової інформації, клієнтських даних, внутрішніх документів і результатів аналітики. Збір, передача та зберігання інформації здійснюється із застосуванням сучасних цифрових технологій, які відповідають вимогам безпеки, надійності та чинного законодавства. Це може включати використання локальної мережі для внутрішнього обміну даними, голосової внутрішньої та зовнішньої голосової комунікації, а також захищених з'єднань (VPN, SSL/TLS) для обміну інформацією з клієнтами та іншими юридичними установами. Окрім цього, важливо забезпечити систему резервного копіювання та архівації даних для уникнення їх втрати в разі непередбачених ситуацій.

Основними джерелами збору інформації є:

– інтегровані CRM-системи (Customer Relationship Management), які акумулюють інформацію про клієнтів, історію звернень, надані послуги та документообіг;

– електронна пошта та зашифровані онлайн-форми, через які клієнти передають юридичну інформацію та запити;

– інтеграція з державними реєстрами та базами даних, такими як ЄДР, ДРФО, реєстр судових рішень, що дозволяє оперативно отримувати офіційну правову інформацію;

– системи електронного документообігу (СЕД), які використовуються для внутрішньої координації між підрозділами та збереження юридичних документів.

Передача інформації між офісами та працівниками здійснюється:

– захищеними каналами зв’язку (VPN, TLS, IPsec), що використовуються відповідно до Закону України «Про захист персональних даних» (№2297-VI) для запобігання несанкціонованому доступу до інформації;

– хмарними платформами (Microsoft 365, Google Workspace, AWS або приватні хмари), що використовуються для зберігання, резервного копіювання та спільної роботи з документами;

– інтрамережевими каналами, які використовуються для обміну даними всередині локальної мережі в рамках одного офісу, з можливістю сегментування VLAN для підвищення рівня безпеки;

– доступ через мультифакторну автентифікацію (MFA) – є обов’язковим для входу в системи з конфіденційною інформацією.

Контроль та безпека:

– логування активності користувачів, згідно з вимогами ISO/IEC 27001 [2], що дозволяє фіксувати всі дії з критично важливими даними;

– автоматизовані системи резервного копіювання із шифруванням, які зберігаються в географічно розподілених дата-центрах;

– шифрування даних на етапах передачі та зберігання (AES-256, RSA) згідно з міжнародними стандартами інформаційної безпеки.

Особливу роль відіграє технологія IoT, яка використовується в контексті реалізації системи контролю фізичного доступу на основі RFID-смарт-карт. У цій підсистемі:

– RFID-зчитувачі здійснюють збір ідентифікаторів з карт доступу;

– дані передаються на IoT-сервер через локальну мережу або Wi-Fi;

– сервер аналізує доступ у реальному часі, активує сигналізацію і при потребі, надсилає сповіщення адміністратору на мобільний пристрій.

Таким чином, технології збору та передачі інформації, що використовуються в компанії, дозволяють ефективно та безпечно здійснювати юридичну діяльність, зберігаючи конфіденційність клієнтів та відповідність

законодавчим вимогам у сфері обробки персональних даних і захисту інформації.

1.5 Обґрунтування вибраного напрямку інженерного рішення

Зважаючи на специфіку діяльності юридичної фірми, яка пов’язана з обробкою великого обсягу конфіденційної інформації, критичною вимогою до проєктованої комп’ютерної системи є забезпечення високого рівня безпеки, надійності зв’язку, гнучкої сегментації та контрольованого доступу як до інформаційних, так і до фізичних ресурсів.

Обраний напрямок інженерного рішення полягає у створенні інтегрованої корпоративної комп’ютерної системи, що включає:

– побудову багаторівневої комп’ютерної мережі за ієрархічною моделлю «ядро-доступ» з логічною сегментацією за допомогою VLAN;

– використання стандартизованих протоколів TCP/IP, DHCP, DNS, NAT, HSRP для забезпечення маршрутизації, адресації, відмовостійкості та трансляції адрес;

– впровадження централізованих серверів з файловими, поштовими, FTP та авторизаційними службами;

– реалізацію IP-телефонії (VoIP) для внутрішньої комунікації з підтримкою QoS та резервування;

– впровадження системи контролю фізичного доступу (СКД) на базі RFID-смарт-карт і IoT-платформи з сигналізацією та моніторингом;

– застосування механізмів безпеки, таких як списки контролю доступу (ACL), брандмауери, VPN, шифрування.

Реалізація системи в середовищі Cisco Packet Tracer дозволяє моделювати роботу мережі, перевіряти функціонування служб, тестувати резервування каналів, працездатність VoIP-сегменту та взаємодію IoT-пристроїв у системі доступу.

Таким чином, таке рішення дозволяє значно підвищити рівень безпеки та зменшити ризик несанкціонованого доступу до чутливих даних.

Враховуючи специфіку роботи юридичних фірм, де кожен документ є потенційно конфіденційним, таке рішення є надзвичайно важливим для забезпечення належного рівня безпеки.

1.6 Завдання і мета роботи

Мета роботи полягає у створенні безпечної, функціональної комп'ютерної системи для юридичної фірми з детальним опрацюванням побудови та налаштування корпоративної мережі відповідно до галузевих і технічних стандартів.

Для досягнення цієї мети необхідно вирішити наступні завдання:

– розробити логічну топологію корпоративної мережі з урахуванням підрозділів, офісів і серверного сегменту;

– здійснити вибір мережевого та серверного обладнання, розрахувати IP-адресний простір;

– розрахувати IP-адресний простір на основі VLSM, виділивши окремі VLAN для підрозділів та VoIP;

– налаштувати ключові апаратні компоненти (маршрутизатори, комутатори, сервери, IP-телефонію) та відповідне програмне забезпечення;

– впровадити механізми захисту інформації, зокрема шифрування, багаторівневу автентифікацію та контроль доступу;

– розробити та протестувати систему контролю фізичного доступу на основі RFID-смарт-карт із сигналізацією та IoT-керуванням;

– здійснити тестування функціонування мережі та СКД у середовищі Cisco Packet Tracer, перевірити надійність функціонування, взаємодію пристроїв і відмовостійкість.

2 РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ СИСТЕМИ

2.1 Технічні вимоги до комп'ютерної системи юридичної фірми

2.1.1 Найменування і функціональне призначення КС юридичної фірми

Об'єктом професійної діяльності є комп'ютерна система юридичної фірми, яка слугує технологічною основою для підтримки основних функцій компанії: опрацювання правової інформації, управління справами клієнтів, зберігання електронних документів, забезпечення внутрішньої та зовнішньої комунікації, захисту конфіденційних даних. КС інтегрує апаратні та програмні компоненти у цілісне інформаційне середовище, що сприяє зростанню продуктивності праці та підвищенню рівня сервісу.

2.1.2 Вимоги до структури і функціонуванню КС юридичної фірми

Комп'ютерна система юридичної фірми повинна мати модульну, багаторівневу структуру, яка забезпечує надійну, безпечну та масштабовану взаємодію між усіма підрозділами організації. Вона повинна бути побудована за принципами централізованого керування, розмежування доступу, логічної сегментації і з резервуванням критичних компонентів:

Вимоги до структури системи передбачають наявність таких основних підсистем:

– інформаційно-комунікаційної підсистеми, що включає локальну мережу, маршрутизатори, комутатори, бездротові точки доступу та зовнішні канали зв'язку;

– обчислювального ядра, представленого серверами для забезпечення роботи служб DNS, DHCP, Active Directory, CRM, документообігу, резервного копіювання та поштової інфраструктури);

– підсистеми безпеки, яка містить міжмережеві екрани, контролери доступу, систему журналювання подій, відеоспостереження, а також логічні механізми шифрування та багатофакторної автентифікації;

– підсистеми керування, до складу якої входять інструменти централізованого адміністрування, моніторингу та оновлення;

– користувацьких пристроїв – робочих станцій, IP-телефонів, принтерів, які взаємодіють із центральною мережею через VLAN.

Функціонування системи має відповідати таким критеріям:

– забезпечення безперебійної роботи протягом 24/7 з гарантованим рівнем доступності не менше 99,9 %;

– підтримка захищеного доступу до внутрішніх ресурсів як з локальної мережі, так і віддалено (через VPN);

– відповідність нормам інформаційної безпеки, включаючи стандарт ISO/IEC 27001 [2] та Закон України «Про захист персональних даних» [3];

– забезпечення масштабованості, що дозволяє інтегрувати нові вузли, сервіси або філії без потреби повної перебудови архітектури;

– логічна сегментація мережі за VLAN з ізоляцією трафіку між підрозділами відповідно до ролей користувачів;

– можливість централізованого резервного копіювання та відновлення даних із заданою періодичністю.

2.1.3 Вимоги до способів і засобів зв'язку між компонентами КС

Зв’язок між компонентами комп’ютерної системи повинен базуватися на принципах швидкодії, безпеки та масштабованості. До основних вимог належать:

– використання структурованої кабельної системи (СКС) категорії не нижче Cat 6 для обробки великих масивів юридичних документів;

– застосування комутаторів з підтримкою VLAN для логічної сегментації мережі;

– захищені канали комунікації з державними правовими системами (через VPN, криптозахист);

– підтримка мережевих протоколів TCP/IP, DHCP, DNS, SNMP, які забезпечують динамічне адресування, іменування вузлів, моніторинг і управління мережею;

– впровадження IP-телефонії з підтримкою протоколів SIP/RTP для забезпечення внутрішньої й зовнішньої голосової комунікації в рамках єдиної мережі;

– використання PoE-комутаторів для живлення IP-телефонів без потреби в додаткових джерелах живлення;

– ізоляція голосового трафіку у виділеному VLAN для забезпечення безпеки та стабільності передачі аудіо-даних;

– резервування критичних каналів зв’язку (двійне підключення до інтернету, резервна маршрутизація).

2.1.4 Вимоги функцій, виконуваним КС юридичної фірми

Комп’ютерна система повинна виконувати такі основні функції:

– забезпечення безперервного доступу до цифрових юридичних документів і баз даних;

– збереження конфіденційності, цілісності та доступності даних клієнтів;

– реалізація системи контролю доступу до ресурсів (логічного й фізичного);

– підтримка обміну даними між підрозділами через внутрішню мережу та безпечне підключення ззовні;

– можливість віддаленої роботи із захищеним входом і багатофакторною автентифікацією.

Додатково до базових функцій, система має підтримувати механізми інтеграції з державними реєстрами та судовими порталами для підвищення ефективності правової діяльності.

2.1.5 Вимоги до показників призначення

У рамках розробки системи контролю доступу на основі RFID-смарт-карт критично важливими є вимоги до показників призначення, які визначають ефективність та безпеку функціонування системи. Ці вимоги включають кілька основних аспектів:

– відмовостійкість мережі: при виході з ладу одного із основних вузлів (комутатора або маршрутизатора) трафік має бути автоматично переадресований через резервний канал (HSRP, STP);

– масштабованість: система повинна забезпечувати одночасну роботу не менше 50 користувачів із можливістю розширення до 100 без змін топології;

– система повинна забезпечувати швидку та точну ідентифікацію користувачів за допомогою RFID-міток, з часом реакції не більше ніж 1-2 секунди;

– усі дані, що передаються між RFID-зчитувачем, IoT-сервером та іншими компонентами системи, повинні бути зашифровані для забезпечення конфіденційності та захисту від перехоплення;

– рівень захисту даних повинен відповідати стандартам, наприклад, AES (Advanced Encryption Standard);

– система повинна мати показник доступності не менше ніж 99.9%, для забезпечення безперебійної роботи контролю доступу;

– всі фізичні компоненти системи, включаючи зчитувачі, замки та сервери, повинні бути захищені від фізичного доступу сторонніх осіб;

– необхідно реалізувати резервні механізми (наприклад, механічні замки), які активуються у разі виходу системи з ладу;

– система контролю доступу повинна мати можливість інтеграції з іншими інформаційними системами підприємства, такими як системи відеоспостереження та управління будівлею.

Всі зазначені показники підлягають перевірці під час тестування мережі та її сервісів у симуляційному середовищі Cisco Packet Tracer.

2.2 Розробка інженерних рішень для реалізації КС юридичної фірми

2.2.1 Розробка загальної архітектури КС

Загальна архітектура мережі будується за ієрархічним принципом і включає три рівні:

– ядро мережі (core) – виконує маршрутизацію між VLAN і фільтрацію трафіку, базується на маршрутизаторі з функціями міжмережевого екрану (наприклад, Cisco ISR або FortiGate);

– розподільчий рівень (distribution) – відповідає за агрегацію трафіку від підрозділів, використовує L2+/L3-комутатори з підтримкою VLAN, QoS і STP;

– рівень доступу (access) – з'єднує кінцеві пристрої (ПК, принтери, точки доступу), передбачає PoE-підтримку для живлення IP-телефонів або камер.

Планування мережі базується на організаційній структурі юридичної фірми, яка охоплює керівництво, юридичний та адміністративний персонал, а також ІТ-відділ, бухгалтерію та гостьовий доступ. Метою є забезпечення сегментованого та захищеного доступу до цифрових ресурсів з урахуванням службових обов'язків кожного підрозділу. Всі офіси юридичної фірми об'єднуються в логічно сегментовану корпоративну мережу з поділом трафіку між підрозділами: адміністрацією, юристами, клієнтською зоною, серверною частиною. Це дозволяє реалізувати контроль доступу, балансування навантаження та підвищення безпеки.

Система має підтримувати як локальну взаємодію, так і віддалене підключення через VPN.

Забезпечення електронної комунікації через корпоративну електронну пошту та IP-телефонію з маршрутизацією викликів, голосовою поштою та журналюванням дзвінків.

Фізична топологія побудована за зіркоподібною моделлю. Центральним вузлом є серверна шафа з маршрутизатором, комутаторами доступу (PoE), серверним обладнанням та точками доступу Wi-Fi 6. Робочі станції кожного підрозділу підключаються до відповідних портів комутаторів. Комутатор ядра зв'язує всі VLAN у єдину інфраструктуру.

На основі описаної структури пропонується виділити такі логічні сегменти VLAN (табл.2.1) :

Таблиця 2.1 – Сегменти VLAN

VLAN	Назва підрозділу	Приблизна кількість користувачів	Призначення
10	Адміністрація та партнери	5–6	стратегічне управління, доступ до всіх звітів та внутрішніх систем
20	Старші юристи, юристи, молодші юристи	20–25	робота з документами, CRM, базами даних, правовими реєстрами
30	Секретарі, асистенти	3–5	обробка вхідної/вихідної документації, внутрішня комунікація
40	Бухгалтерія та фінансовий відділ	2–3	фінансові операції, рахунки, доступ до облікових систем
50	Відділ маркетингу та розвитку бізнесу	2–3	сайт, email-розсилки, аналітика
60	Гостьова мережа Wi-Fi	необмежено	мережа без доступу до внутрішніх ресурсів
70	VoIP	10	мережа IP-телефонії
90	Серверна зона та IT-відділ	5	адміністрування, моніторинг, резервне копіювання, управління доступом, керування серверами, журналювання, зберігання конфіденційних даних

Загальна архітектура представлена на рисунку 2.2.

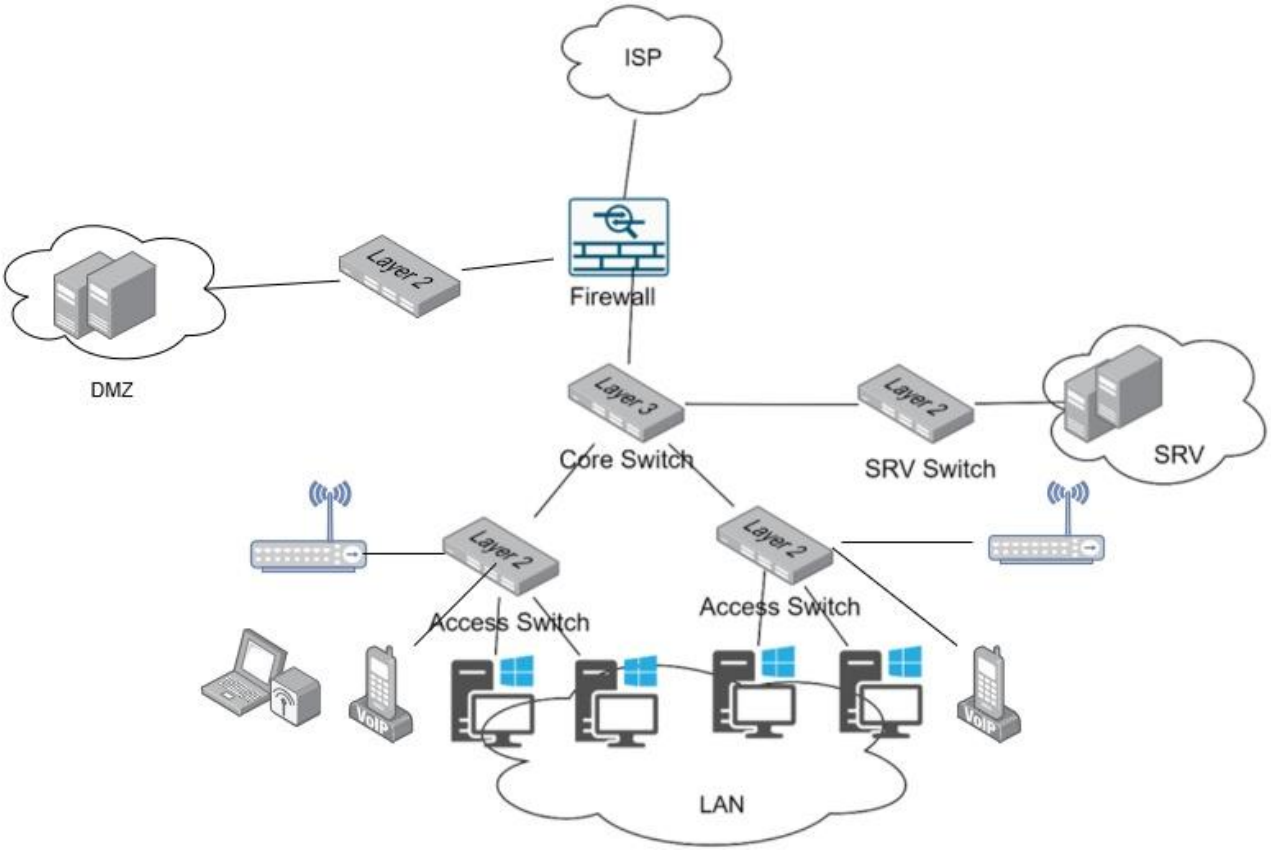

Рисунок 2.2 – Загальна архітектура КС фірми

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

Структурна схема КС включає наступні компоненти:

а) Distribution & Core Layer рівні представлені маршрутизатором R1 і комутаторами CS1 та CS2. Ці компоненти забезпечують маршрутизацію даних між різними сегментами мережі та контроль доступу до ресурсів. Важливий елемент firewall, який сприяє захисту мережі, фільтруючи небажаний трафік;

б) Acces Layer На рівні доступу відзначаються різні VLAN (Virtual Local Area Network), які забезпечують логічну сегментацію мережі для груп користувачів. Наприклад, VLAN 10 відповідає за управлінські функції, VLAN 20 – за правові питання, а VLAN 30 – за асистентів. Відокремлення цих груп дозволяє знижувати ризики безпеки, оптимізуючи при цьому обробку даних.

в) серверний сегмент, який розміщується в окремому приміщенні із обмеженим доступом. Сегмент включає сервери файлового сховища, домену

(Active Directory), CRM-системи, резервного копіювання, DNS/DHCP та електронної пошти;

г) мережевий сегмент, що складається з маршрутизатора з підтримкою VPN/NAT, L2/L3-комутаторів із підтримкою VLAN і PoE для живлення IP-телефонів та точок доступу, а також бездротової мережі стандарту Wi-Fi 6 для мобільного підключення. Комутатори спрямовані на агрегацію трафіку, підтримку VLAN для логічного розділення мережі та PoE для живлення Wi-Fi точок доступу і камер. Використання двох комутаторів забезпечує резервування та балансування навантаження, що підвищує стабільність і безпеку мережі. Маршрутизатор забезпечує основну маршрутизацію мережевого трафіку, підтримує функції NAT і VPN. Це головний елемент для безпечного з'єднання офісу з інтернетом і міжмережевого обміну даними, що важливо для забезпечення захищеного доступу і зв'язку.

д) робочі станції працівників (юристів, адміністрації, бухгалтерії), представлені енергоефективними ПК або моноблоками з базовими офісними конфігураціями, підключені через комутатори доступу з розмежуванням за VLAN;

е) система контролю доступу, яка включає зчитувачі смарт-карт, контролери смарт-карт, турнікет (при потребі), що підключаються до керуючого сервера;

ж) периферійні пристрої, зокрема IP-телефони, багатофункціональні принтери, сканери, які підключаються через PoE або USB до робочих станцій та інтегруються у внутрішню мережу з відповідним обмеженням доступу;

з) джерела безперебійного живлення (UPS) для забезпечення захисту критичних елементів системи у разі зникнення електропостачання.

и) ІБП (UPS) для резервного живлення ключового обладнання (сервери, маршрутизатор, комутатори).

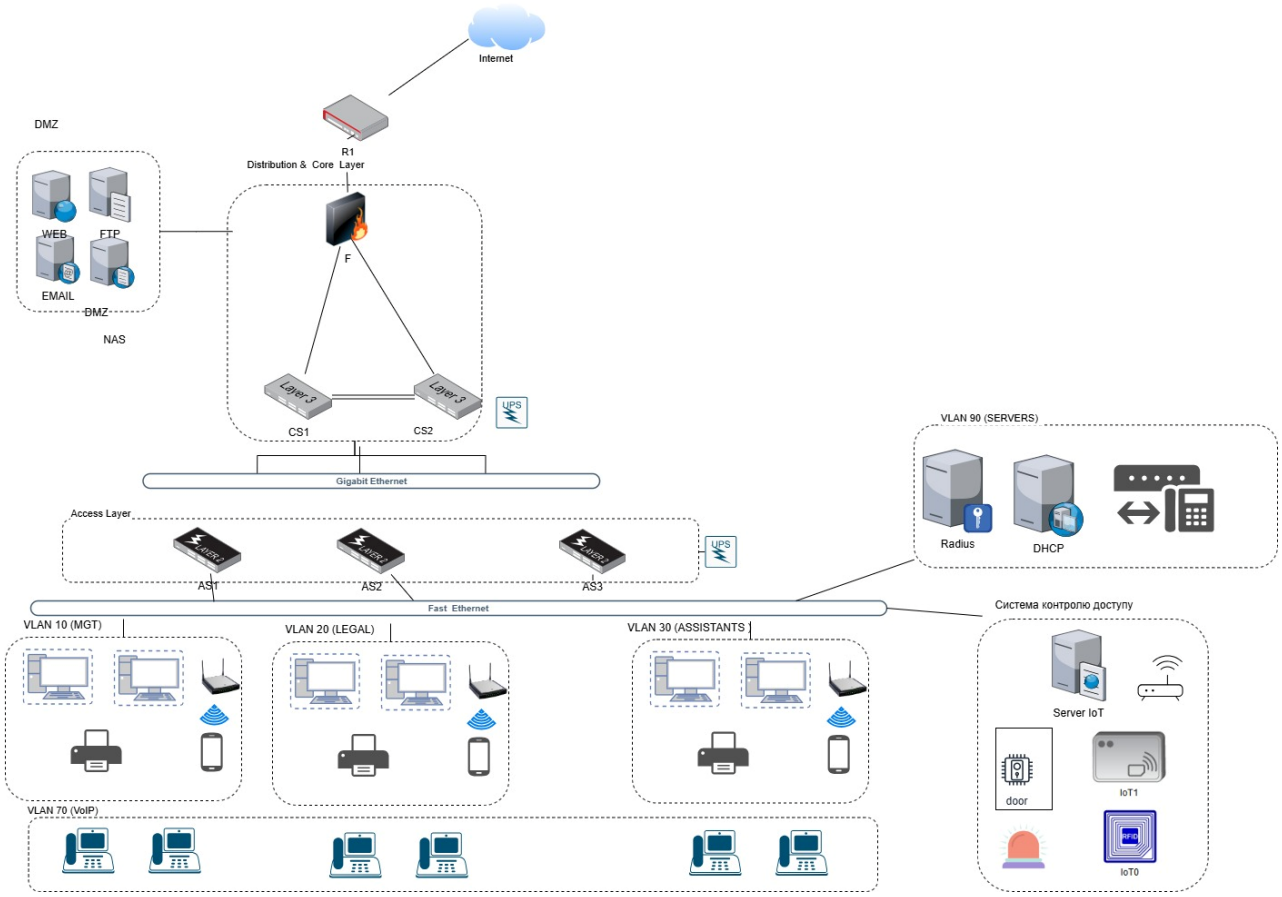

Рисунок 2.3 – Структурної схеми комплексу технічних засобів

2.2.3 Розробка специфікації апаратних засобів КС

У таблиці 2.2 подано рекомендовану специфікацію основного апаратного забезпечення для філії юридичної фірми на 30–40 працівників.

Для апаратної складової обрано Cisco, адже саме це обладнання підтримується у Packet Tracer. Це дає можливість моделювати і тестувати мережі на основі реального обладнання, що значно знижує ризики при впровадженні, покращує навички IT-персоналу та підвищує загальну ефективність системи контролю доступу.

Таблиця 2.2 – Специфікація обладнання

№	Компонент	Модель / Тип	Кіль.	Призначення
1	Маршрутизатор	Cisco ISR 1100	1	Основна маршрутизація, NAT, VPN
2	Комутатор L2+/L3	Cisco Catalyst 1000-24P	2	Агрегація трафіку, VLAN, PoE
3	Сервер	HPE ProLiant DL360	2	Контролер домену, CRM, файли, DNS, DHCP
4	Робочі станції	Dell OptiPlex	35	Юридична діяльність, обробка документів
5	Система резервного копіювання	NAS Synology	1	Архівування документів, щоденні копії
6	Wi-Fi точки доступу	Ubiquiti UniFi 6 LR	4	Безпровідне покриття офісу
7	ІБП	APC Smart-UPS	2	Безперебійне живлення серверів та маршрутизатора
9	Система відеоспостереження	IP-камери + NVR Dahua	4–6	Контроль офісу і серверної
10	Зчитувач смарт-карт USB	HID OMNIKEY 3121	10–15	Ідентифікація користувачів на робочих місцях
11	Контролер доступу	U-Prox IP500	1–2	Обробка запитів доступу, зберігання журналів входу/виходу
12	Електронні зчитувачі фізичного доступу	U-Prox SL	4–6	Доступ до серверної, архіву, адміністративних зон
13	Смарт-карти	HID Crescendo	40–50	Видаються співробітникам для ідентифікації
14	ПЗ для управління контролем доступу	U-Prox Web	1 ліцензія	Центральне адміністрування та звітність

З огляду на необхідність ідентифікації співробітників та обмеження доступу до критично важливих ресурсів комп’ютерної системи юридичної фірми, до апаратної структури включено систему контролю доступу на основі

смарт-карт. Така система реалізує фізичний контроль доступу до приміщень (серверної, архіву, офісних зон) шляхом використання електронних зчитувачів смарт-карт, з інтеграцією в систему безпеки.

Впровадження системи смарт-карт є критично важливим для юридичної фірми, яка оперує конфіденційною інформацією та підпадає під дію законодавства щодо захисту персональних даних (Закон України №2297-VI, ISO/IEC 27001) [3]. Така система також дозволяє адаптувати модель zero-trust security для доступу до цифрових сервісів.

Усі компоненти сумісні між собою, мають офіційну технічну підтримку та можуть інтегруватися з існуючими системами документації, безпеки та хмарного середовища.

3 РОЗРОБКА КОРПОРАТИВНОЇ МЕРЕЖІ ЮРИДИЧНОЇ ФІРМИ

3.1 Обґрунтування вибору компонентів та рішень

Міжмережеві екрани. Використання спеціалізованих міжмережевих екранів на периметрі є фундаментальним для захисту від зовнішніх загроз. Наявність двох пристроїв, підключених до різних ISP, забезпечує відмовостійкість інтернет-з'єднання.

Комутатори ядра. Вибір високопродуктивних L3-комутаторів для ядра мережі дозволяє ефективно маршрутизувати трафік між численними VLAN та забезпечувати високу пропускну здатність.

Технології HSRP та LACP. Впровадження HSRP гарантує безперервність роботи мережі у випадку відмови основного шлюзу, тоді як LACP збільшує пропускну здатність та надійність з'єднань між ключовими комутаторами.

Сегментація за допомогою VLAN. Розділення мережі на VLAN дозволяє ізолювати трафік різних функціональних груп, покращуючи безпеку, зменшуючи широкомовний трафік та спрощуючи адміністрування.

Розгортання DMZ. Винесення публічно доступних серверів у DMZ є стандартною практикою для захисту внутрішньої корпоративної мережі від прямих атак з Інтернету.

Виділені сервери для служб. Розгортання окремих серверів для DNS, DHCP та RADIUS забезпечує надійність та продуктивність цих критично важливих мережевих служб.

Централізоване управління WLAN. Використання контролера бездротової мережі спрощує розгортання, управління та моніторинг точок доступу Wi-Fi.

3.2 Розробка логічної топології мережі

Логічна структура відображає поділ мережі на зони безпеки, VLAN та основні маршрути між ними. Для реалізації цієї моделі обрано структуру на

основі VLAN, що відповідає принципу мінімальних прав доступу та знижує ризик міжсегментного проникнення.

Внутрішня мережа поділена на окремі віртуальні локальні мережі відповідно до організаційних підрозділів:

– VLAN 10 (MGT) – адміністрація;

– VLAN 20 (LEGAL) – юридичний відділ;

– VLAN 30 (ASSISTANTS) – асистенти, секретарі;

– VLAN 40 (FINANSE) – бухгалтерія;

– VLAN 50 (PR) – маркетинг і PR;

– VLAN 60 (WLAN) – робочі та гостьова мережі Wi-Fi;

– VLAN 70 (VoIP) – IP-телефонія;

– VLAN 90 (SERVERS) – серверна зона та моніторинг.

Кожен VLAN має бути ізольований за допомогою ACL. Доступ між сегментами контролюється міжмережевим екраном.

Така сегментація обмежує розповсюдження широкомовного трафіку, дозволяє впроваджувати політики безпеки й QoS на рівні кожної групи, покращує керованість і масштабованість інфраструктури.

3.3 Опис топології корпоративної мережі

Архітектура мережі побудована відповідно до принципів модульної мережної інфраструктури Cisco Hierarchical Campus Design [4] із розділенням на рівні доступу, агрегації та ядра з акцентом на безпеку, сегментацію, високу доступність та керованість (рис. 3.1). Мережа сформована на базі розподілу на DMZ-зону, внутрішні VLAN-сегменти для окремих відділів, серверний сегмент та зовнішні підключення до інтернет-провайдера та віддалений користувач. Передбачена інтеграція DMZ-зони, серверної ферми, резервування шлюзів з використанням HSRP, а також каналів LACP між основними комутаторами.

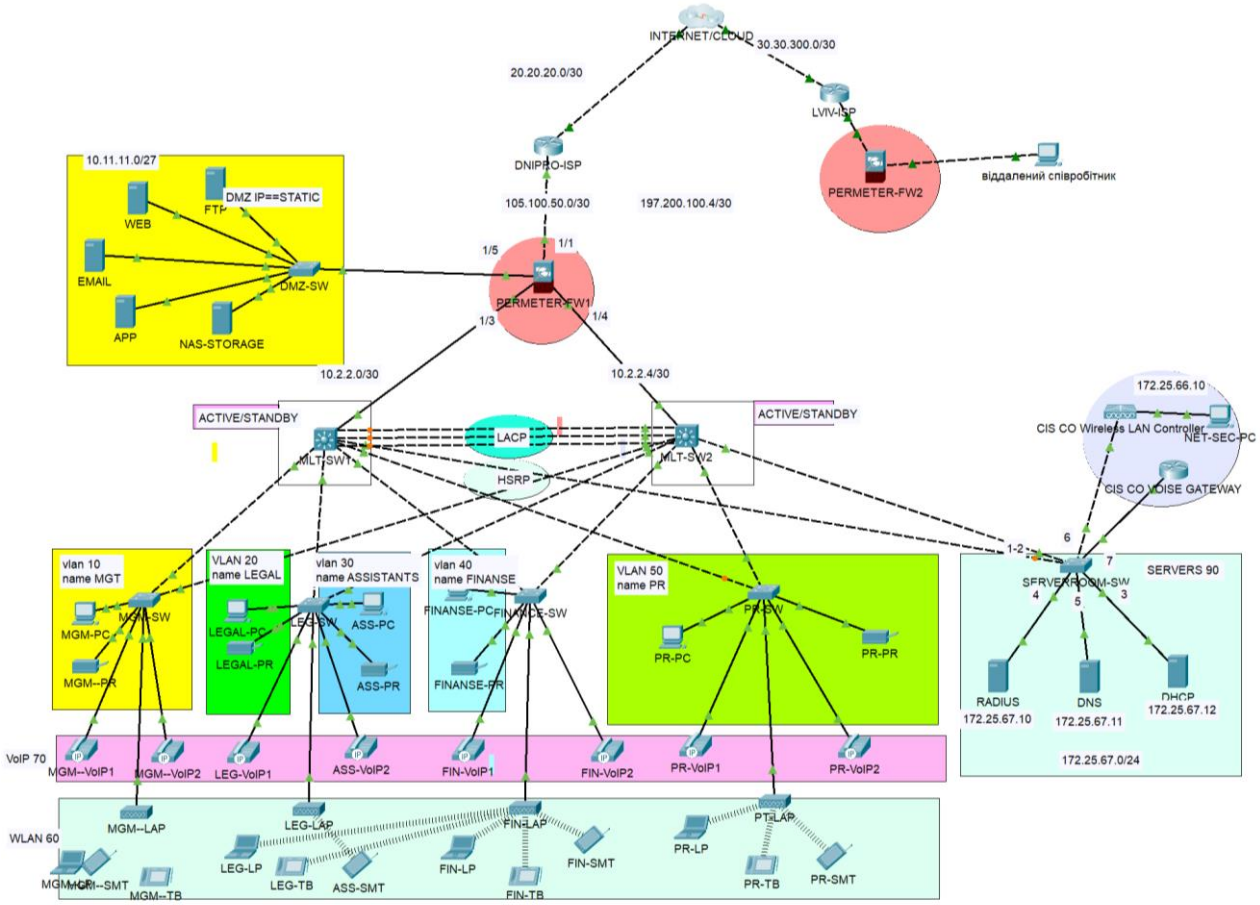

Рисунок 3.1 – Логічна топологія юридичної фірми

3.3.2 Distribution та Core Layer

Ядро мережі (рис. 3.2) побудоване на базі високопродуктивних комутаторів CORE-SW1, з наявністю резервного пристрою CORE-SW2 та реалізують протоколи високої доступності (HSRP, LACP). Ці комутатори забезпечують швидке, надійне магістральне транспортування трафіку між усіма частинами мережі (локальними сегментами, DMZ, серверною кімнатою та підключенням до интернету).Завдяки цьому досягається підвищена надійність системи маршрутів між ключовими сегментами. Ці комутатори L3 забезпечують швидкісну маршрутизацію між VLAN.

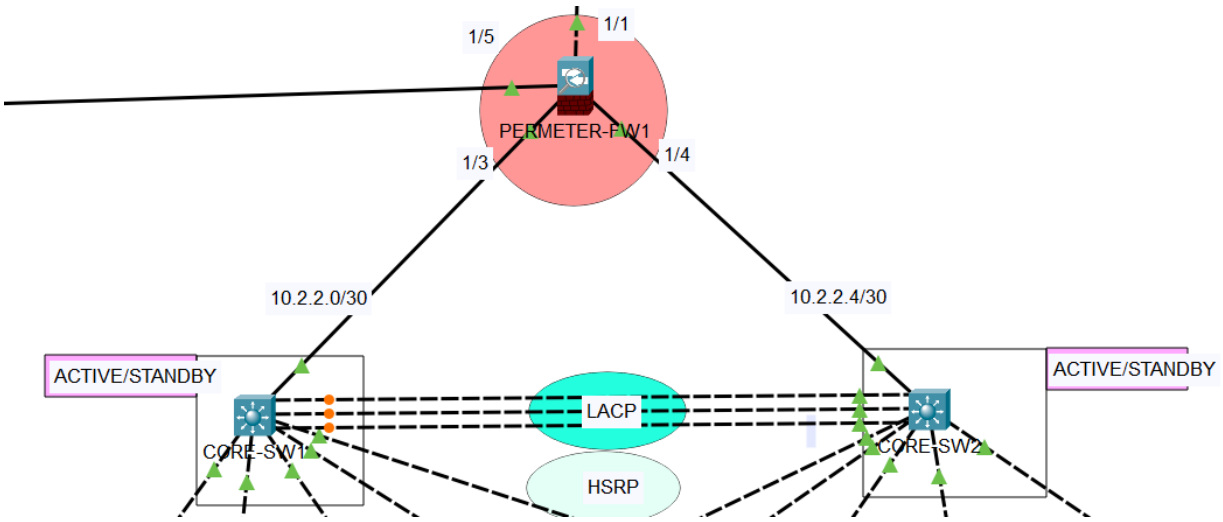

Рисунок 3.2 – Core Layer

HSRP (Hot Standby Router Protocol) застосовується для забезпечення резервування шлюзу за замовчуванням для підключених пристроїв.

LACP (Link Aggregation Control Protocol) використовується для агрегації декількох фізичних каналів в один логічний канал між комутаторами ядра, підвищуючи пропускну здатність та відмовостійкість.

З'єднання комутаторів ядра з фаєрволом PERMETER-FW1 є надлишковим (Gig інтерфейси), що мінімізує точку відмови.

PERIMETER-FW (фаєрвол) здійснює міжмережевий контроль трафіку між внутрішньою мережею, DMZ і зовнішніми інтерфейсами (Інтернет). Цей вузол реалізує роль граничного фільтра.

Всі комутатори доступу (MGM-SW, LEGAL-SW, ASSISTANTS-SW, FINANSE-SW, PR-SW, SERVERROOM-SW) під'єднані до ядра і таким чином потрапляють під централізоване управління фільтрацією та маршрутизацією трафіку.

Серверна частина (SERVERROOM-SW), яка також отримує підключення безпосередньо до ядра.

3.3.3 Access Layer

Цей рівень включає комутатори доступу, до яких приєднані кінцеві пристрої конкретних відділів (рис. 3.3). Кожна відділ має VoIP-телефони.

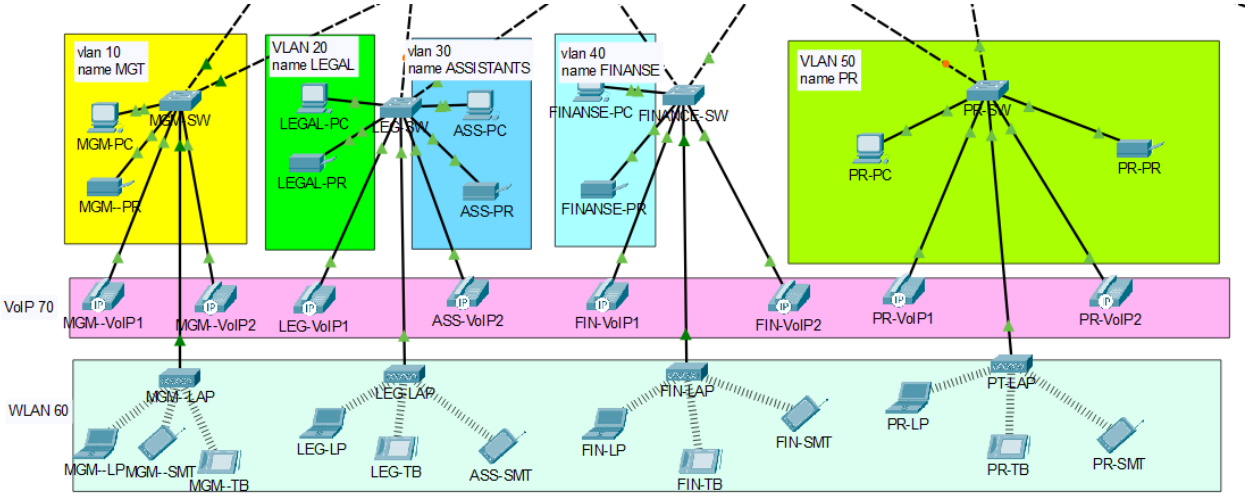

Рисунок 3.3 – Access Layer

MGM-SW (VLAN 10 MGT) – підключає комп'ютери керівництва.

LEGAL-SW (VLAN 20 LEGAL), ASSISTANTS-SW (VLAN 30 ASSISTANTS), FINANSE-SW (VLAN 40 FINANSE), PR-SW (VLAN 50 PR) – реалізують доступ до пристроїв відповідних підрозділів, виділяючи кожен відділ у свою VLAN.

SERVERROOM-SW (VLAN 90 SERVERS) – серверна кімната з ключовими сервісами: RADIUS, DNS, DHCP.

До комутаторів підключені IP-телефони (VLAN 70 VoIP), таким чином голосовий трафік теж сегментується окремо від даних.

У нижній частині топології є додаткові сервіси – Wi-Fi контролер та голосовий шлюз (Cisco Voice Gateway), що приєднані до серверної частини та ядра.

3.3.4 Зовнішні підключення та підключення до Інтернету

Два міжмережеві екрани, PERMETER-FW1 та PERMETER-FW2, слугують першою лінією оборони. PERMETER-FW1 підключений до DNIPRO-ISP, а PERMETER-FW2 до LVIV-ISP (рис. 3.4).

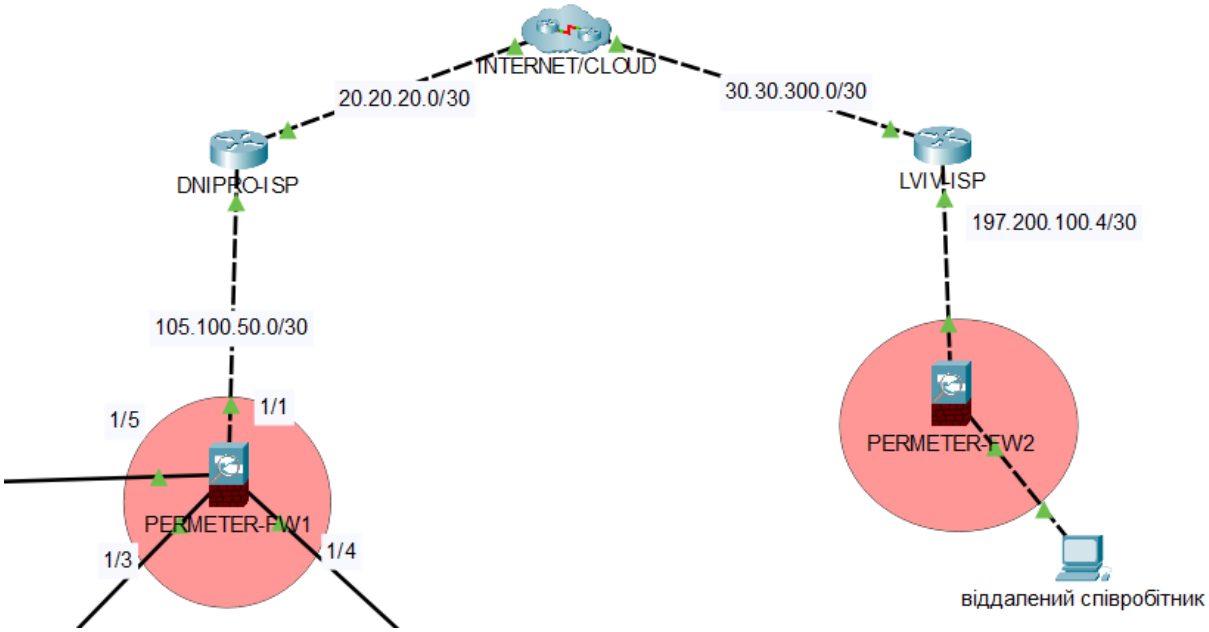

Рисунок 3.4 – Підключення до Інтернет

Ці пристрої відповідають за фільтрацію трафіку, трансляцію мережевих адрес (NAT), запобігання вторгненням та VPN-з'єднання.

Мережа фірми підключена до інтернет-провайдеру DNIPRO-ISP. Віддалений користувач підключений до до інтернет-провайдеру LVIV-ISP. Для налаштування підключення віддаленого користувача через VPN змодельована мережа Internet.

Підключення до DNIPRO-ISP використовує IP-адреси з діапазону 105.100.50.0/30.

Підключення до LVIV-ISP використовує IP-адресу з діапазону 197.200.100.0/30.

3.3.5 Демілітаризована зона (DMZ)

Виділена ізолована підмережа для серверів (EMAIL, FTP, NAS-STORAGE, APP), призначених для взаємодії з зовнішніми клієнтами та обробки неавторизованого трафіку (рис.3.5). Це ізольований сегмент, що підвищує безпеку внутрішньої мережі.

Компоненти:

– комутатор DMZ-SW агрегує трафік DMZ;

– сервери: WEB, EMAIL, FTP, APP, NAS-STORAGE зі статичною адресацією.

DMZ підключена до інтерфейсу Fa0/1 на PERMETER-FW1. Використовується статична IP-адресація в підмережі 10.11.11.0/27.

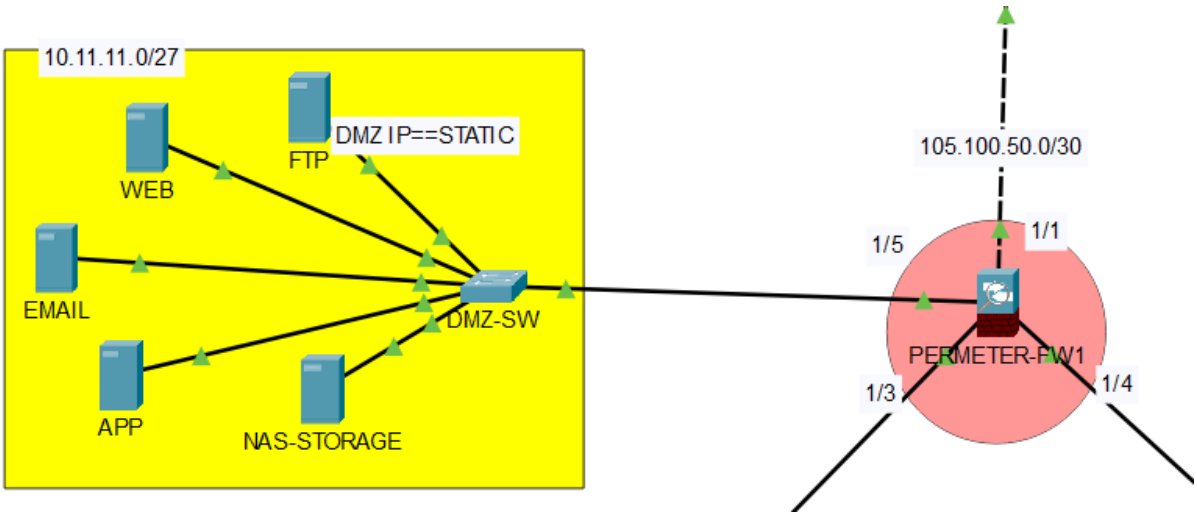

Рисунок 3.5 – Сегмент DMZ

3.3.6 Серверна кімната та мережеві сервіси

Окрема VLAN для критичних служб: DHCP, DNS, RADIUS, як основа для централізованого керування аутентифікацією та адмініструванням мережевих ресурсів.

Підключення здійснюється через окремий комутатор SERVERROOM-SW (рис. 3.6).

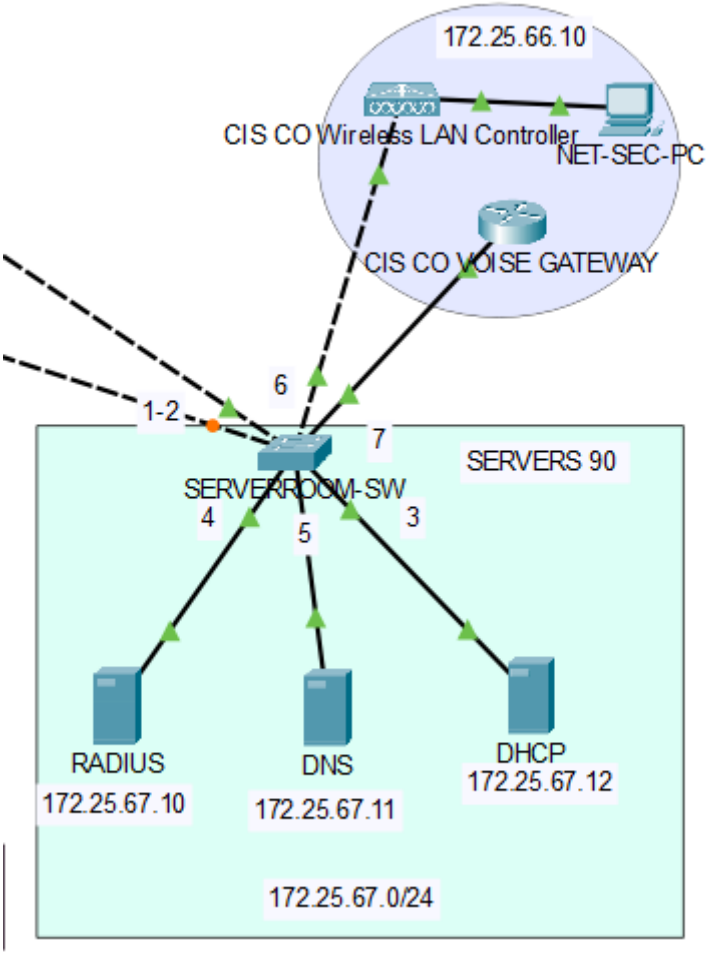

Рисунок 3.6 – Внутрішні сервери (VLAN 90)

Внутрішні сервери (VLAN 90, підмережа 172.25.67.0/24):

– RADIUS (172.25.67.10): для централізованої автентифікації, авторизації та обліку користувачів;

– DNS (172.25.67.11): для розв'язання доменних імен;

– DHCP (172.25.67.12): для автоматичного призначення IP-адрес клієнтським пристроям.

Cisco Wireless LAN Controller та Cisco Voice Gateway (172.25.66.10) під VLAN 60 для бездротового доступу, також підключені через серверний комутатор.

Інфраструктура IP-телефонії

– CISCO VOISE GATEWAY (або голосовий шлюз): забезпечує функціональність VoIP (VoIP, VLAN 70).

3.4 Розрахунок адресного простору

Адресація в локальній мережі організована з використанням приватних діапазонів IPv4 для внутрішніх сегментів, що дозволяє гнучко масштабувати мережу без ризику колізій та лімітує видимість внутрішньої інфраструктури ззовні.

Для доступу в Інтернет використовуються публічні адреси з таблиці 3.1.

Таблиця 3.1 – Схема адресації мереж

Ім’я VLAN	Номер VLAN	Адреса підмережі	Діапазон допустимих IP-адрес вузлів	Шлюз
DMZ	1	10.11.11.0/27	10.11.11.1–10.11.11.30	10.11.11.1
ISP1 – FWL1	1	105.100.50.0/30	105.100.50.1–105.100.50.2	
ISP1 – FWL2	1	105.100.50.4/30	105.100.50.5–105.100.50.6	
ISP1–Internet	1	20.20.20.0/30	20.20.20.1 – 20.20.20.2	
ISP2–Internet	1	30.30.30.0/30	30.30.30.1 – 30.30.30.2	
LAN	172.25.64.0/22			
MGT	10	172.25.64.0/25	172.25.64.1 – 172.25.64.126	172.25.64.1
LEGAL	20	172.25.64.128/25	172.25.64.129 – 172.25.64.254	172.25.64.129
ASSISTANTS	30	172.25.65.0/26	172.25.65.1 – 172.25.65.62	172.25.65.1
FINANSE	40	172.25.65.64/26	172.25.65.65 – 172.25.65.126	172.25.65.65
PR	50	172.25.65.128/26	172.25.65.129 – 172.25.65.190	172.25.65.129
WLAN	60	172.25.66.0/24	172.25.66.1 –172.25.66.254	172.25.66.1
VoIP	70	172.25.65.192/26	172.25.65.193 – 172.25.65.254	172.25.65.193
SERVERS	90	172.25.67.0/24	172.25.67.1 –172.25.67.254	172.25.67.1

Локальні підмережі жорстко фіксовані під конкретні VLAN, що забезпечує чітке логічне розмежування доменів мовлення.

Базовий блок адрес для локальної мережі LAN – 172.25.64.0/22 (діапазон: 172.25.64.0 – 172.25.67.255). Цей блок потім розумно поділений на менші підмережі для різних VLAN, враховуючи їхні потреби в кількості хостів.

VLAN 10 та 20 є більшими (до 126 хостів кожна).

VLAN 30, 40, 50, 60 є меншими (до 62 хостів кожна).

VLAN 70 та 99 (можливо, для спеціальних потреб, як-от гостьова мережа, управління або сервери) є стандартними мережами класу C (до 254 хостів кожна).

Таким чином простір VLAN розподіллено так.

VLAN 10: 172.25.64.0/25

Мережева адреса: 172.25.64.0

Маска підмережі: /25 = 255.255.255.128

Кількість бітів для хостів: 32 - 25 = 7 біт

Загальна кількість адрес в підмережі: 2^7 = 128

Кількість доступних хостів: 128 - 2 (адреса мережі та широкомовна адреса) = 126 хостів.

Широкомовна адреса (Broadcast): 172.25.64.127

Діапазон IP-адрес для хостів: 172.25.64.1 - 172.25.64.126

VLAN 20: 172.25.64.128/25

Мережева адреса: 172.25.64.128

Маска підмережі: /25 = 255.255.255.128

Кількість доступних хостів: 126 хостів.

Широкомовна адреса (Broadcast): 172.25.64.255

Діапазон IP-адрес для хостів: 172.25.64.129 - 172.25.64.254

Примітка: VLAN 10 та VLAN 20 разом займають весь діапазон 172.25.64.0/24.

VLAN 30: 172.25.65.0/26

Мережева адреса: 172.25.65.0

Маска підмережі: /26 = 255.255.255.192

Кількість бітів для хостів: 32 - 26 = 6 біт

Загальна кількість адрес в підмережі: 64

Кількість доступних хостів: 64 - 2 = 62 хости.

Широкомовна адреса (Broadcast): 172.25.65.63

Діапазон IP-адрес для хостів: 172.25.65.1 - 172.25.65.62

VLAN 40: 172.25.65.64/26

Мережева адреса: 172.25.65.64

Маска підмережі: /26 = 255.255.255.192

Кількість доступних хостів: 62 хости.

Широкомовна адреса (Broadcast): 172.25.65.127

Діапазон IP-адрес для хостів: 172.25.65.65 - 172.25.65.126

VLAN 50: 172.25.65.128/26

Мережева адреса: 172.25.65.128

Маска підмережі: /26 = 255.255.255.192

Кількість доступних хостів: 62 хости.

Широкомовна адреса (Broadcast): 172.25.65.191

Діапазон IP-адрес для хостів: 172.25.65.129 - 172.25.65.190

VLAN 60: 172.25.65.192/26

Мережева адреса: 172.25.65.192

Маска підмережі: /26 = 255.255.255.192

Кількість доступних хостів: 62 хости.

Широкомовна адреса (Broadcast): 172.25.65.255

Діапазон IP-адрес для хостів: 172.25.65.193 - 172.25.65.254

Примітка: VLAN 30, 40, 50 та 60 разом займають весь діапазон 172.25.65.0/24.

VLAN 70: 172.25.66.0/24

Мережева адреса: 172.25.66.0

Маска підмережі: /24 = 255.255.255.0

Кількість бітів для хостів: 32 - 24 = 8 біт

Загальна кількість адрес в підмережі: 256

Кількість доступних хостів: 256 - 2 = 254 хости.

Широкомовна адреса (Broadcast): 172.25.66.255

Діапазон IP-адрес для хостів: 172.25.66.1 - 172.25.66.254

VLAN 99: 172.25.67.0/24

Мережева адреса: 172.25.67.0

Маска підмережі: /24 = 255.255.255.0

Кількість доступних хостів: 254 хости.

Широкомовна адреса (Broadcast): 172.25.67.255

Діапазон IP-адрес для хостів: 172.25.67.1 - 172.25.67.254

Адресація серверів, шлюзів і служб резервується у верхньому діапазоні кожного VLAN. Це дозволяє забезпечити стабільність керування IP та централізований моніторинг.

3.5 Базові налаштування безпеки та SSH

В Додатку А наведено базові налаштування для маршрутизаторів та 3-рівневих комутаторів сприяють створенню безпечного середовища для управління мережевими пристроями.

Виконується встановлення ідентифікатора, що дозволяє вказати ім'я хоста, яке допомагає в управлінні мережевими пристроями.

Конфігурація консолі є важливою для локального доступу до пристрою. Установлені наступні параметри:

– пароль: встановлення пароля *cisco*, що вимагає авторизації для входу;

– синхронне ведення журналу: реалізує функцію *logging synchronous*, яка запобігає перериванню введення команд інформацією з журналу;

– часова аутентифікація: параметр *exec-timeout 3 0*, що встановлює тайм-аут входу в консоль на 3 хвилини бездіяльності.

Заходи безпеки:

– шифрування паролів: команда *service password-encryption* забезпечує захист паролів в конфігурації, перетворюючи їх у закодований формат;

– локальний обліковий запис: створення локального користувача *cisco* з паролем *cisco*, що дозволяє контролювати доступ до системи;

– вимкнення DNS-резолюції: виконання команди *no ip domain-lookup* запобігає спробам DNS-резолюції у випадку введення помилкових команд.

SSH (Secure Shell) забезпечує надійний та зашифрований протокол для віддаленого доступу до мережевих пристроїв. Налаштуванням передбачено:

– генерація RSA-ключів для SSH: команда crypto key generate rsa general-keys modulus 1024 генерує ключі шифрування для підключення;

– налаштування версії SSH: через команду *ip ssh version 2* прописується використання безпечнішої другої версії протоколу;

– контроль доступу до VTY з 0 до 15 реалізується в поєднанні з використанням локального користувача, що забезпечить автентифікацію через *login local* і дозволить лише SSH-підключення з параметром *transport input ssh*.

3.6 Сегментація мережі VLAN

Сегментація мережі через використання VLAN (Virtual Local Area Networks) є важливим елементом для оптимізації управління трафіком та підвищення безпеки. В Додатку А наведено конфігурації комутаторів доступу, включаючи MK-SW, HR-SW, FINANCE-SW, ADMIN-SW, LEG-SW, SERVER-SW, MLT1 та MLT2.

Мережа логічно сегментована на декілька VLAN для ізоляції трафіку різних відділів та служб, підвищення безпеки та керованості:

– VLAN 10 (MGT): 172.25.64.0/25 (адміністрація);

– VLAN 20 (LEGAL): 172.25.64.128/25 (Юридичний відділ)

– VLAN 30 (ASSISTANTS): 172.25.65.0/25 (Асистенти)

– VLAN 40 (FINANSE): 172.25.65.64/25 (бухгалтерія)

– VLAN 50 (PR): 172.25.65.128/26 (Відділ зв'язків з громадськістю)

– VLAN 60 (WLAN): 172.25.66.0/24 (Бездротова мережа)

– VLAN 70 (VoIP): 172.25.65.192/28 (IP-телефонія)

– VLAN 90 (SERVERS): 172.25.67.0/24 (Внутрішні сервери)

Комутатори рівня доступу (наприклад, FINANSE-SW, PR-SW, та інші, що підключаються до ядра) забезпечують підключення кінцевих пристроїв (ПК, принтери, VoIP-телефони, точки доступу Wi-Fi) до відповідних VLAN.

Комутатори (MK-SW, HR-SW, FINANCE-SW, ADMIN-SW, ICT-SW)

Для кожного з перерахованих комутаторів налаштування виглядають наступним чином:

– trunk ports: Fa0/1-2 налаштовані на роботу в режимі транку, що дозволяє з’єднувати їх з іншими комутаторами або маршрутизаторами, передаючи трафік усіх VLAN.

– access port: Fa0/3-4 призначені до відповідного VLAN відділіу, в якому працює співробітник, Fa0/5-6 – для VLAN 70 (з VoIP). Порт Fa0/7 підключений до VLAN 50 (WLAN).

Конфігурація SERVERROOM-SW є подібною до попередніх комутаторів з додаванням нового VLAN 90 (рис.3.7-3.8):

– trunk ports:Fa0/1-2, Fa0/7;

– accesss port: Fa0/3-5 налаштовані на VLAN 90, а Fa0/6 – на VLAN 60.

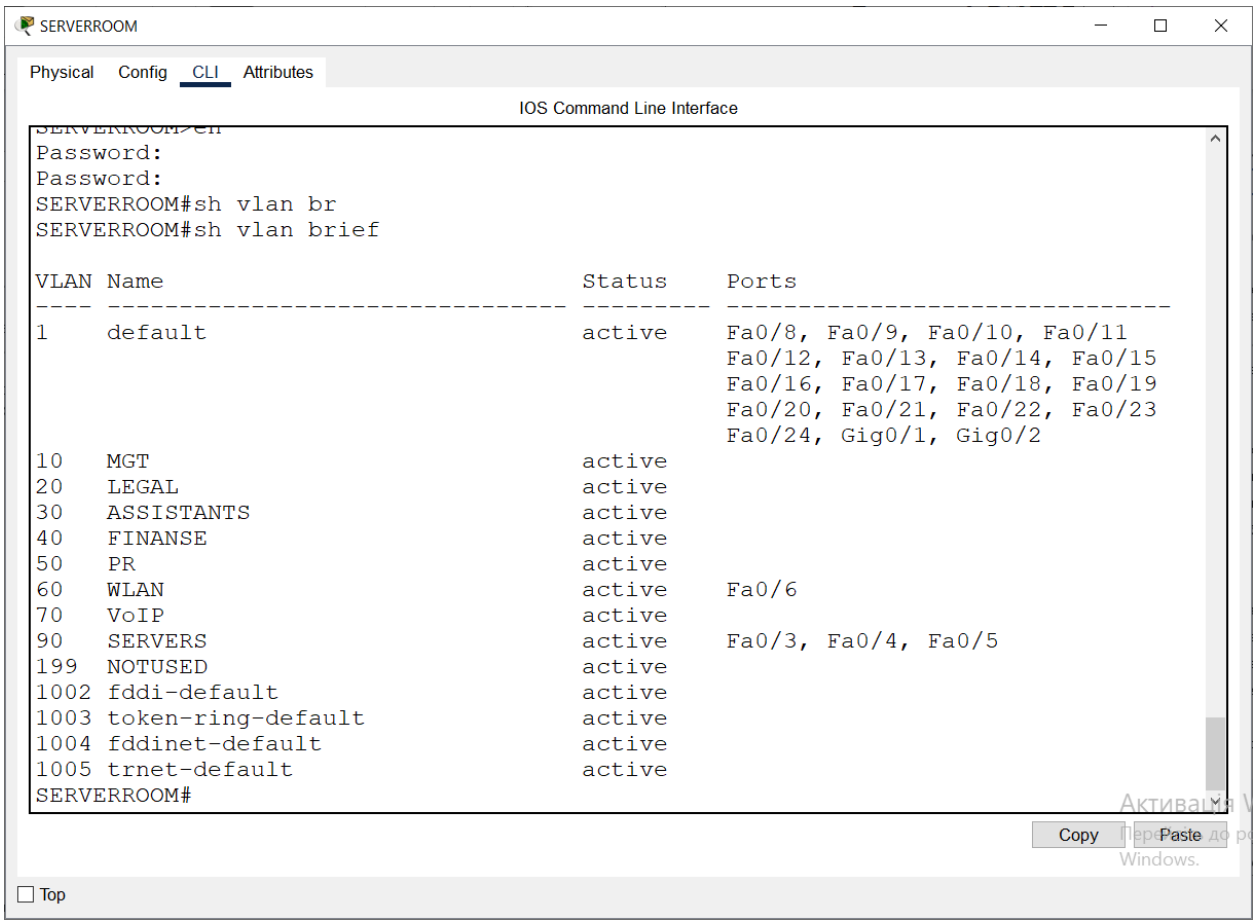

Рисунок 3.7 – VLAN на SERVERROOM-SW

```
SERVERROOM#sh  interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      1
Fa0/2       on           802.1q         trunking      1
Fa0/7       on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-1005
Fa0/2       1-1005
Fa0/7       1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1,10,20,30,40,50,60,70,90,199
Fa0/2       1,10,20,30,40,50,60,70,90,199
Fa0/7       1,10,20,30,40,50,60,70,90,199

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       none
Fa0/2       1,10,20,30,40,50,60,70,90,199
Fa0/7       1,10,20,30,40,50,60,70,90,199
```

Рисунок 3.8 – Налаштування транкових портів на SERVERROOM-SW

3.7 HSRP та Inter-VLAN

В Додатку А реалізовано розподілену маршрутизацію на рівні доступу з використанням віртуальних інтерфейсів VLAN (SVI) на MLT-SW1 і MLT-SW2.

Ці комутатори утворюють резервну пару з високою доступністю завдяки протоколу HSRP (Hot Standby Router Protocol), який забезпечує безперервність доступу до шлюзів підмереж у разі відмови одного з пристроїв.

Кожен з комутаторів має окрему IP-адресу в кожному VLAN для участі в маршрутизації.

HSRP використовується для створення резервних шлюзів. Комутатори MLT-SW1 і MLT-SW2 мають реальні IP-адреси у VLAN, а також розділяють віртуальні IP-адреси як основні шлюзи для відповідних підмереж (табл. 3.2).

Таблиця 3.2 – VLAN та адресація

VLAN	Назва	Адреса HSRP шлюзу	IP на MLT-SW1	IP на MLT-SW2	Маска
10	MGT	172.25.64.1	172.25.64.2	172.25.64.3	255.255.255.128
20	LEGAL	172.25.64.129	172.25.64.130	172.25.64.131	255.255.255.128
30	ASSISTANTS	172.25.65.1	172.25.65.2	172.25.65.3	255.255.255.192
40	FINANCE	172.25.65.65	172.25.65.66	172.25.65.67	255.255.255.192
50	PR	172.25.65.129	172.25.65.130	172.25.65.131	255.255.255.192
60	WLAN	172.25.66.1	172.25.66.2	172.25.66.3	255.255.255.0
70	VoIP	172.25.65.193	172.25.65.194	172.25.65.195	255.255.255.192
90	SERVER-SW	172.25.67.1	172.25.67.2	172.25.67.3	255.255.255.0

При цьому один комутатор виступає активним маршрутизатором, інший – резервним. У разі відмови активного вузла, HSRP автоматично активує резервний.

Усі SVI інтерфейси мають налаштування *ip helper-address*, скеровані на IP-адресу сервера DHCP (172.25.67.12). Це дозволяє пересилати DHCP-запити з відповідної VLAN до центрального DHCP-сервера, який фізично може бути розташований в іншому сегменті мережі.

Перевірка правильності конфігурації HSRP та функціонування здійснювалася за допомогою таких діагностичних команд та етапів:

1. Перевірка статусу HSRP на активному та резервному пристрої командою:

show standby brief

Ця команда дозволяє отримати стислу інформацію про всі групи HSRP, налаштовані на комутаторі. Очікуваним результатом є наявність статусу Active на одному пристрої (рис. 3.9) та Standby – на іншому (рис.3.10). IP-адреса віртуального шлюзу повинна бути ідентичною на обох комутаторах для відповідної VLAN-групи.

```
MLT-SW1#sh standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Vl10        10   100   Standby  172.25.64.3     local           172.25.64.1
Vl20        20   100   Standby  172.25.64.131   local           172.25.64.129
Vl30        30   100   Standby  172.25.65.3     local           172.25.65.1
Vl40        40   100   Standby  172.25.65.67    local           172.25.65.65
Vl50        50   100   Standby  172.25.65.131   local           172.25.65.129
Vl60        60   100   Standby  172.25.66.3     local           172.25.66.1
Vl70        50   100   Active   local           unknown         172.25.65.193
Vl90        90   100   Standby  172.25.67.3     local           172.25.67.1
```

Рисунок 3.9 – Перевірка статусу HSRP на MLT-SW1

```
MLT-SW2#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Vl10        10   100   Active   local           172.25.64.2     172.25.64.1
Vl20        20   100   Active   local           172.25.64.130   172.25.64.129
Vl30        30   100   Active   local           172.25.65.2     172.25.65.1
Vl40        40   100   Active   local           172.25.65.66    172.25.65.65
Vl50        50   100   Active   local           172.25.65.130   172.25.65.129
Vl60        60   100   Active   local           172.25.66.2     172.25.66.1
Vl70        50   100   Active   local           unknown         172.25.65.193
Vl90        90   100   Active   local           172.25.67.2     172.25.67.1
```

Рисунок 3.10 – Перевірка статусу HSRP на MLT-SW2

2. Тестування доступності шлюзу з боку кінцевих станці:

За допомогою команди tracert на IP-адресу провайдера із клієнтськлої машини у VLAN20 проводилась перевірка доступності віртуального шлюзу.

На рисунку 3.11 ПК має адресу віртуального шлюзу, але шлях пролягав через MLT_SW2, так як він має статус Active.

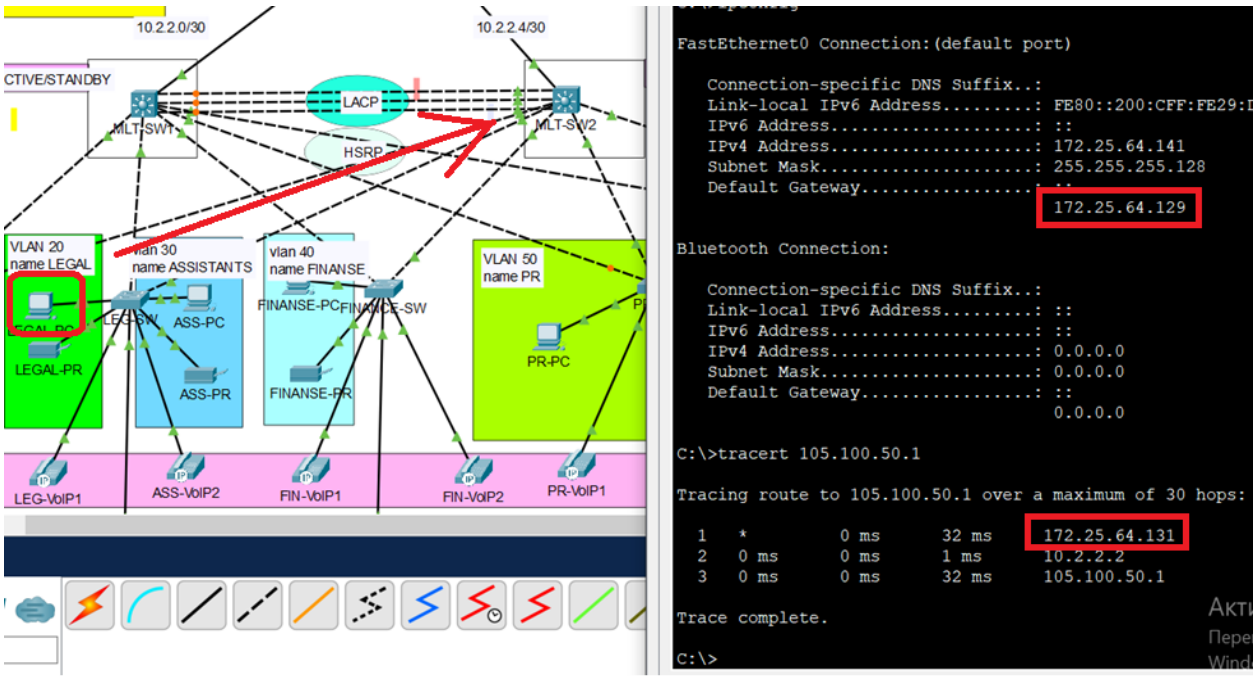

Рисунок 3.11 – Перевірка HSRP

На рисунку 3.12 змодельована ситуація, коли MLT-SW2 вийшов з ладу, тоді роль Active переходить на MLT-SW1, що підтверджує результат tracert.

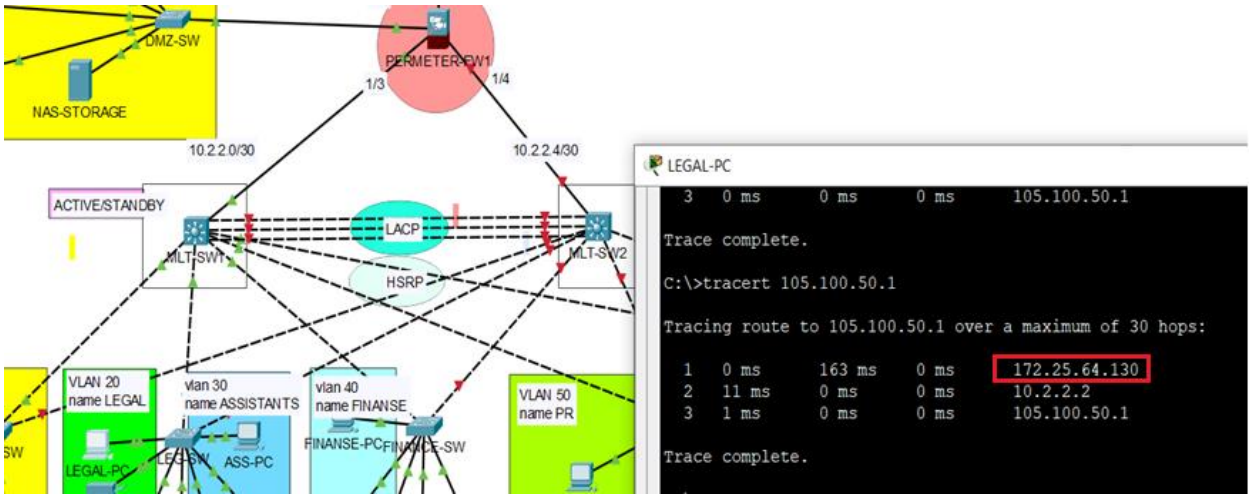

Рисунок 3.12 – Перевірка HSRP

3.8 Налаштування механізмів захисту рівня доступу

В додатку А налаштовані функції spanning-tree portfast та bpduguard enable на портах доступу є стандартною та рекомендованою практикою в архітектурі корпоративних мереж Cisco. Вони забезпечують:

– зменшення часу підключення клієнтів до мережі;

– захист від STP-атак і неправильних підключень;

– стабільність і безпеку мережевого рівня доступу.

Ці параметри повинні застосовуватись до всіх інтерфейсів, які використовуються для підключення кінцевих пристроїв, однак не повинні бути активовані на uplink-портах або trunk-з'єднаннях між комутаторами.

Типова конфігурація для всіх комутаторів доступу:

```
interface range fa0/3 - 24
 spanning-tree portfast
 spanning-tree bpduguard enable
```

Ця конфігурація застосовується до всіх комутаторів рівня доступу. Вона забезпечує захист користувацьких портів, які, як правило, підключаються до кінцевих пристроїв (робочих станцій, принтерів тощо). Таке налаштування дозволяє зменшити час підключення клієнтів до мережі та знижує ризик порушень в роботі STP через неправильне або зловмисне підключення обладнання.

Налаштування комутатора серверної кімнати SERVERROOM-SW інтерфейси Fa0/3–Fa0/6 та Fa0/8–Fa0/24 переводяться в режим швидкої активації (PortFast) , що дозволяє негайне включення портів без проходження стандартних фаз STP (Blocking → Listening → Learning → Forwarding). Такий підхід зменшує час очікування підключення серверів до мережі. Додатково, задіяно BPDU Guard, що є критичним механізмом захисту для портів доступу. У разі виявлення на таких портах BPDU-повідомлень (ознака підключення іншого комутатора), порт буде автоматично вимкнений, що унеможливлює виникнення петель та несанкціонованих підключень до мережевої інфраструктури.

```
interface FastEthernet0/3
 switchport access vlan 90
 switchport mode access
 spanning-tree portfast
 spanning-tree bpduguard enable
```

DMZ (Demilitarized Zone) – це окрема частина мережі, яка містить ресурси, доступні як для внутрішніх, так і зовнішніх користувачів (наприклад,

веб-сервери, поштові шлюзи). Конфігурація аналогічна до попередніх блоків, однак тут охоплено всі 24 порти (fa0/1–24), з можливістю підключення різних сервісних пристроїв. Увімкнення PortFast у DMZ-SW обумовлене потребою у швидкій доступності сервісів після перезавантаження пристроїв. BPDU Guard тут критично важливий, оскільки порти DMZ є потенційно вразливими через відкритість до зовнішніх джерел трафіку.

3.9 Конфігурація агрегованого каналу

У сучасних корпоративних мережах для підвищення пропускної здатності та забезпечення відмовостійкості між магістральними або ключовими комутаторами використовується агрегація каналів. У даній інфраструктурі для цього реалізовано LACP-агрегацію між комутаторами MLT-SW1 і MLT-SW2 з використанням інтерфейсів GigabitEthernet1/0/9-11 (рис.3.13). Такий підхід дозволяє не лише збільшити смугу пропускання між ключовими вузлами мережі, але й значно покращити її стійкість до збоїв та ефективність використання ресурсів.

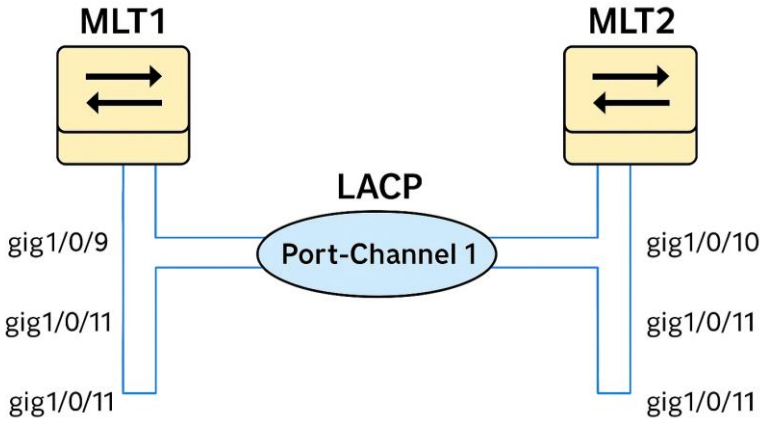

Рисунок 3.13 – Агрегування каналів

Для формування об'єднаного каналу використано LACP (IEEE 802.3ad) – динамічний протокол, який автоматизує процес створення port-channel, забезпечує перевірку сумісності портів та дозволяє автоматичне виявлення відмов каналів.

В Додатку А наведено налаштування на комутаторах MLT-SW1 і MLT-SW2. На комутаторі MLT-SW1 відповідні інтерфейси (gig1/0/9-11) об'єднуються в канал з параметром *mode active,* тобто комутатор активно ініціює створення LACP-зв’язку.

Після об’єднання, логічний інтерфейс *Port-Channel 1* переводиться у режим транкування (switchport mode trunk), що дозволяє передавати трафік із декількох VLAN-ів через один об’єднаний логічний канал.

На комутаторі MLT-SW2 відповідні порти (gig1/0/9-11) об'єднуються в той самий порт-канал з параметром *mode passive*, тобто комутатор очікує ініціацію з боку MLT-SW1:

На рисунку 3.14 наведено перевірка роботи портів.

```
MLT-SW1#sh etherchannel port-channel
                Channel-group listing:
                ----------------------

Group: 1
----------
                Port-channels in the group:
                ---------------------------

Port-channel: Po1    (Primary Aggregator)
------------

Age of the Port-channel   = 00d:01h:39m:09s
Logical slot/port   = 2/1       Number of ports = 3
GC                  = 0x00000000      HotStandBy port = null
Port state          = Port-channel
Protocol            =   LACP
Port Security       = Disabled

Ports in the Port-channel:

Index   Load   Port     EC state        No of bits
------+------+------+------------------+-----------
  0     00     Gig1/0/10Active             0
  0     00     Gig1/0/11Active             0
  0     00     Gig1/0/9 Active             0
Time since last port bundled:    00d:01h:39m:08s    Gig1/0/9
MLT-SW1#
```

```
MLT-SW2#sh etherchannel port-channel
                Channel-group listing:
                ----------------------

Group: 1
----------
                Port-channels in the group:
                ---------------------------

Port-channel: Po1    (Primary Aggregator)
------------

Age of the Port-channel   = 00d:01h:38m:39s
Logical slot/port   = 2/1       Number of ports = 3
GC                  = 0x00000000      HotStandBy port = null
Port state          = Port-channel
Protocol            =   LACP
Port Security       = Disabled

Ports in the Port-channel:

Index   Load   Port     EC state        No of bits
------+------+------+------------------+-----------
  0     00     Gig1/0/11Passive            0
  0     00     Gig1/0/10Passive            0
  0     00     Gig1/0/9 Passive            0
Time since last port bundled:    00d:01h:38m:38s    Gig1/0/9
MLT-SW2#
```

Рисунок 3.14 – Перевірка Port-Channel

На рисунку 3.15 в розділі пропускної здатності маємо значення 300 Мб/с, що відповідає нашим очікуванням.

```
MLT-SW2#show interfaces port-channel 1
Port-channel1 is up, line protocol is up (connected)
  Hardware is EtherChannel, address is 00d0.bc18.2047 (bia 00d0.bc18.2047)
  MTU 1500 bytes, BW 3000000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Half-duplex, 3000Mb/s
  input flow-control is off, output flow-control is off
  Members in this channel: Gig1/0/9 ,Gig1/0/10 ,Gig1/0/11 ,
```

Рисунок 3.15 – Властивості port-channel 1

3.10 Налаштування динамічної маршрутизації OSPF

У розробленій комп'ютерній системі для юридичної фірми реалізовано динамічну маршрутизацію за допомогою протоколу OSPF (Open Shortest Path First) версії 2. Обраний протокол належить до внутрішньої маршрутизації типу *link-state*, є масштабованим, стабільним і широко використовується в корпоративних мережах із багатьма підмережами.

Для прикладного впровадження у мережі організації створено OSPF-процес з номером 35, який охоплює всі основні маршрутизатори та L3-комутатори в архітектурі.

L3-комутатор MLT-SW1 виконує функцію магістрального маршрутизатора ядра. Призначено унікальний router-id 1.1.1.1, що забезпечує ідентифікацію вузла в топології OSPF. У процес маршрутизації включено мережу 10.2.2.0/30, це точка зв'язку з іншим ядром (MLT-SW2), а також мережу 172.25.64.0/22, що охоплює локальну адресацію корпоративної мережі (офіси, сервери, VLAN).

Другий магістральний комутатор MLT-SW2 дублює та резервує функції першого, має свій router-id 1.1.2.2, бере участь у маршрутизації тієї ж корпоративної підмережі, канал між MLT-SW1 та MLT-SW2 (10.2.2.0/30, 10.2.2.4/30) забезпечує відмовостійкість зв'язку всередині ядра.

DNIPRO-ISP (граничний маршрутизатор) реалізує зв'язок між центральним офісом у Дніпрі та глобальною мережею:

– 105.100.50.0/30 канал до провайдера або GRE-тунель до іншого офісу;

– 20.20.20.0/30 резервна точка або DMZ для фільтрації зовнішнього трафіку.

Щоб перевірити коректність роботи протоколу виконаємо низку діагностичних дій.

3.11 Конфігурація VoIP

У сучасному бізнес-середовищі важливість комунікаційних технологій важко переоцінити. Одним із найзначніших інновацій у цій сфері стало впровадження системи IP-телефонії, яка дозволяє передавати голосові дані через Інтернет-протоколи. Конфігурація VoIP, представлена в Додатку А, ілюструє приклад реалізації цього рішення на маршрутизаторі CISCO VOISE GATEWAY (або голосовий шлюз).

Першим кроком у конфігурації є створення підінтерфейсу FastEthernet0/0.70, що підтримує інкапсуляцію 802.1Q для VLAN 70. Дана дія реалізується через команду `interface FastEthernet0/0.70`, де їй призначається IP-адреса 172.25.65.193 з маскою підмережі 255.255.255.192. Ця адреса виконує функцію віртуального шлюзу для телефонів, підключених до даної VLAN.

Подальшим етапом є налаштування служби DHCP, що дозволяє автоматично призначати IP-адреси VoIP-телефонам у межах пулу VOIP.POOL. Це досягається шляхом створення налаштувань, які включають шлюз за замовчуванням (172.25.65.193) та специфічну опцію 150, що вказує на IP-адресу TFTP-сервера, необхідного для отримання конфігурації телефонів. Упровадження служби DHCP знижує адміністративні витрати, оскільки спрощує процес налаштування кожного окремого пристрою.

Наступний аспект – це налаштування `telephony-service`, яке дозволяє маршрутизатору підтримувати до 30 елементів телефонії одночасно. Важливими параметрами є максимальна кількість внутрішніх номерів (max-dn) і автоматичне призначення номерів. У даному випадку маршрутизатор

використовує IP-адресу 172.25.65.193 як вихідну адресу для обробки трафіку на порту 2000. Це забезпечує ефективну маршрутизацію голосового трафіку.

Для обліку внутрішніх комунікацій на маршрутизаторі формуються номери для ephone-dn, що включають числа від 401 до 410. Кожен номер відповідає певному телефону, який ідентифікується за MAC-адресою та типом пристрою. У даному випадку використано десять IP-телефонів Cisco 7960, які налаштовуються без режиму безпеки (`device-security-mode none`), що спрощує процес первинного налаштування.

Кожному телефону призначається кнопка 1:x, яка відповідатиме його номеру. Це забезпечує простоту використання для кінцевих користувачів, оскільки доступ до голосових комунікацій стає зручним і зрозумілим.

Для підтвердження працездатності служби IP-телефонії (VoIP), яка реалізована в корпоративній мережі юридичної фірми, проведено комплексне тестування із застосуванням середовища Cisco Packet Tracer.

Після підключення IP-телефони отримали IP-адреси з DHCP-сервера. Телефони отримали унікальні номер, наприклад для LEG-VoIP1 (рис. 3.16):

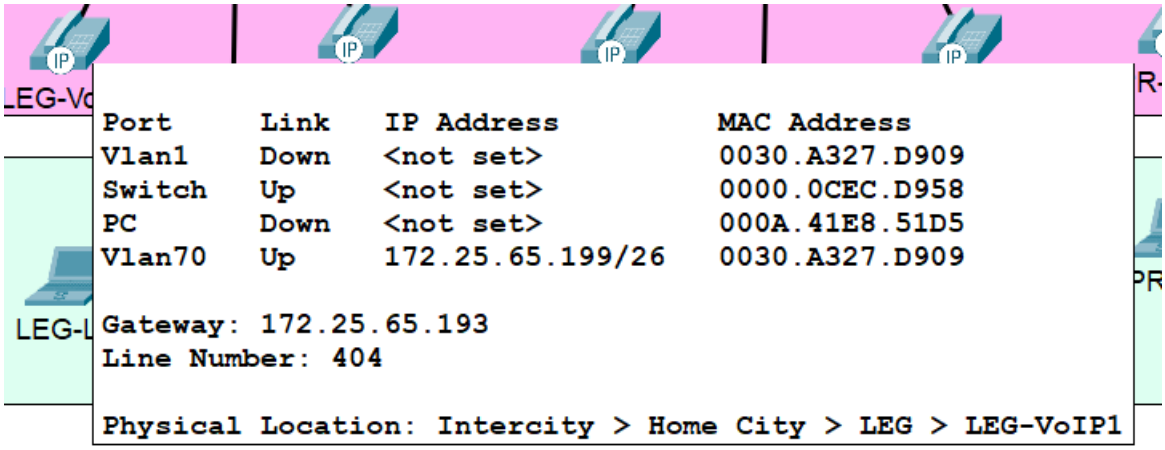

Рисунок 3.16 – Номери телефонів

На маршрутизаторі зареєстровано SIP-клієнтів (рис. 3.17)

```
Router#show ephone

ephone-1 Mac:0002.4AEC.1A88 TCP socket:[1] activeLine:0 REGISTERED in SCCP ver
12 and Server in ver 8
mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0 paging 0 debug:0 caps:8
IP:172.25.65.196 1025 7960   keepalive 43 max_line 2
 button 1: dn 1  number 401 CH1   IDLE

ephone-4 Mac:0030.A327.D909 TCP socket:[1] activeLine:0 REGISTERED in SCCP ver
12 and Server in ver 8
mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0 paging 0 debug:0 caps:8
IP:172.25.65.199 1025 7960   keepalive 43 max_line 2
 button 1: dn 4  number 404 CH1   IDLE
```

Рисунок 3.17 – На маршрутизаторі зареєстровані SIP-клієнти

На рисунку 3.18 здійснено тестування вихідних і вхідних викликів. ASS-VoIP2→ LEG-VoIP1:

– набір номера 404;

– телефон LEG-VoIP1 отримує виклик.

– після підняття слухавки встановлено двосторонній голосовий зв’язок.

Рисунок 3.18 – Перевірка викликів VoIP

3.12 Налаштування бездротової мережі

Реалізована бездротова мережа VLAN 60, яка має 4 точки доступу,

Бездротова мережа містить у собі: Radius Server, який виконує роль DHCPсерверу для безпровідної мережі, контролер бездротової мережі, за допомогою якого можна керувати та налаштовувати точки доступу (рис.3.19)

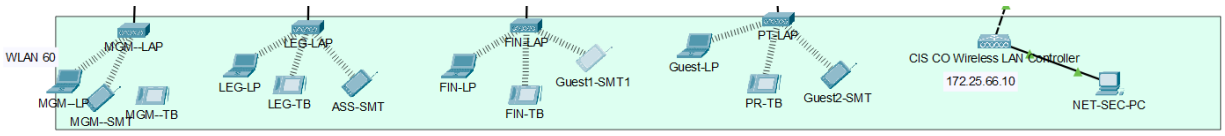

Рисунок 3.19 – Бездротова мережа

Контролер бездротової мережі має адресу 172.23.89.2, для того, щоб налаштувати бездротові точки доступу, потрібно перейти у PC_Admin → Desktop → Web Browser → Ввести адресу WLC Controller, у данному випадку 172.25.66.10 (Сайт відкривається тільки через HTTPS), після чого потрібно увійти в обліковий запис за логіном admin та паролем admin. Після успішного входу з’явиться меню налаштування контролеру бездротової мережі (рис.3.20).

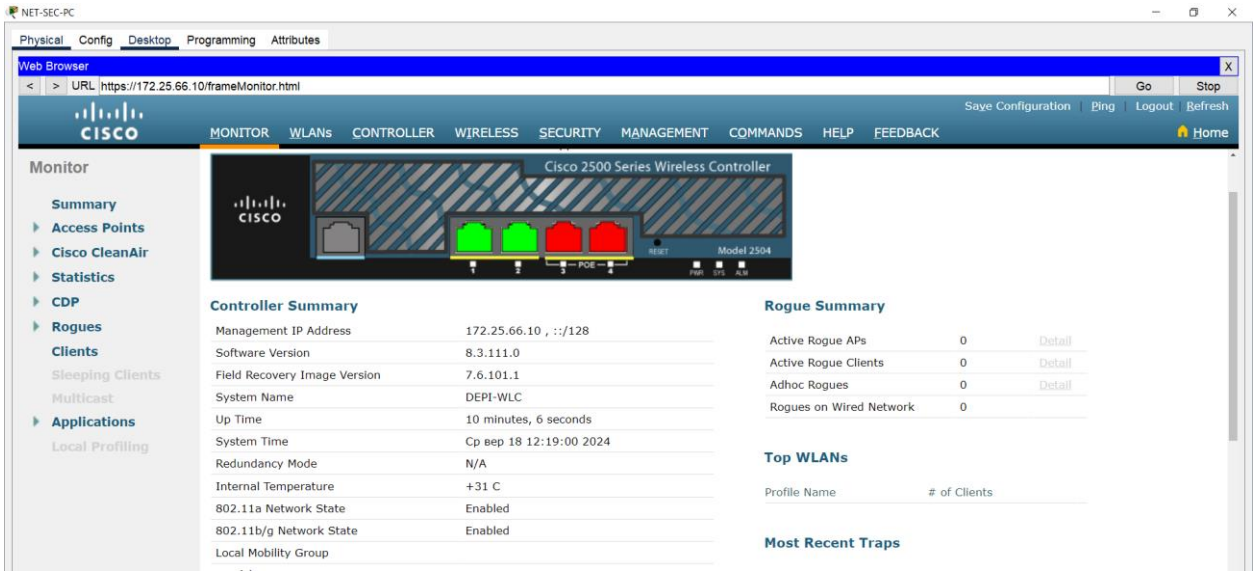

Рисунок 3.20 – Меню Wireless LAN Controller 3504

У меню відображено кількість активних та неактивних портів на контролері, активні бездротові точки доступу, службову інформацію про контролер тощо У меню відображено кількість активних та неактивних портів на контролері, активні бездротові точки доступу, службову інформацію про контролер тощо.

У вкладці WLANs (рис. 3.21) інтерфейс керування безпроводними точками доступу (AP) в мережі. У таблиці наведено інформацію про п'ять точок доступу, включаючи:

– AP Name (назва точки доступу);

– IP Address (IP-адреси);

– AP Model (модель точки доступу);

– AP MAC (MAC-адреси);

– AP Up Time (години роботи).

Одна з точок доступу має IP-адресу 0.0.0.0 і відзначена як "NA" у полі часу роботи, що може свідчити про те, що вона не активна. Інші пристрої мають IP-адреси в діапазоні 172.25.66.6 та 172.25.66.8.

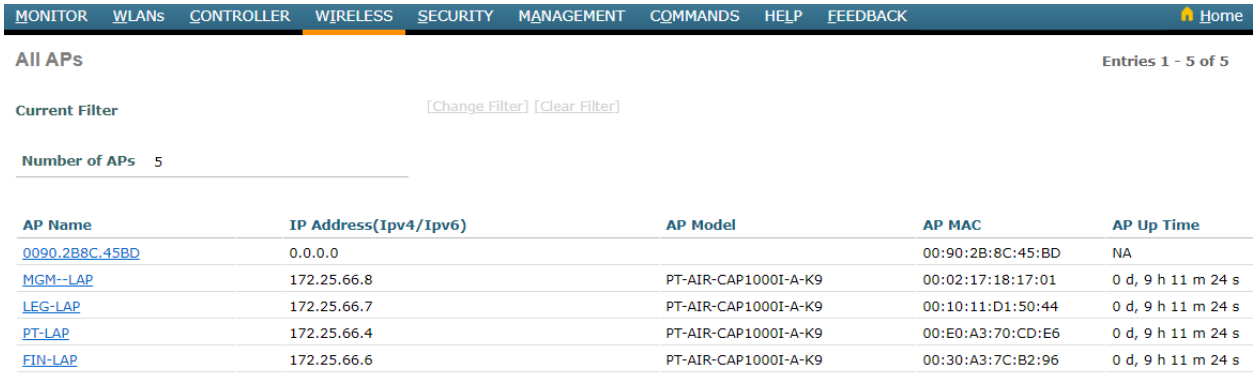

Рисунок 3.21 – Вкладка WLANs

На рисунку 3.22 представлено інтерфейс для керування безпровідними локальними мережами (WLANs). В таблиці наведено деталі чотирьох WLAN:

– WLAN ID (ідентифікатор WLAN) – унікальний номер для кожної мережі;

– Type (тип) – усі записи відзначені як WLAN;

– Profile Name (ім'я профілю) – назви профілів для кожної мережі (EMPLOYEES WIFI, LEGAL WIFI, ACCESS CONTROL SYSTEM WIFI, GUEST WIFI);

– WLAN SSID – імена мереж (SSID), які відображаються для користувачів;

– Admin Status (статус адміністратора) – всі мережі мають статус "Enabled" (увімкнено);

– Security Policies (політики безпеки) – всі мережі використовують стандарт WPA2 з автентифікацією PSK.

Це дозволяє адміністраторам ефективно управляти різними WLAN у мережі.

Рисунок 3.22 – Безпровідні локальні мережі (WLANs)

Після виконання налаштувань на контролері на прикладі точки доступу FIN-LAP (рис. 3.23) пристрій підключено до адреси 172.25.66.10, що вказує на його зв'язок з контролером через протокол CAPWAP (Control And Provisioning of Wireless Access Points). Це свідчить про централізоване управління точкою доступу, що дозволяє більш ефективно налаштовувати та моніторити мережу.

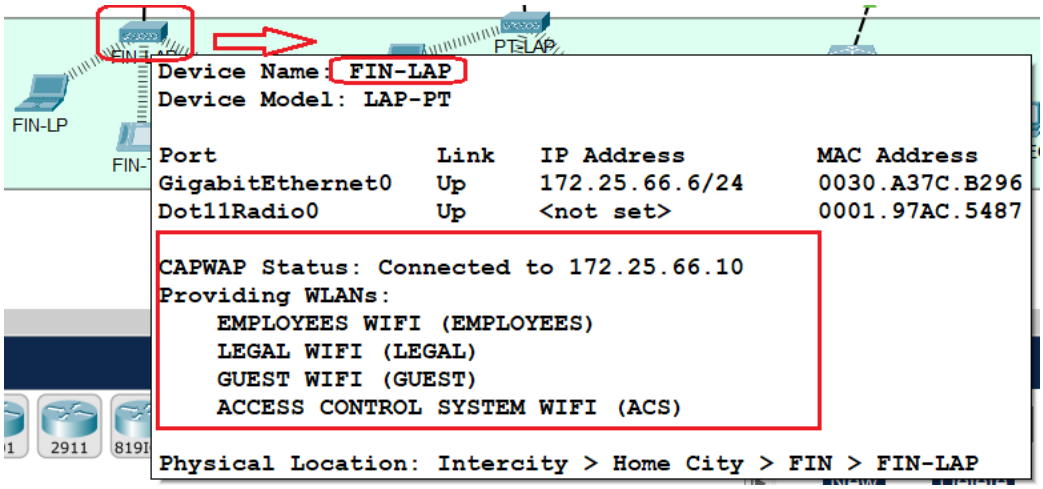

Рисунок 3.23 – Параметри пристрою FIN-LAP

FIN-LAP забезпечує кілька ідентифікованих безпровідних локальних мереж (WLANs):

– EMPLOYEES WIFI: для співробітників;

– LEGAL WIFI: мережа для юридичних цілей;

– GUEST WIFI: відкрита мережа для гостей;

– ACCESS CONTROL SYSTEM WIFI (ACS): спеціалізована мережа для систем контролю доступу.

Це свідчить про гнучкість та адаптивність точки доступу до різних потреб користувачів, що продемонстровано на рисунку 3.24 для гостьового користувача та для співробітника юридичної фірми. Конфігураційні налаштування для бездротових мереж GUEST і LEGAL демонструють чіткий розподіл функцій у мережі.

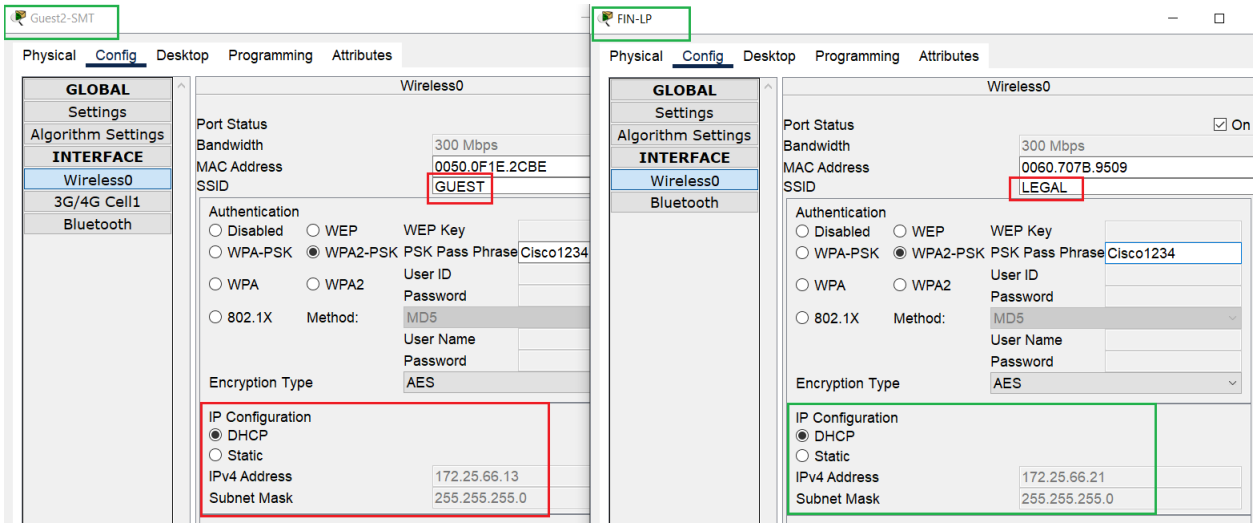

Рисунок 3.24 – Налаштування для бездротових користувачів

4 РОЗРОБКА СИСТЕМИ КОНТРОЛЮ ДОСТУПУ НА ОСНОВІ RFID-СМАРТ-КАРТ

4.1 Мета та призначення системи

Система контролю доступу (СКД) є важливою складовою безпеки комп'ютерної інфраструктури юридичної фірми. Вона дозволяє забезпечити контрольовану ідентифікацію персоналу за допомогою RFID-міток (схожих на смарт-карти) та інтегрувати фізичну безпеку із загальною IT-інфраструктурою. У даній моделі реалізовано прототип СКД, що забезпечує авторизований доступ до приміщення через обробку запитів RFID-зчитувачем, який взаємодіє із центральним IoT-сервером.

4.2 Топологія системи контролю доступу

На рисунку 4.1 представлено структурну схему моделі, що включає такі компоненти:

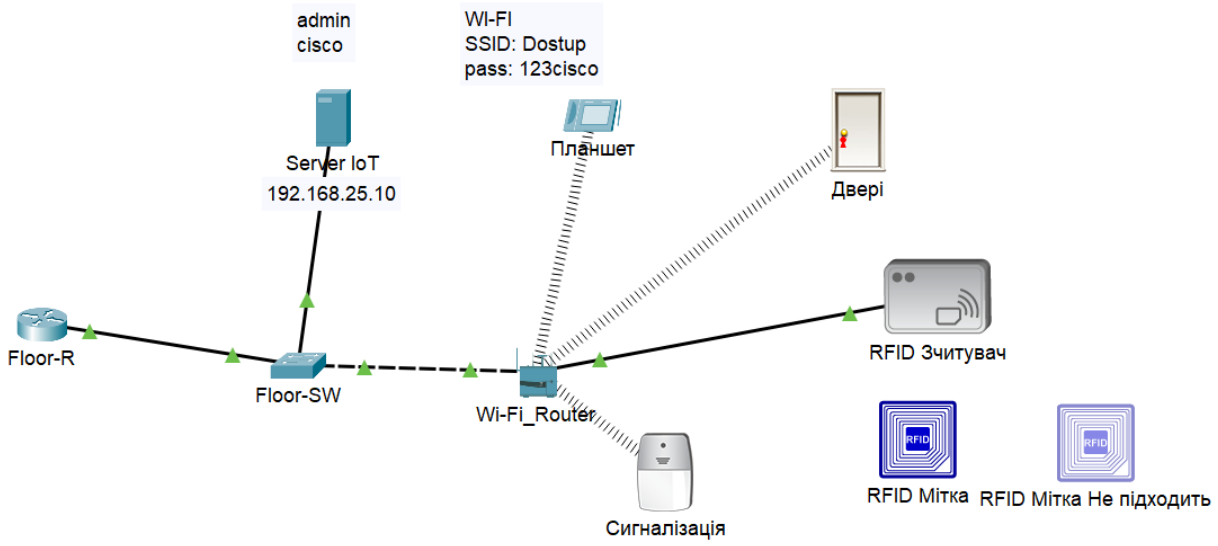

Рисунок 4.1 – Топологія системи контролю доступу

– RFID-зчитувач: виконує функцію реєстрації мітки та передає її унікальний ідентифікатор до серверу перевірки;

– двері (електромагнітний замок): під'єднані до зчитувача; відчиняються лише у разі авторизованої мітки;

– RFID-мітка: носій ідентифікаційного коду (може бути авторизованою або відхиленою);

– Wi-Fi-роутер: забезпечує бездротовий канал зв’язку між RFID-зчитувачем, планшетом і іншими IoT-пристроями;

– IoT-сервер з IP-адресою `192.168.25.10: зберігає список дозволених міток, реалізує логіку перевірки доступу, зв’язаний із сигналізацією;

– сигналізація: активується у разі спроби несанкціонованого доступу (невідповідна мітка);

– планшет: мобільний пристрій адміністратора, що може підключатися по Wi-Fi для моніторингу стану системи доступу;

– маршрутизатор Floor-R та комутатор Floor-SW: об’єднують IoT-сервер із корпоративною мережею.

Адміністратор має можливість переглядати журнали доступу через планшет по бездротовому з’єднанню (SSID: Dostup, пароль: 123cisco).

Вся передача даних здійснюється в локальній мережі з ізоляцією IoT-сегменту за допомогою VLAN та фільтрації на комутаторі.

4.3 Принцип реалізації доступу через RFID-систему

Алгоритм роботи системи наступний (рис. 4.2):

1. Користувач підносить RFID-мітку до зчитувача.

2. Зчитувач передає унікальний ID мітки до IoT-сервера.

3. IoT-сервер перевіряє ID у базі дозволених доступів:

– якщо мітка авторизована, відкриваються двері;

– якщо неавторизована, то активується сигналізація, в журналі реєструється інцидент.

На представленому зображенні показано налаштування системи доступу за допомогою RFID, що ілюструє їх інтеграцію з IoT-сервером для контролю доступу.

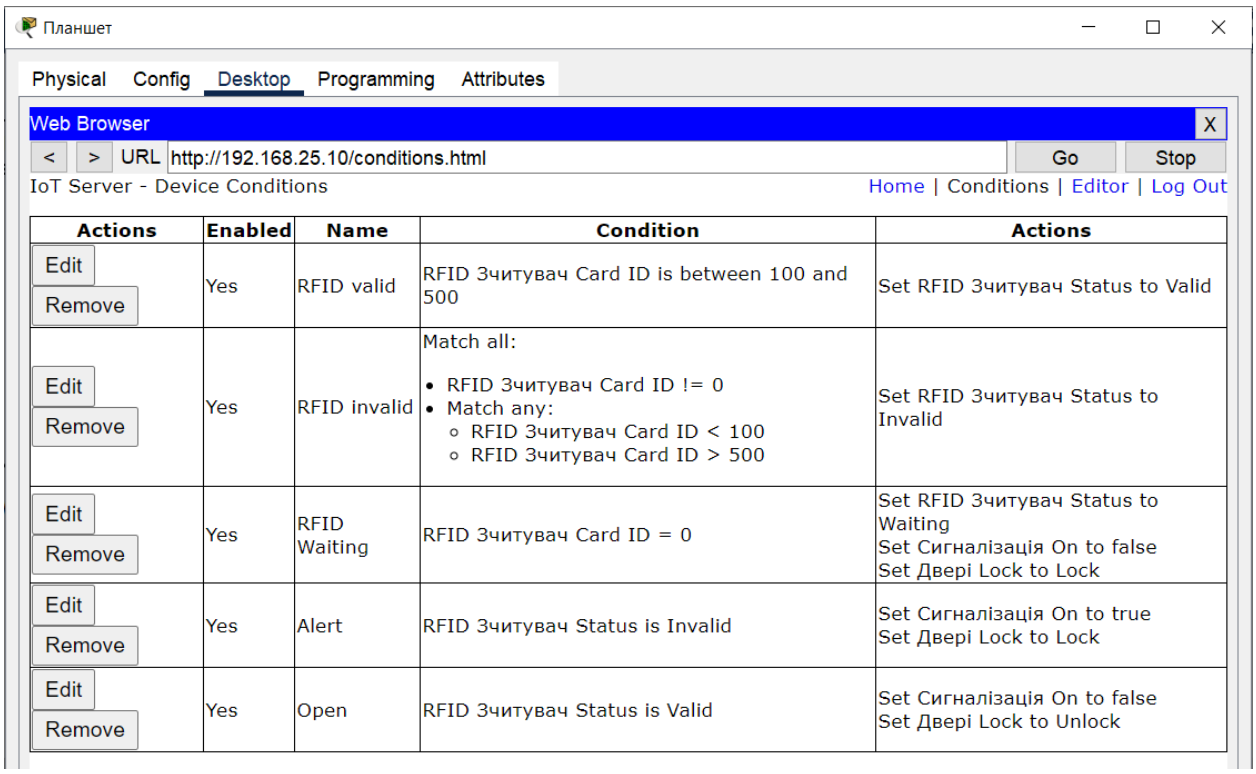

Рисунок 4.2 – Алгоритм роботи системи доступу

Система базується на використанні RFID-карт, які мають унікальні ідентифікатори. Кожен з цих ідентифікаторів проходить перевірку за певними умовами, що визначають статус доступу.

У системі реалізовані різні умови для обробки даних RFID:

– RFID valid: умова перевіряє, чи знаходиться ID картки в межах 100 і 500. Якщо так, статус картки змінюється на "Valid". Це дозволяє забезпечити доступ користувачам з дійсними картами;

– RFID invalid: Умова активується при ID картки, що не дорівнює 0 і потрапляє в діапазон менше 100 або більше 500. У цьому випадку статус картки змінюється на "Invalid", що блокує доступ;

– RFID Waiting: умова перевіряє, чи дорівнює зчитаний ID нулю. Якщо так, статус картки встановлюється на "Waiting", сигналізація вимикається, а двері блокуються;

– Alert: активується, коли статус RFID-картки вважається "Invalid". Це призводить до блокування дверей та включення сигналізації;

– Open: коли статус картки вважається "Valid", система знімає блокування з дверей і вимикає сигналізацію.

Кожна з умов виконує певні дії, які визначають доступ користувача:

– зміна статусу картки: випадки зміни статусу RFID-картки впливають на внутрішні налаштування системи доступу;

– управління сигналізацією: умикання та вимикання сигналізації забезпечує безпеку об'єкта, попереджаючи про потенційні загрози;

– блокування/розблокування дверей: керування доступом до приміщень шляхом відкриття або закриття дверей на основі статусу картки.

4.4 Перевірка роботи СКД

З метою підтвердження працездатності розробленої системи контролю доступу було проведено функціональне тестування моделі, реалізованої в середовищі Cisco Packet Tracer. Метою тестування є перевірка коректності реакції СКД на дії користувачів з RFID-мітками, а також здатності IoT-сервера до обробки запитів у реальному часі.

Тестування проводилося шляхом імітації дій користувача, що підносить RFID-мітку до зчитувача. Сценарії охоплювали:

– використання авторизованої мітки (рис. 4.3);

– використання неавторизованої мітки (рис. 4.4);

– доступ адміністратора до інформації через планшет (рис 4.5).

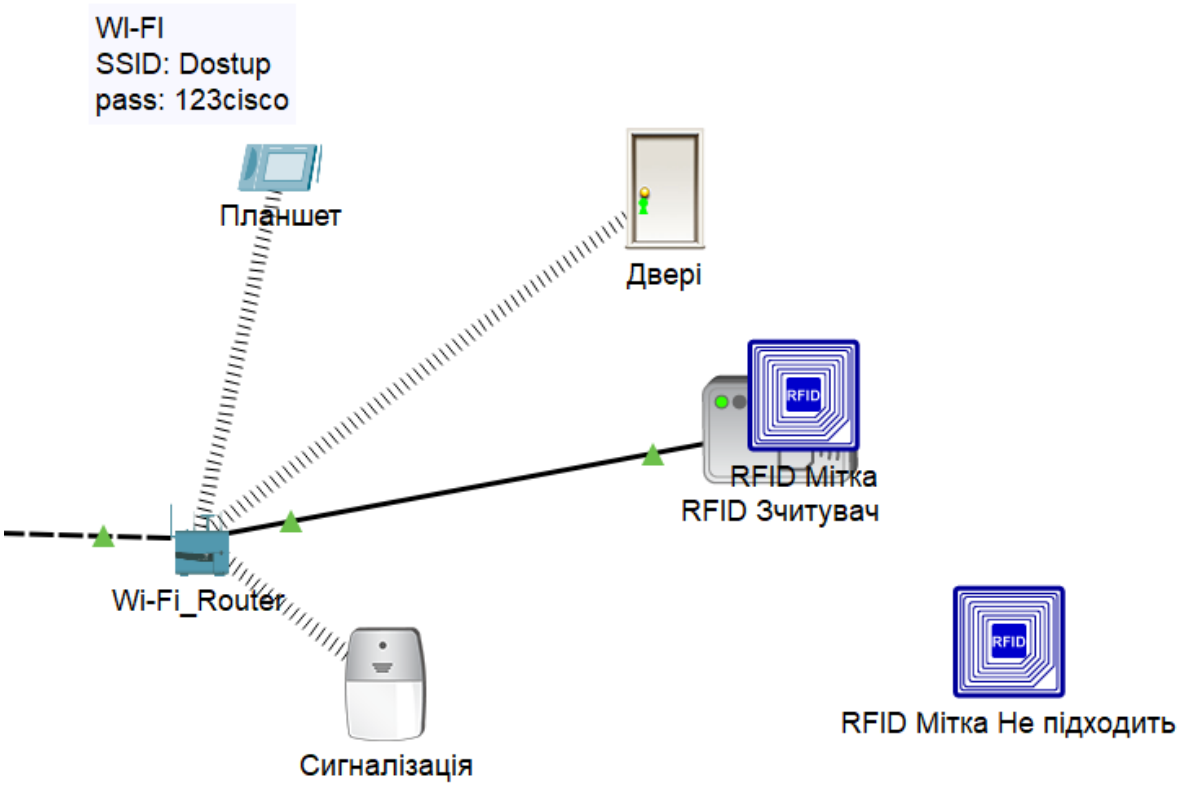

Рисунок 4.3 – Використання авторизованої мітки

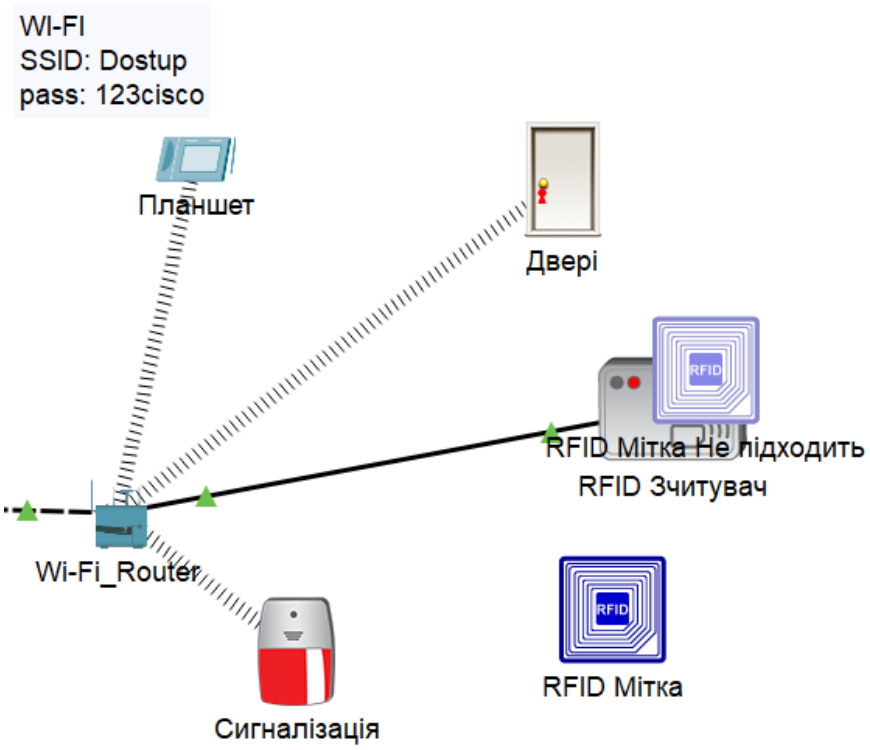

Рисунок 4.4 – Використання неавторизованої мітки

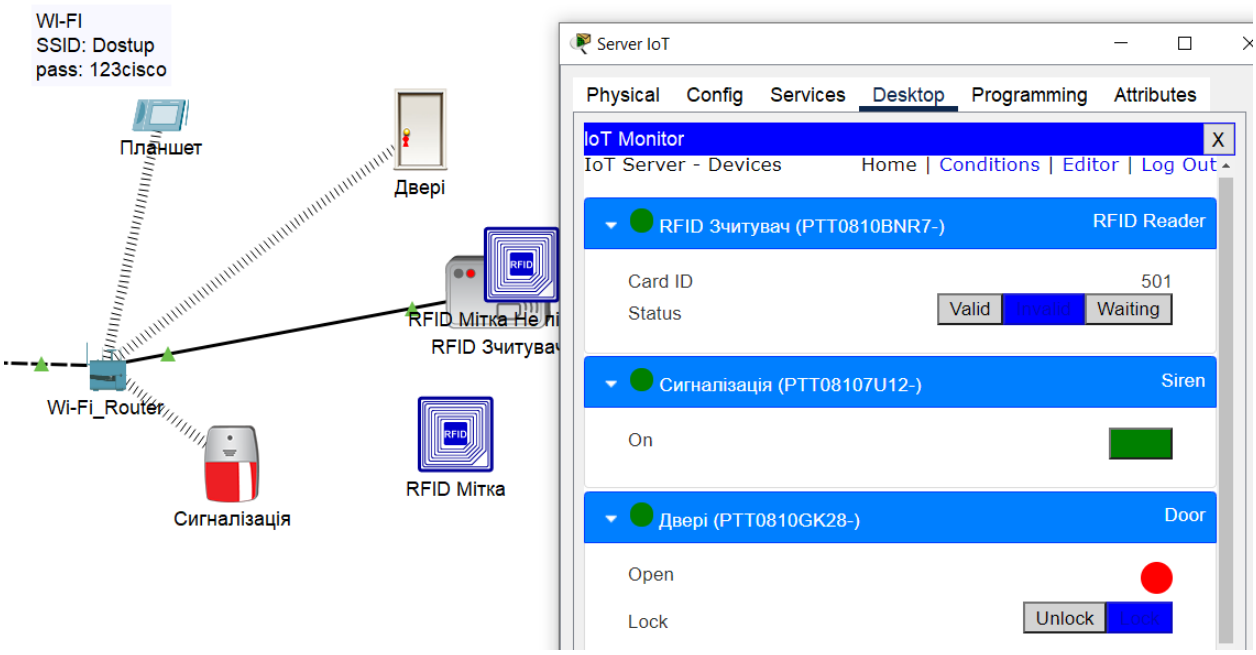

Рисунок 4.5 – Доступ адміністратора до інформації через планшет

Ця RFID-система реалізує комплексний підхід до управління доступом, ґрунтуючись на чітко визначених умовах перевірки карток та відповідних діях. Завдяки цьому, забезпечується високий рівень безпеки та контролю доступу.

Результати тестування підтверджують працездатність розробленої системи. Реалізована логіка дозволяє оперативно реагувати на спроби доступу, підтримує базову безпеку та адміністративний контроль. Система показала надійну взаємодію компонентів і може бути масштабована до рівня реальної офісної інфраструктури юридичної фірми.

ВИСНОВКИ

У рамках даної кваліфікаційної роботи було здійснено комплексна розробка та моделювання комп’ютерної системи юридичної фірми, що поєднала корпоративну мережу, серверну інфраструктуру, IP-телефонію та систему фізичного контролю доступу. Архітектура мережі вибудована за трирівневою моделлю «Core–Distribution–Access» із логічною сегментацією VLAN та механізмами резервування каналів (HSRP) та віддаленого підключення (VPN). Такий підхід забезпечує стійке функціонування служб, високу продуктивність та масштабованість інфраструктури.

Розроблена система контролю доступу на основі RFID-смарт-карт інтегрована з IoT-платформою, що дозволяє автоматично ідентифікувати співробітників на вході, блокувати або дозволяти доступ до критичних зон і вести централізовані журнали подій.

Експериментальна перевірка в середовищі Cisco Packet Tracer підтвердила коректність обраних рішень: динамічна маршрутизація OSPF, механізми захисту (ACL, PortFast, BPDU Guard), якість VoIP-зв’язку та відмовостійкість мережі працюють згідно з технічними вимогами. Запропоноване рішення може бути адаптоване для реального впровадження в юридичних організаціях різного масштабу, що підвищить рівень їх інформаційної безпеки та ефективності бізнес-процесів.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Законодавча реформа в Україні: тенденції та перспективи. [Електронний ресурс]. – URL: https://www.legislation.gov.ua/ (дата звернення: 05.05.2025).

2. ДСТУ ISO/IEC 27001:2015. Інформаційні технології. Методи забезпечення безпеки. Системи управління інформаційною безпекою. Вимоги. – [Чинний від 01.09.2016]. – К. : ДП «УкрНДНЦ», 2016. – 40 с.

3. Про захист персональних даних. Офіційний вебпортал парламенту України. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 05.06.2025).

4. О.В. Співаковський, М.І. Шерман, В.М. Стратонов, В.В. Лапінський Інформаційні технології в юридичній діяльності: базовий курс: [навчальний посібник]. – Херсон: ХДУ, 2012. – 220 с.

5. Cisco Systems. Cisco Smart Business Architecture – Foundation Design Guide. – Cisco Press, 2020. – 214 с.

6. Cisco Networking Academy. Протокол IPv4 та основи маршрутизації в корпоративних мережах. Навчальний курс CCNA. – Cisco, 2022. – [Електронний ресурс]. – URL: https://www.netacad.com (дата звернення: 15.04.2025).

7. Столяр С. В., Мазур О. І. Мережеві технології та протоколи TCP/IP. – Київ : КНУ, 2021. – 215 с.

8. Cisco Networking Academy. RFID Access Control with Alarm and Door in Packet Tracer : tutorial [Електронний ресурс]. – Cisco Skills For All, 2023. – Режим доступу: https://skillsforall.com/course/iot-rfid-access-control

9. Шевчук Ю. О. Проектування локальних обчислювальних мереж для малого бізнесу : навч. посіб. – Харків : ХНУРЕ, 2021. – 142 с.

10. Packet Tracer 8.2 - HSRP Configuration - Packet Tracer Network. Packet Tracer Network. URL: https://www.packettracernetwork.com/tutorials/hsrp-configuration-new.html (date of access: 05.06.2025).

11. Anthony Lucas. Packet Tracer 9.3.3 - HSRP Configuration Guide, 2021. YouTube. URL: https://www.youtube.com/watch?v=-5KCxihML2w (date of access: 05.06.2025).

12. Gurutech Networking Training. How to Configure VoIP Phones in Cisco Packet Tracer | Configure IP Phones Telephony Service, 2022. YouTube. URL: https://www.youtube.com/watch?v=UrzKYKi8NEM (date of access: 05.06.2025).

Додаток А

Тексти програм налаштувань мережного обладнання

ЗМІСТ

1. Базові налаштування безпеки та SSH

1. Basic Settings to all devices plus SSH on the Routers AND L3 Switches

```
ena
conf t
hostname DMZ-SW

line console 0
password cisco
login
logging synchronous
exec-timeout 3 0
exit

enable password cisco
banner motd &

Name: Motornyi OM
Group: 123-21-2
project: Law firm computer system with detailed development of
corporate network construction and configuration

password: cisco
&
no ip domain-lookup

service password-encryption

username cisco password cisco
ip domain-name itki.com

crypto key generate rsa general-keys modulus 1024
ip ssh version 2

line vty 0 15
login local
transport input ssh
exit

access-list 1 permit 192.168.10.0 0.0.0.255
access-list 1 deny any

line vty 0 15
```

```
access-class 1 in
exit

do wr
```

1. Сегментація мережі VLAN

```
############################## MK-SW, HR-SW, FINANCE-SW,
ADMIN-SW, ICT-SW#########################################
int range fa0/1-2
switchport mode trunk
exit

vlan 10
name MGT
VLAN 20
NAME LAN
VLAN 50
NAME WLAN
VLAN 70
NAME VoIP
VLAN 199
NAME Blachole
exit

int range fa0/3-4
switchport mode access
switchport access vlan 20
exit

int range fa0/5-6
switchport mode access
switchport access vlan 70
exit

int range fa0/7
switchport mode access
switchport access vlan 50
exit

do wr
```

```
############################## SERVER-SW
########################################
int range fa0/1-2, fa0/7
switchport mode trunk
exit

vlan 10
name MGT
VLAN 20
NAME LAN
VLAN 50
NAME WLAN
VLAN 70
NAME VoIP
VLAN 90
NAME INSIDE-SERVERS
exit

int range fa0/3-5
switchport mode access
switchport access vlan 90
exit

int fa0/6
switchport mode access
switchport access vlan 50
exit

do wr

############################## MLT1 & MLT2
########################################
int range gig1/0/3-8
switchport mode trunk
exit

vlan 10
name MGT
VLAN 20
NAME LAN
VLAN 50
NAME WLAN
```

```
VLAN 70
NAME VoIP
VLAN 90
NAME INSIDE-SERVERS
exit

do wr
################################## modification
########################################
INT range fa0/5-6
no switchport access vlan 70
switchport voice vlan 70
exit
do wr
```

2. HSRP та Inter-VLAN

```
MLT-SW1
**************************************************

interface Vlan10
 ip address 172.25.64.2 255.255.255.128
 ip helper-address 172.25.67.12
 standby 10 ip 172.25.64.1
!
interface Vlan20
 ip address 172.25.64.130 255.255.255.128
 ip helper-address 172.25.67.12
 standby 20 ip 172.25.64.129
!
interface Vlan30
 ip address 172.25.65.2 255.255.255.192
 ip helper-address 172.25.67.12
 standby 30 ip 172.25.65.1
!
interface Vlan40
 ip address 172.25.65.66 255.255.255.192
 ip helper-address 172.25.67.12
 standby 40 ip 172.25.65.65
!
interface Vlan50
 ip address 172.25.65.130 255.255.255.192
```

```
 ip helper-address 172.25.67.12
 standby 50 ip 172.25.65.129
!
interface Vlan60
 ip address 172.25.66.2 255.255.255.0
 ip helper-address 172.25.67.12
 standby 60 ip 172.25.66.1
!
interface Vlan70
 ip address 172.25.65.194 255.255.255.192
 ip helper-address 172.25.67.12
 standby 50 ip 172.25.65.193
!
interface Vlan90
 ip address 172.25.67.2 255.255.255.0
 standby 90 ip 172.25.67.1
**************************************************
MLT-SW2
**************************************************

interface Vlan10
 ip address 172.25.64.3 255.255.255.128
 ip helper-address 172.25.67.12
 standby 10 ip 172.25.64.1
!
interface Vlan20
 ip address 172.25.64.131 255.255.255.128
 ip helper-address 172.25.67.12
 standby 20 ip 172.25.64.129
!
interface Vlan30
 ip address 172.25.65.3 255.255.255.192
 ip helper-address 172.25.67.12
 standby 30 ip 172.25.65.1
!
interface Vlan40
 ip address 172.25.65.67 255.255.255.192
 ip helper-address 172.25.67.12
 standby 40 ip 172.25.65.65
!
interface Vlan50
 ip address 172.25.65.131 255.255.255.192
```

```
 ip helper-address 172.25.67.12
 standby 50 ip 172.25.65.129
!
interface Vlan60
 ip address 172.25.66.3 255.255.255.0
 ip helper-address 172.25.67.12
 standby 60 ip 172.25.66.1
!
interface Vlan70
 ip address 172.25.65.195 255.255.255.192
 ip helper-address 172.25.67.12
 standby 50 ip 172.25.65.193
!
interface Vlan90
 ip address 172.25.67.3 255.255.255.0
 standby 90 ip 172.25.67.1
```

3. **Налаштування** механізмів захисту рівня доступу

```
FOR SERVERROOM SWITCH
**********************

INT range FA0/3-6, FA0/8-24
spanning-tree portfast
spanning-tree bpduguard enable
ex
do wr

********************
for all switches
********************
INT range FA0/3-24
spanning-tree portfast
spanning-tree bpduguard enable
ex
do wr

******************
DMZ
******************

INT range FA0/1-24
```

```
spanning-tree portfast
spanning-tree bpduguard enable
ex
do wr
```

4. Конфігурація агрегованого каналу

```
MLT1
**********
interface range gig1/0/9-11
channel-group 1 mode active
ex
interface port-channel 1
switchport mode trunk
ex
do wr

MLT2
**********
interface range gig1/0/9-11
channel-group 1 mode passive
ex
interface port-channel 1
switchport mode trunk
ex
do wr
```

5. Конфігурація VoIP

```
voip configuration
****************************************

config t
int f0/0
no shut
interface FastEthernet0/0.70
 encapsulation dot1Q 70
 ip address 172.25.65.193 255.255.255.192

service dhcp
ip dhcp pool VOIP.POOL
 network 172.25.65.192 255.255.255.192
 default-router 172.25.65.193
```

```
 option 150 ip 172.25.65.193
ex

telephony-service
 max-ephones 30
 max-dn 30
 ip source-address 172.25.65.193 port 2000
 auto assign 1 to 30

ephone-dn 1
 number 401
!
ephone-dn 2
 number 402
!
ephone-dn 3
 number 403
!
ephone-dn 4
 number 404
!
ephone-dn 5
 number 405
!
ephone-dn 6
 number 406
!
ephone-dn 7
 number 407

ephone-dn 8
 number 408
!
ephone-dn 9
 number 409
!
ephone-dn 10
 number 410
!
ephone 1
 device-security-mode none
 mac-address 0002.4AEC.1A88
```

```
 type 7960
 button 1:1
!
ephone 2
 device-security-mode none
 mac-address 00D0.D3CC.4940
 type 7960
 button 1:2
!
ephone 3
 device-security-mode none
 mac-address 0090.2B7B.040A
 type 7960
 button 1:3
!
ephone 4
 device-security-mode none
 mac-address 0030.A327.D909
 type 7960
 button 1:4
!
ephone 5
 device-security-mode none
 mac-address 00E0.B056.970A
 type 7960
 button 1:5
!
ephone 6
 device-security-mode none
 mac-address 00E0.F7ED.DAA9
 type 7960
 button 1:6
!
ephone 7
 device-security-mode none
 mac-address 00E0.F725.8C7A
 type 7960
 button 1:7
!
ephone 8
 device-security-mode none
 mac-address 0090.2190.DDD0
```

```
 type 7960
 button 1:8
!
ephone 9
 device-security-mode none
 mac-address 0060.3E26.5002
 type 7960
 button 1:9
!
ephone 10
 device-security-mode none
 mac-address 0060.7004.0D27
 type 7960
 button 1:10
```