Хмельницький національний університет
Факультет інформаційних технологій
Кафедра комп'ютерної інженерії та інформаційних систем

КВАЛІФІКАЦІЙНА РОБОТА

бакалавр
Освітній рівень

Комп'ютерна мережа магазину з розмежуванням доступу
Назва теми

КвРКІ 210115.21.01.54 ПЗ
Шифр

Галузь знань *12 «Інформаційні технології»*
Шифр, назва

Спеціальність *123 «Комп'ютерна інженерія»*
Шифр, назва

Освітня програма *«Комп'ютерна інженерія та програмування»*
Назва

Виконав: студент IV курсу, група КІ2-21-1 _____ Інна КУЗЬМІНСЬКА
Підпис, Ініціали, прізвище

Керівник _____ Марія КАПУСТЯН
Підпис, дата, Ініціали, прізвище

Нормоконтролер _____ Тетяна КИСІЛЬ
Підпис, дата, Ініціали, прізвище

До захисту допускаю:
зав. кафедри комп'ютерної інженерії та інформаційних систем _____ Ольга ПАВЛОВА
Підпис, Ініціали, прізвище

«16» червня 2025 р.

Хмельницький 2025

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій

Кафедра Комп'ютерної інженерії та інформаційних систем

Освітній рівень бакалавр

Галузь знань 12 Інформаційні технології

Спеціальність 123 Комп'ютерна інженерія

Освітня програма «Комп'ютерна інженерія та програмування»

ЗАТВЕРДЖУЮ

Зав. кафедри Ольга ПАВЛОВА

" 10 " 01 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ БАКАЛАВРА

Інні КУЗЬМІНСЬКІЙ

Прізвище, ім'я, по батькові студента

1. Тема проекту (роботи) Комп'ютерна мережа магазину з розмежуванням доступу

Керівник проекту (роботи) Марія КАПУСТЯН, к.т.н, доцент.

Прізвище, ім'я, по батькові, науковий ступінь, вчене звання

Затверджена наказом ректора університету від 07.02.2025 р. № 23

2. Строк подання студентом проекту (роботи) на кафедру 01.06.2025 р.

3. Вихідні дані до проекту (роботи) Завдання на кваліфікаційну роботу

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити)

Теоретичні основи досліджуваної проблеми

Проєктування комп'ютерної мережі магазину

Практична розробка комп'ютерної мережі

5. Перелік графічного матеріалу (із зазначенням обов'язкових креслень)

Структурна схема мережі

Функціональна схема локальної мережі

Карта комп'ютерної мережі

№ рядка	формат	Позначення	Найменування	Кіл. листів	№ екз	Примітка
			Текстові документи			
1		КРКІ.210115.21.01.54 ПЗ	Пояснювальна записка	55		
			Графічні матеріали			
2		КРКІ.210115.21.01.54 Е8	Структурна схема мережі	1		
			локальної мережі			
3		КРКІ.210115.21.01.54 Е8	Функціональна схема	1		
			локальної мережі			
4		КРКІ.210115.21.01.54 Е8	Карта комп'ютерної мережі	1		

КРКІ.210115.21.01.54 ВП

Зм	Арк	№ докум	Підпис	Дата	Відомість проекту	Літера	Аркуш	Аркушів
Розробив		Кузьмінська				У	1	1
Перевір.		Капустян						
						ХНУ, КІ2-21-1		
Н. контр.		Кисіль		16.06.25				
Затв.		Павлова		16.06.25				

№ рядка	формат	Позначення	Найменування	Кіл. листів	№ екз	Примітка
			Текстові документи			
1		КРКІ.210115.21.01.54 ПЗ	Пояснювальна записка	55		
			Графічні матеріали			
2		КРКІ.210115.21.01.54 Е8	Структурна схема мережі	1		
			локальної мережі			
3		КРКІ.210115.21.01.54 Е8	Функціональна схема	1		
			локальної мережі			
4		КРКІ.210115.21.01.54 Е8	Карта комп'ютерної мережі	1		

Зм	Арк	№ докум	Підпис	Дата	КРКІ.210115.21.01.54 ВП			
Розробив		Кузьмінська			Відомість проекту	Літера	Аркуш	Аркушів
Перевір.		Капустян				У	1	1
						ХНУ, КІ2-21-1		
Н. контр.		Кисіль		16.06.25				
Затв.		Павлова		16.06.25				

АНОТАЦІЯ

Тема кваліфікаційної роботи: «Комп'ютерна мережа магазину з розмежуванням доступу».

Автор роботи: Інна КУЗЬМІНСЬКА.

Керівник роботи: Марія КАПУСТЯН.

Пояснювальна записка: 55 с., 26 рис., 2 табл., 3 дод., 50 джерел.

Графічна частина: 3 креслення.

КОМП'ЮТЕРНА МЕРЕЖА, БЕЗПЕКА МЕРЕЖІ, ІНФРАСТУКТУРА.

Метою дипломної роботи є визначення умов та особливостей побудови локальної комп'ютерної мережі для магазину, а також оцінка технічних рішень щодо структури, конфігурації та безпеки мережі з урахуванням сучасних вимог до надійності, швидкості обміну даними та масштабованості.Об'єктом дослідження є інфраструктура комп'ютерної мережі магазину.

Предметом дослідження є технічні рішення, архітектурні моделі, топології та протоколи, які використовуються під час проектування та впровадження локальної комп'ютерної мережі в комерційних структурах.

Під час проведення дослідження були використані методи систематичного аналізу літературних джерел, технічної документації та галузевих стандартів у сфері телекомунікацій і комп'ютерних мереж.

Підпис студента

30.05.2025

Дата

ЗМІСТ

ВСТУП

У сучасних умовах цифрової трансформації бізнесу ефективність роботи будь-якого комерційного підприємства значною мірою залежить від надійної та функціональної комп’ютерної мережі. Магазини, як елемент торгівельної інфраструктури, все частіше впроваджують електронні системи обліку, автоматизовані касові комплекси, системи відеоспостереження, CRM-платформи та хмарні сервіси. Усі ці рішення базуються на використанні стабільної локальної мережі, яка забезпечує оперативну обробку інформації, централізоване управління ресурсами та швидкий доступ до даних як для працівників, так і для керівництва.

Проєктування локальної мережі магазину вимагає врахування ряду факторів: кількість робочих місць, особливості планування приміщення, типи та обсяги трафіку, потреба в бездротовому доступі, резервуванні каналів зв’язку та забезпеченні захисту від несанкціонованого доступу. З огляду на це, актуальним є використання спеціалізованих інструментів для віртуального моделювання, таких як Cisco Packet Tracer, які дозволяють не лише проєктувати мережу, а й візуалізувати її функціонування до етапу фізичного впровадження.

Актуальність даної роботи обумовлена потребою малого і середнього бізнесу у доступних та ефективних рішеннях для побудови локальної інфраструктури з урахуванням перспективи масштабування та захисту даних. Проєктування комп’ютерної мережі дозволяє зменшити витрати на обслуговування IT-систем, оптимізувати внутрішні процеси та підвищити рівень обслуговування клієнтів.

Метою дипломної роботи є розробка оптимальної структури комп’ютерної мережі магазину з використанням сучасного мережевого обладнання та програмного забезпечення, включаючи її функціональне тестування в середовищі Cisco Packet Tracer. У межах дослідження виконано аналіз вимог до мережевої інфраструктури магазину, розглянуто варіанти топологій та архітектурних рішень, здійснено моделювання мережі, оцінено її працездатність і розроблено рекомендації щодо впровадження.

1 ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖУВАНОЇ ПРОБЛЕМ

Огляд предметної сфери, проблематики та ключових завдань

Метою цього дослідження є оцінка технічного стану комп'ютерної мережі магазину, ідентифікація поточних проблем, а також створення рекомендацій для підвищення ефективності її функціонування, що в свою чергу сприятиме оптимізації роботи магазину.

Для досягнення поставленої мети потрібно виконати такі завдання.

Необхідно провести аналіз структури та функціональних можливостей комп'ютерної мережі магазину, що дозволить оцінити її ефективність та виявити потенційні проблеми. Важливим етапом є визначення вузьких місць мережі, що можуть негативно впливати на операційну діяльність магазину, з подальшою оцінкою їхнього впливу на загальну продуктивність. Також слід ознайомитися з існуючими мережевими технологіями, провести порівняння їхніх переваг і недоліків, щоб вибрати оптимальні варіанти для реалізації. Окрім того, на основі отриманих даних буде розроблено комплекс рекомендацій щодо необхідного обладнання та програмного забезпечення, що дозволить створити ефективну комп'ютерну мережу для магазину.

Насамперед потрібно детально дослідити архітектуру комп'ютерної мережі магазину, враховуючи її технічні характеристики, мінімальні вимоги до обладнання, тип застосовуваної мережі та програмне забезпечення для її адміністрування.

За результатами аналізу визначається модель інформаційної мережі, яка повинна відповідати критеріям високої продуктивності, надійності та інформаційної безпеки. Основною метою даного проєкту є розробка технічних специфікацій для побудови мережевої інфраструктури магазину, включаючи проєктування її архітектури, вибір оптимального мережевого обладнання, налаштування необхідних мережевих сервісів та реалізацію комплексної системи захисту даних.

За підсумками роботи буде представлений повноцінний проєкт мережевої інфраструктури магазину, впровадження якого дозволить покращити ефективність взаємодії внутрішніх процесів підприємства та забезпечить високий рівень інформаційної безпеки. Це, у свою чергу, позитивно вплине на стабільність роботи бізнесу та його загальну результативність.

1.2 Історичні аспекти становлення та еволюції комп’ютерних мереж

Виникнення комп'ютерних мереж відбулося у відповідь на необхідність обміну інформацією між комп'ютерами, що працюють в одній локалізованій мережі або на відстані. Ідея з'єднання різних комп'ютерів для обміну даними була розроблена ще в середині 20-го століття. Перші комп'ютерні мережі були обмежені по функціональності, але вже тоді з'явилася основа для подальшого розвитку технологій. У 1960-х роках була створена ARPANET, що стала попередником сучасного Інтернету. Ця мережа дозволяла з'єднувати комп'ютери через телефонні лінії для обміну даними. Завдяки своїй здатності до комунікації через різні маршрути ARPANET стала основною системою для обміну науковою інформацією[1].

Пізніше ARPANET була вдосконалена, і в 1983 році було введено протокол TCP/IP, який дозволяв з'єднувати комп'ютери з різних мереж. Цей протокол став основою для створення Інтернету, оскільки забезпечував спільний стандарт для з'єднання різних систем. Вже на початку 1990-х років Інтернет став доступним не тільки для науковців і військових, а й для широкої аудиторії, що дозволило йому стати основною платформою для обміну інформацією на глобальному рівні.

У 1991 році було вперше представлено World Wide Web (WWW), що дозволило перетворити Інтернет на систему для перегляду та доступу до інформації через браузери[2]. Це стало великою революцією, яка значно спростила доступ до даних. Поява веб-сайтів призвела до стрімкого розвитку електронної комерції, пошукових систем, соціальних мереж та інших онлайн-сервісів. Інтернет став

надзвичайно популярним, і в кінці 90-х років уже мільйони людей користувалися ним для навчання, роботи та комунікації.

В середині 2000-х років відбулася значна трансформація технологій зв'язку завдяки розвитку Wi-Fi. Це дозволило зменшити залежність від проводів і значно спростило підключення до мережі. В результаті Wi-Fi став стандартом для домашніх та офісних комп'ютерних мереж, а також для мобільних пристроїв, таких як смартфони та планшети. Мобільний доступ до Інтернету став доступним для більшої кількості людей, що призвело до росту популярності мобільних додатків і послуг.

Розвиток мобільних технологій призвів до появи 3G і 4G мереж, що забезпечили високу швидкість передачі даних для мобільних пристроїв. Це дозволило здійснювати стрімінг відео, завантаження великих файлів і забезпечити безперебійний доступ до Інтернету з будь-якого місця. Мобільні мережі стали основою для розвитку таких технологій, як Інтернет речей (IoT), що дозволяє підключати до Інтернету різноманітні пристрої, такі як побутова техніка, автомобілі та сенсори.

В середині 2010-х років почали розвиватися 5G мережі, які обіцяють ще більш швидкий доступ до Інтернету з низьким рівнем затримки. 5G дозволяє підключати мільярди пристроїв в реальному часі, що стане основою для розвитку розумних міст, автономних автомобілів і нових форм промислового виробництва [3]. Завдяки 5G також значно покращується якість мобільного відео, а також зростає можливість для розвитку технологій віртуальної і доповненої реальності.

У той же час з'явилися нові стандарти для локальних мереж (LAN), зокрема Ethernet, який став основним протоколом для з'єднання комп'ютерів в межах одного офісу або будівлі. Протягом кількох десятиліть Ethernet постійно вдосконалювався, збільшуючи швидкість передачі даних з 10 Мбіт/с до 100 Гбіт/с. Це дозволяє створювати високопродуктивні мережі для великих компаній, наукових установ і дата-центрів.

Однією з основних проблем, яка виникає з розвитком мереж, є безпека даних. Оскільки все більше інформації зберігається в електронному вигляді, зростає і кількість спроб несанкціонованого доступу до неї. Захист даних став одним із найважливіших завдань для мережевих інженерів, що призвело до розвитку таких технологій, як шифрування, VPN і брандмауери (файєрволи). Це дозволило забезпечити безпечний обмін інформацією, навіть через публічні мережі.

У другій половині 2000-х років почався розвиток хмарних технологій, що дозволили зберігати дані не на локальних комп'ютерах, а на віддалених серверах, до яких можна отримати доступ через Інтернет.. Хмарні технології стали основою для розвитку таких сервісів, як Google Drive, Dropbox і Microsoft OneDrive.

Разом з розвитком технологій комп'ютерних мереж виникли нові стандарти для забезпечення якості сервісу (QoS) і інтернет-трафіку[4]. Це дозволяє визначати пріоритети для різних видів даних, що особливо важливо для стрімінгових послуг, відеоконференцій та інших ресурсомістких сервісів. QoS дозволяє гарантувати високоякісне підключення і мінімальні затримки для критичних додатків.

Зараз ми спостерігаємо нову хвилю розвитку мобільних мереж та бездротових технологій. Однією з ключових інновацій є IoT, де комп'ютерні мережі дозволяють інтегрувати різноманітні пристрої, що взаємодіють між собою в реальному часі. Це відкриває нові можливості для автоматизації, моніторингу і управління в різних сферах життя.

Паралельно з мобільними мережами активно розвиваються оптоволоконні мережі, що дозволяють досягати надзвичайно високих швидкостей передачі даних. Це дає можливість розширити можливості для обробки великих обсягів інформації та підтримки нових інноваційних технологій.

Комп'ютерні мережі також стали основою для розвитку нових технологій, таких як штучний інтелект (ШІ) і машинне навчання. Ці технології використовують великі обсяги даних, що зберігаються в хмарних платформах, і для їх ефективної роботи необхідні швидкі і надійні мережі. Комп’ютерною мережею є система з’єднаних між собою комп’ютерів та/або іншого обладнання (серверів, комутаторів, маршрутизаторів тощо) для обміну даними. Для передавання

інформації використовуються різні середовища, як електричні сигнали по кабелях, оптичні сигнали по волокну або бездротове радіовипромінювання. Мережа може об’єднувати різні вузли - окремі пристрої, кожен з яких оснащено мережевим адаптером для взаємодії. Основні компоненти будь-якої локальної мережі включають:

Кінцеві пристрої (клієнти) включають комп’ютери, робочі станції, ноутбуки, принтери, IP-телефони та інші пристрої, які безпосередньо використовують користувачі. Кінцеві або клієнтські пристрої є джерелами і споживачами інформації в мережі.

Сервери, до яких належать високопродуктивні комп’ютери або спеціалізовані пристрої, що надають послуги та ресурси іншим вузлам мережі. Сервери можуть виконувати роль файлового сховища, бази даних, веб-сервера.

Канал передачі даних - середовище, через яке відбувається обмін даними між вузлами. Розрізняють дротове середовище (кабелі витої пари, коаксіальний кабель, оптоволокно) та бездротове (радіоканали Wi-Fi, мобільний зв’язок, Bluetooth тощо). У дротових мережах найпоширенішим є кабель «вита пара» категорії 5e/6 для Ethernet, що забезпечує швидкості до 1 Гбіт/с і вище на відстанях до ~100 м[5]. В оптичних мережах використовуються волоконно-оптичні кабелі для передавання на великі відстані і високих швидкостях. Бездротове середовище застосовується для мобільності та зручності підключення, але чутливе до завад і має обмежену зону покриття.

Мережеве обладнання (комунікаційні пристрої) - спеціалізовані пристрої, що забезпечують з’єднання сегментів мережі та управління трафіком. До них належать комутатори, маршрутизатори, точки бездротового доступу, концентратори, модеми, тощо. Мережеве обладнання необхідне для функціонування комп’ютерної мережі. Серед комунікаційних пристроїв виділяють активне обладнання (яке виконує інтелектуальну обробку трафіку - комутатори, маршрутизатори, точки доступу, мережеві адаптери) та пасивне обладнання (яке лише передає сигнал без «розумної» обробки - кабелі, роз’єми, патч-панелі, а також концентратори та повторювачі).

Програмне забезпечення мережі - це системне та прикладне ПЗ, що забезпечує роботу мережі на різних рівнях. До нього належать: операційні системи з мережевими функціями (наприклад, мережеві ОС Windows Server, Linux), програмні реалізації мережевих протоколів (TCP/IP стек, служби DNS, DHCP), засоби мережевого управління та моніторингу, мережеві утиліти (ping, traceroute) тощо[6]. Мережеве ПЗ дозволяє налаштовувати параметри мережі, керувати трафіком, забезпечувати безпеку (фаєрволи, антивіруси), а також реалізовувати прикладні служби (електронна пошта, веб-служби) на рівні додатків.

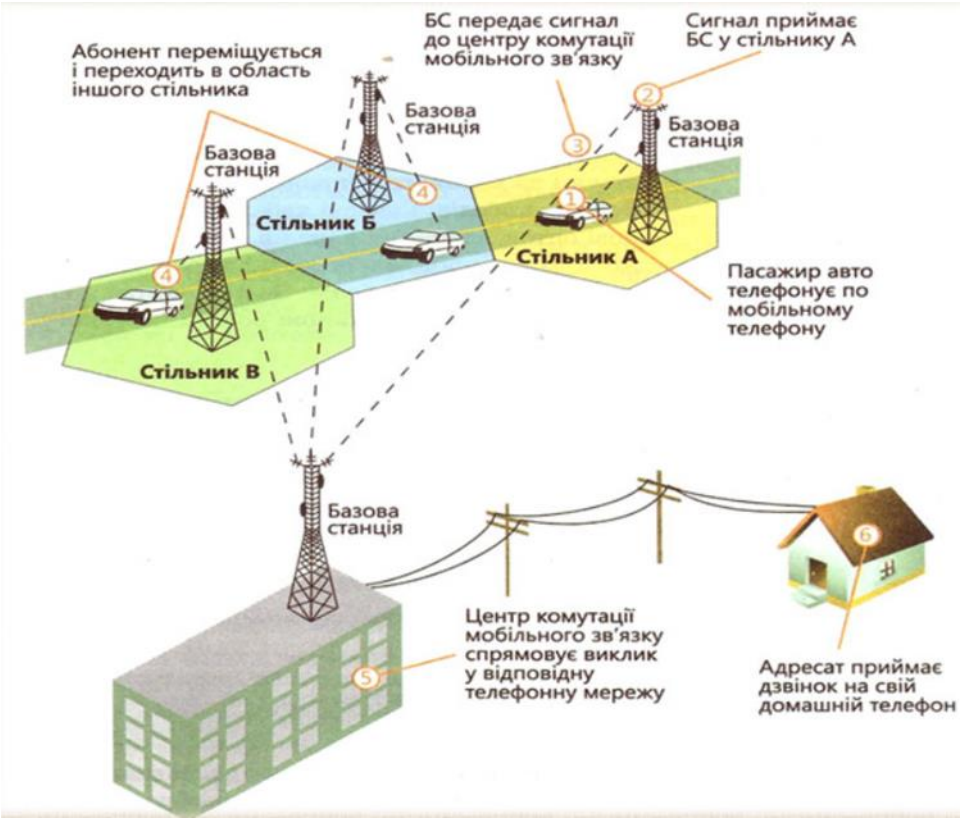


Рисунок 1.1 – Мережа пристроїв [1]

Таким чином, для побудови локальної мережі необхідно мати належним чином підібрану сукупність клієнтських пристроїв, серверів, середовища передавання даних (кабельної інфраструктури або Wi-Fi) та мережевого обладнання, а також відповідне програмне забезпечення для управління взаємодією між цими компонентами.

1.3. Роль мережевих технологій у підвищенні ефективності функціонування магазину

Впровадження технологій комп'ютерної мережі має значний вплив на ефективність і продуктивність роботи магазину. Завдяки комп'ютерним мережам магазини можуть значно покращити управління запасами, продажами, комунікацією з клієнтами та забезпеченням безпеки. Ось декілька ключових аспектів впливу технологій комп'ютерних мереж на роботу магазину:

Оптимізація управління запасами, впровадження комп'ютерних мереж дає змогу ефективно відслідковувати наявність товарів на складі в реальному часі. Це дозволяє уникнути ситуацій, коли товар вичерпується або, навпаки, надлишок товару не забезпечує потрібної ліквідності. Через мережу можна підключити систему для автоматичного оновлення запасів, а також оперативно передавати дані між центральним офісом і філіями магазину.

Швидка обробка замовлень та платежів, завдяки комп'ютерним мережам процес оформлення замовлення і обробки платежів став значно швидшим та зручнішим. Використовуючи електронні платіжні системи та онлайн-оплату, клієнти можуть здійснювати покупки без необхідності обробляти фізичні чеки, що знижує ризик помилок і підвищує швидкість обслуговування.

Покращення комунікації з клієнтами, завдяки комп'ютерним мережам магазини можуть ефективно взаємодіяти з клієнтами через різноманітні канали: електронну пошту, месенджери, соціальні мережі. Це дозволяє не лише покращити сервіс, але й надавати оперативну допомогу клієнтам у разі виникнення питань або проблем. Також це дозволяє магазину збирати зворотний зв'язок, що сприяє підвищенню лояльності клієнтів.

Інтеграція з постачальниками та партнерами, омп'ютерні мережі дають можливість автоматизувати процеси закупівлі товарів і управління постачанням. Магазин може інтегрувати свої інформаційні системи з постачальниками, що дозволяє отримувати актуальні дані про наявність товару, терміни доставки та

умови співпраці в режимі реального часу. Це дозволяє знижувати витрати на транспортування і скорочувати час доставки.

Безпека даних і захист від злому, адже провадження мережевих технологій забезпечує можливість захисту конфіденційних даних клієнтів і компанії. Використання шифрування даних, антивірусного програмного забезпечення, брандмауерів і систем моніторингу дозволяє захистити електронні платіжні системи, особисті дані покупців та фінансові операції від несанкціонованого доступу.

Моніторинг та аналітика, тому що комп'ютерні мережі дозволяють магазинам здійснювати моніторинг продажів, аналізувати попит на товари та виводити статистику в реальному часі. Це допомагає приймати обґрунтовані рішення щодо закупівель, маркетингових акцій, планування витрат і прибутків. Завдяки такій аналітиці можна оперативно коригувати стратегію продажів і маркетингу.

Мобільні технології для співробітників для роботи з інформацією в режимі реального часу. Це може бути особливо корисно для менеджерів і касирів, які можуть отримувати дані про наявність товарів, здійснювати продажі або навіть допомагати клієнтам в онлайн-форматі.

Покращення взаємодії між філіями магазину, завдяки комп'ютерним мережам, магазини, що мають кілька філій, можуть забезпечити централізоване управління. Дані про товарні запаси, фінансові операції, клієнтські дані та продажі можуть бути зібрані в єдину систему, що дозволяє здійснювати ефективне управління всіх підрозділів магазину, не залежно від їхнього місця розташування.

Впровадження технологій комп'ютерної мережі має величезний вплив на роботу магазину, значно покращуючи ефективність управління, забезпечуючи швидку комунікацію, автоматизацію процесів і підвищуючи рівень обслуговування клієнтів. Завдяки цьому магазини можуть не тільки знижувати витрати, але й підвищувати конкурентоспроможність на ринку.

1.4 Основи мережевої архітектури: моделі та протокол

Для стандартизації роботи мережевого обладнання і програмного забезпечення використовують багаторівневі еталонні моделі мереж. Найвідомішою є Модель взаємодії відкритих систем (OSI), яка визначає 7 рівнів мережевої взаємодії: фізичний, канальний, мережевий, транспортний, сеансовий, рівень представлення та прикладний рівень. Кожен рівень відповідає за певний аспект передачі даних (наприклад, мережевий рівень за маршрутизацію пакетів, транспортний за надійність доставки та порти, прикладний за інтерфейс до прикладних програм). Іншою поширеною є модель TCP/IP, яка фактично використовується в Інтернеті і має 4 рівні: рівень доступу до мережі, мережевий (Internet), транспортний та прикладний. Модель TCP/IP є спрощеною практичною реалізацією концепцій OSI, що фокусується на основних протоколах Інтернету - IP, TCP, UDP, HTTP, FTP тощо[7]. Завдяки багаторівневим моделям стало можливим розробляти сумісне обладнання і ПО: протоколи кожного рівня можуть змінюватися незалежно, не порушуючи роботу інших рівнів, якщо дотримано стандартних інтерфейсів між ними. Мережеві протоколи - це формальні правила і домовленості, що визначають формат та порядок обміну повідомленнями між мережевими пристроями. Кожен рівень моделі має свій набір протоколів. На мережевому рівні найпоширенішим протоколом є IP (Internet Protocol) версії IPv4 або новий IPv6, що відповідає за адресацію вузлів в мережі і маршрутизацію пакетів між мережами. IP-адреса - це унікальний числовий ідентифікатор мережевого рівня, який використовується для адресації пристроїв у мережах на основі стека TCP/IP. У IPv4 адреса складається з 4 байт (32 біт), записаних у десятковій формі через крапки (наприклад, 192.168.0.1), а в IPv6 - з 16 байт у шістнадцятковій формі. Для доставки даних по мережі IP-пакети вкладаються в кадри канального рівня, які передаються по фізичному середовищу.

Рисунок 1.2 – Модель OSI [2]

На транспортному рівні ключовими протоколами є TCP (Transmission Control Protocol) та UDP (User Datagram Protocol). TCP забезпечує надійну встановлення з'єднання, контроль доставки (квитування, повторна передача втрачених сегментів, впорядкування), використовується для важливих даних (веб-сторінки по HTTP/HTTPS, передача файлів, пошта). UDP надає ненадійний, але швидший спосіб передачі (без встановлення з'єднання) використовується для потокових даних або служб, чутливих до затримок (онлайн-відео, VoIP, DNS-запити).

На прикладному рівні діють протоколи, що відповідають конкретним сервісам: HTTP/HTTPS - для веб, FTP - для файлів, SMTP/IMAP - для електронної пошти, DNS - служба доменних імен, яка перетворює символьні доменні імена на IP-адреси і навпаки (за допомогою DNS-серверів).

Отже, мережеві моделі OSI та TCP/IP описують принципи побудови і функціонування мереж, а набір протоколів кожного рівня забезпечує реалізацію відповідних функцій, від фізичного з'єднання до прикладних сервісів[8]. Розуміння цих моделей і протоколів є необхідним при проектуванні мережі магазину. У

сучасному роздрібному бізнесі стабільна та безпечна комп’ютерна мережа є критично важливою складовою для ефективної роботи магазину. Вона забезпечує безперебійну взаємодію між робочими станціями, торговим обладнанням, системами відеоспостереження, серверами обліку товарів, а також доступ до Інтернету та централізованих сервісів. Вірно спроєктована локальна мережа дає змогу автоматизувати процеси обліку, контролювати операції продажу в реальному часі та забезпечувати швидкий обмін даними між різними підрозділами магазину.

1.5 Постановка задачі

Для досягнення поставленої мети у розробці моделі комп’ютерної мережі для магазину з використанням програмного середовища Cisco Packet Tracer. потрібно провести детальний аналіз функціональних вимог до мережі магазину. Після цього розробляється як логічна, так і фізична структура локальної мережі, що враховує всі зони обслуговування. На основі цього здійснюється вибір відповідного мережевого обладнання, як-от комутатори, маршрутизатори та точки доступу, із обґрунтуванням доцільності їхнього використання. Наступним етапом є налаштування IP-адресації для всіх пристроїв згідно з розробленою схемою підмереж, що забезпечить коректну маршрутизацію трафіку. Важливою частиною є налаштування віртуальних локальних мереж (VLAN) для розмежування трафіку між різними відділами магазину, що підвищує ефективність і безпеку мережі. Додатково реалізуються базові функції безпеки, включаючи ACL, обмеження доступу та сегментацію VLAN.

Завершальним етапом є симуляційне тестування мережі у віртуальному середовищі, що дозволяє перевірити працездатність налаштувань та виявити можливі проблеми до впровадження системи в реальних умовах.

Результатом цієї роботи має стати повноцінна модель комп’ютерної мережі магазину з детально задокументованими налаштуваннями, схемами, а також поясненнями вибору технічних рішень. Ця модель може бути використана як основа для впровадження реальної мережі в магазині.

1.6 Висновки першого розділу

У першому розділі було здійснено детальний аналіз основних аспектів, що стосуються побудови та функціонування комп’ютерних мереж. Вивчення основних компонентів та структур мережі дозволяє розуміти важливість правильної архітектури для забезпечення ефективної роботи всіх елементів, від пристроїв до сервісів. Досліджено різноманітні типи мережевих технологій, зокрема бездротові та дротові рішення, які мають різні характеристики, що впливають на їхнє застосування в різних умовах. Також було проведено порівняння переваг і недоліків кожної технології з урахуванням вимог до швидкості, надійності та безпеки.

Визначення вузьких місць у мережі стало важливим етапом, оскільки це дозволяє прогнозувати потенційні проблеми в процесі роботи магазину. Рішення щодо вибору обладнання та програмного забезпечення повинні бути підкріплені результатами цього аналізу, щоб уникнути ускладнень і забезпечити стабільне функціонування мережі. На основі виконаного аналізу розроблено рекомендації для покращення існуючої мережевої інфраструктури магазину, що дозволить підвищити ефективність її роботи та забезпечити високий рівень безпеки.

Таким чином, отримані результати дозволяють закласти основи для подальшої розробки технічного проекту комп’ютерної мережі магазину, враховуючи як поточні потреби, так і перспективи розвитку.

2 ПРОЄКТУВАННЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ МАГАЗИНУ

2.1 Порівняльний аналіз варіантів топологій локальних мереж

Топологія мережі визначає фізичну або логічну схему з'єднання вузлів. Існує кілька базових топологій локальних мереж: шинна, кільцева, зіркоподібна (зірка), деревоподібна, mesh (комірчаста) тощо. Вибір топології впливає на продуктивність мережі, складність її розгортання і стійкість до відмов окремих вузлів.

Шиною називається історично перша топологія Ethernet-мереж, всі вузли якої підключені до спільного коаксіального кабелю (магістралі). Сигнал передається по шині і може прийматися всіма вузлами, кожен вузол «слухає» трафік і забирає пакети, адресовані саме йому[9]. На кінцях кабелю-шини встановлюються термінатори, щоб поглинати сигнал і запобігати його відбиттю. Топологія шина проста, але має суттєві недоліки: обмежену довжину і кількість вузлів, колізії при одночасній передачі, складність локалізації несправностей (обрив кабелю виводить з ладу всю мережу). Наразі шинна топологія майже не використовується, поступившись більш гнучкій схемі «зірка».

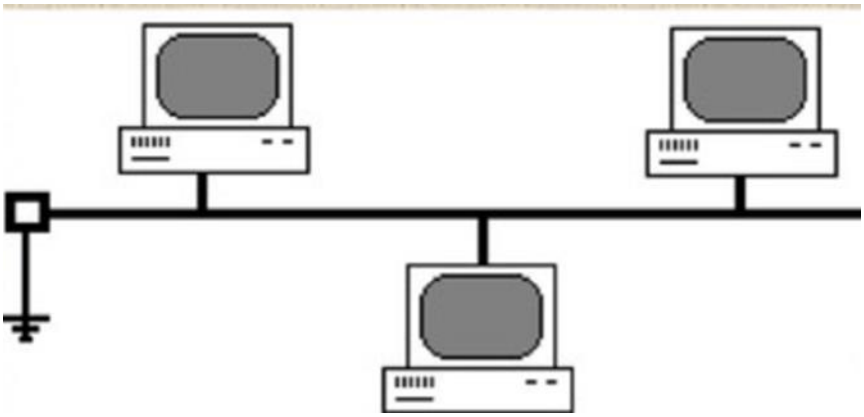


Рисунок 2.1 – Шинна технологія [3]

Інтегровані бездротові інтерфейси, зокрема Wi-Fi і Bluetooth, роблять ESP32 ідеальним вибором для створення бездротових і розподілених систем. Цей проєкт вимагає постійної комунікації між різними елементами системи, тому можливість використання Wi-Fi для підключення до мережі та Bluetooth для з'єднання з іншими

пристроями забезпечить зручність і стабільність у роботі. Крім того, ESP32 має великий обсяг оперативної пам’яті і підтримує до 34 GPIO-пінів, що дозволяє підключати багато датчиків та пристроїв, що є важливим аспектом для проєкту.

У кільці кожен комп’ютер з’єднаний з двома сусідніми, утворюючи замкнене кільце. Дані передаються від вузла до вузла по кільцю, поки не досягнуть отримувача[10]. В класичному кільці використовується метод передачі «маркер» - спеціальний фрейм, що циркулює в кільці і дає право відправити дані. Кільцеві мережі (Token Ring, FDDI) мали детермінований доступ без колізій, але складність конфігурації і вихід з ладу будь-якого вузла порушував усе кільце (якщо немає механізмів обходу). Сьогодні кільцева топологія зустрічається хіба що в мережах специфічних промислових рішень або як логічна топологія (наприклад, двонапрямні кільцеві MAN-мережі).

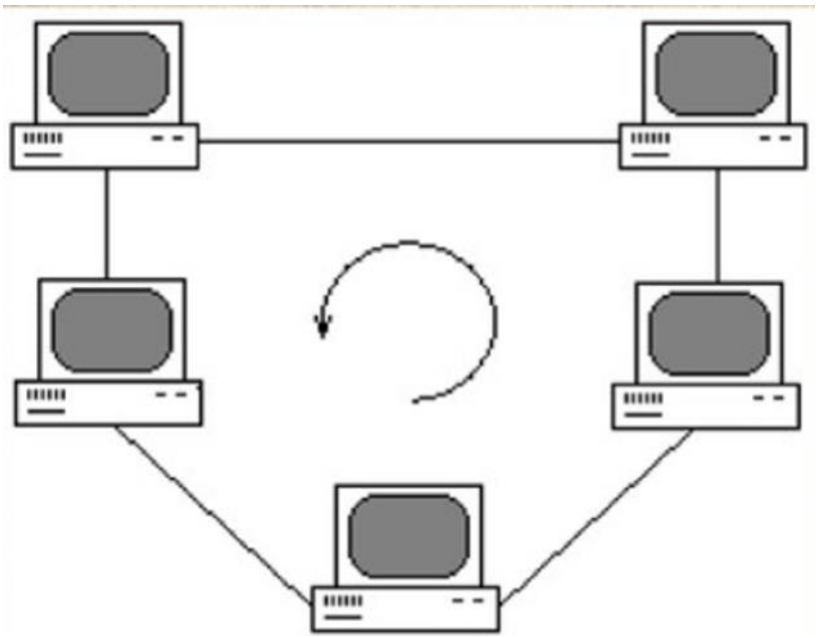


Рисунок 2.2 – Зіркоподібна технологія [4]

Зірка, де всі периферійні вузли підключені до центрального вузла (концентратора, комутатора або маршрутизатора). Топологія «зірка» є найпоширенішою для локальних мереж: кожен комп’ютер має окреме підключення до центру. У разі виходу з ладу одного кабелю, інша мережа продовжує працювати, що покращує надійність. Сучасні Ethernet LAN практично завжди будуються за

принципом зірки (з комутатором у центрі). Зіркоподібна топологія легко масштабується (можна додати новий вузол, підключивши його до комутатора), а продуктивність вища, оскільки кожен порт комутатора - окремий сегмент мережі. Недоліком зірки є залежність від центрального вузла: якщо, наприклад, центральний комутатор знеструмлений або зламаний, вся мережа вийде з ладу. Тому в критичних мережах інколи застосовують резервування центральних вузлів або перехід до дворівневої топології (ієрархічна зірка).

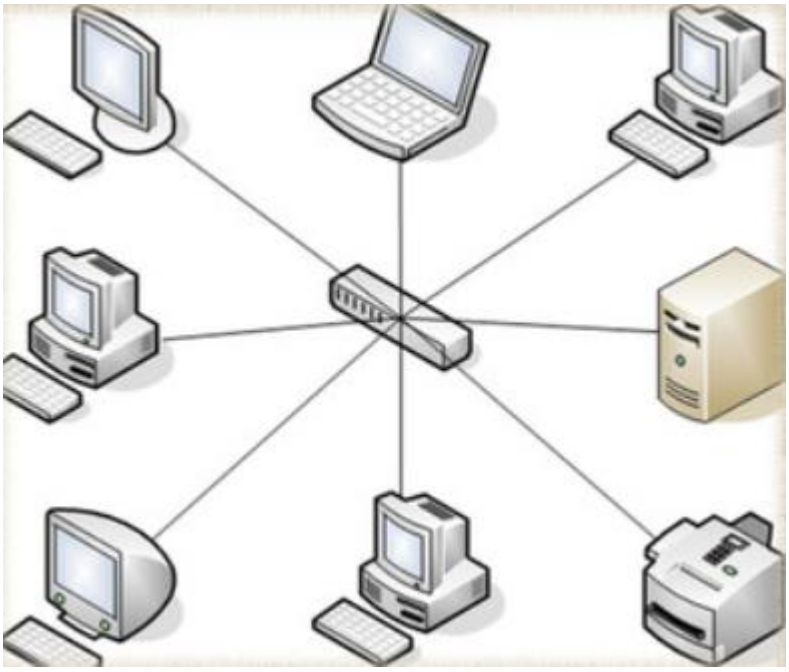


Рисунок 2.3 - Ієрархічна топологія [5]

Дерево (ієрархічна топологія) фактично є багаторівневою зіркою. Один комутатор може підключатися до вищерозташованого комутатора, утворюючи деревоподібну структуру. Така топологія використовується у великих мережах підприємств, де є декілька рівнів: доступу (комутатори до яких підключені кінцеві пристрої), розподілу (проміжні комутатори, що агрегують трафік) та ядра (високопродуктивні комутатори/маршрутизатори, що з’єднують усі сегменти і часто виконують маршрутизацію між ними). Ієрархічна модель мережі Cisco трирівневої архітектури (Core/Distribution/Access) є прикладом деревоподібної топології для підвищення масштабованості та продуктивності мережі[10]. Для

малого магазину масштаб ієрархії може бути меншим (2 рівні - комутатор доступу + маршрутизатор як ядро), але принцип розділення на сегменти зберігається.

Комірчаста (mesh) характеризується тим, що кожен вузол з'єднаний з кількома іншими, утворюючи множину шляхів для трафіку. Повна комірчата топологія означає з'єднання кожного з кожним, що забезпечує максимальну резервування (поломка одного з'єднання не впливає, оскільки є інші шляхи), але вимагає дуже багато з'єднань. Практично застосовуються частково комірчасті топології, зокрема в бездротових mesh-мережах (кілька точок доступу пов'язані бездротово між собою для розширення покриття Wi-Fi). У проводових корпоративних мережах елементи комірчастості можуть бути на верхніх рівнях (кілька ядрових комутаторів зв'язані між собою). Для мережі магазину комірчаста топологія не потрібна, достатньо схеми «зірка» з одним центральним пристроєм і, за необхідності, резервним каналом до Інтернету.

У проєкті мережі магазину як фізична топологія буде використана структура типу «зірка»: всі комп'ютери у відділах підключені кабелями до центрального комутатора (що знаходиться в серверній кімнаті). Така топологія є оптимальною для офісних приміщень і торгових залів, забезпечуючи простоту розгортання і високошвидкісне з'єднання[11]. Логічна топологія мережі (схема VLAN і маршрутизації) буде розглянута в розділі 3.

2.2 Архітектура мережі: компоненти та принципи взаємодії

Як зазначалося, мережеве обладнання - це активні пристрої, що керують передачею даних в мережі. Розглянемо ключові типи обладнання, що використовуються при побудові локальних мереж, а також принципи їхнього застосування:

Мережевий комутатор (свіч, switch) - пристрій для об'єднання вузлів у локальну мережу на основі канального рівня. Комутатор має кілька портів (24, 48 і більше), до яких підключаються комп'ютери або інші комутатори. Він аналізує MAC-адреси вхідних кадрів і пересилає їх лише на порт призначення, тим самим

сегментуючи трафік і зменшуючи кількість колізій. Сучасні комутатори є керованими (managed switches) - дозволяють налаштовувати VLAN, пріоритизацію трафіку (QoS), агрегування каналів, моніторинг. У нашій мережі комутатор слугуватиме центральним вузлом топології «зірка», з'єднуючи всі відділи. Для забезпечення пропускної здатності вибирається гігабітний комутатор з відповідною кількістю портів. Більшість моделей комутаторів працюють на 2 рівні моделі OSI (канальному), але існують багаторівневі комутатори (L3 switches), що можуть виконувати і функції маршрутизації між VLAN.

Маршрутизатор (router) - пристрій мережевого рівня, що з'єднує різні IP-мережі та виконує маршрутизацію пакетів між ними. Маршрутизатор приймає рішення, куди переслати пакет, на основі IP-адреси одержувача і таблиці маршрутів[12]. У домашніх і малих офісах часто використовують комбіновані пристрої (SOHO-роутери), що містять в собі маршрутизатор, комутатор і точку доступу Wi-Fi в одному корпусі. В корпоративних мережах застосовуються окремі маршрутизатори або багатофункціональні маршрутизатори Cisco ISR для підключення до зовнішніх мереж (Інтернет, VPN між філіями) та для організації інтерфейсів з різними каналами (оптика, xDSL, 4G тощо). У проекті магазину маршрутизатор забезпечить вихід всієї локальної мережі в Інтернет через провайдера, а також виконає функцію маршрутизації між кількома внутрішніми підмережами (VLAN). Тобто він буде працювати як шлюз за замовчуванням для усіх внутрішніх VLAN. Реалізовано це може бути або окремим фізичним маршрутизатором, підключеним до комутатора (схема router-on-a-stick через trunk-порт), або використанням L3-функцій комутатора (за наявності L3-switch). В нашому проекті передбачається використання окремого маршрутизатора Cisco для наочності налаштування.

Бездротова точка доступу (Wi-Fi AP) - пристрій, що забезпечує підключення бездротових клієнтів (ноутбуків, смартфонів) до локальної мережі по технології Wi-Fi (стандарти IEEE 802.11 a/b/g/n/ac/ax). Точка доступу зазвичай під'єднується до комутатора дротовим каналом і виступає «містом» між бездротовим сегментом та дротовою мережею[13]. У магазині точка доступу використовується для надання

доступу до мережі у виставковій залі (для клієнтів або для бездротових пристроїв персоналу). Сучасні точки доступу підтримують кілька SSID та VLAN, що дозволяє розділити трафік, наприклад, гостьовий Wi-Fi ізольовано від внутрішньої мережі.

Мережевий сервер - окремий комп'ютер або пристрій, що надає мережеві сервіси. Хоч сервер - це швидше кінцевий пристрій з точки зору мережевої моделі (працює як вузол на прикладному рівні), але він є невід'ємним компонентом мережі підприємства. Сервер може виконувати роль контролера домену, файлового сервера, сервера баз даних, поштового або веб-сервера для внутрішніх потреб компанії. У мережі магазину передбачається виділений сервер у службовому приміщенні. Він буде використовуватися для зберігання спільних документів, баз даних клієнтів/продажів та інших корпоративних даних. Також сервер може виконувати функції DHCP (роздача IP-адрес клієнтам) і DNS-кешу для внутрішньої мережі, якщо це налаштувати. Обрання апаратної платформи сервера залежить від вимог по навантаженню: для невеликого магазину достатньо одного сервера середнього класу (на базі, наприклад, Intel Xeon, 16-32 ГБ ОЗП, RAID-масиву для надійності зберігання даних).

При проектуванні мережі важливо керуватися певними принципами: мережа повинна забезпечувати достатню пропускну здатність для поточних потреб (робота з базою даних, передача файлів, IP-телефонія тощо) і мати резерв для зростання навантаження. Використання гігабітних з'єднань між основними вузлами, можливість додати ще користувацькі порти (наприклад, комутатор з певним запасом портів) - усе це враховується на етапі проектування

Надійність і відмовостійкість: передбачаються мінімізація єдиних точок відмови (single point of failure) та наявність резервних рішень. Наприклад, резервне копіювання важливих даних сервера, джерело безперебійного живлення (UPS) для серверної та ключового обладнання, можливість швидкої заміни несправного комутатора. У більших мережах застосовують дублювання ліній зв'язку, резервні маршрутизатори з протоколами відмовостійкості (VRRP, HSRP), проте для мережі

магазину достатньо простіших рішень (один маршрутизатор і комутатор без дублювання, але із UPS).

Сегментація та безпека: рекомендується розділяти мережу на логічні сегменти (підмережі, VLAN) відповідно до функції підрозділів, щоб обмежити широкомовний трафік і підвищити захищеність. Наприклад, бухгалтерія або адміністрація можуть бути у окремому VLAN, відокремленому від гостьової Wi-Fi мережі. Маршрутизатор зможе контролювати обмін між VLAN, застосовувати списки контролю доступу (ACL) для обмеження доступу до конфіденційних ресурсів[14]. Така мережева ізоляція запобігає несанкціонованому доступу: користувач гостьової мережі не зможе бачити внутрішній сервер, якщо це заборонено політикою.

Принцип ієрархічності: як згадано, навіть у невеликій мережі варто виділити рівні рівень доступу (комутатори, до яких підключені кінцеві пристрої) і рівень ядра/маршрутизації (маршрутизатор, що з'єднує всі VLAN і виходить в Інтернет). Така структуризація полегшує адміністрування та масштабування мережі. Наприклад, якщо в майбутньому магазин розшириться (нові відділи або зали), можна додати ще один комутатор на рівні доступу і з'єднати з ядром, не перебудовуючи всю архітектуру.

Дотримання стандартів: обладнання та технології повинні відповідати загальноприйнятим стандартам (Ethernet, Wi-Fi, TCP/IP). Це забезпечить сумісність пристроїв різних виробників і можливість інтеграції з іншими мережами. В роботі використовується стандарт Ethernet (IEEE 802.3) для дротових з'єднань і IEEE 802.11 для бездротових. IP-адресація застосовується за стандартом IPv4 приватних мереж (RFC 1918), а для виходу в Інтернет - технологія NAT/PAT. Протоколи маршрутизації у межах маленької мережі можуть бути статичними (статичні маршрути), або динамічний протокол не потрібен через простоту топології.

2.3 Підходи до забезпечення кібербезпеки в комп'ютерних мережах

Безпека комп’ютерної мережі - критично важливий аспект, особливо коли мережа забезпечує роботу бізнесу і містить конфіденційні дані (комерційна інформація, персональні дані клієнтів, фінансова документація тощо). Розглянемо базові заходи захисту мережі, які будуть застосовані при побудові мережі магазину:

Міжмережевий екран (фаєрвол) - основний засіб захисту мережі від несанкціонованих доступів. Фаєрвол контролює вхідний і вихідний трафік, блокуючи небезпечні з’єднання та пакети, що не відповідають встановленим правилам. В контексті нашого проекту роль простого фаєрволу виконує NAT/ACL на маршрутизаторі: всі внутрішні адреси приховані за одним зовнішнім IP, а вхідні з’єднання з Інтернету за замовчуванням заборонені (якщо не налаштовано переадресацію портів для якогось сервісу). Це створює базовий захист від зовнішніх атак, оскільки зовнішні користувачі не можуть прямо ініціювати з’єднання до внутрішніх вузлів[15]. Додатково на маршрутизаторі можуть бути налаштовані ACL, що блокують, наприклад, доступ гостьової мережі до адрес внутрішнього серверу. Якщо виникне потреба, може бути встановлено окремий апаратний брандмауер для фільтрації трафіку більш детально або використано вбудований firewall- функціонал роутера.

Контроль доступу та ізоляція мереж: як зазначалося, використання VLAN дозволяє ізолювати трафік різних підрозділів. У нашій мережі гостьова Wi-Fi мережа буде у окремому VLAN без доступу до внутрішніх ресурсів. Також обмежено доступ між внутрішніми сегментами: наприклад, відділ маркетингу не потребує доступу до комп’ютерів відділу охорони і навпаки. Такі обмеження (зоны безпеки) можна впровадити списками доступу на маршрутизаторі. Крім того, на самому комутаторі варто вимкнути невикористовувані порти або закріпити конкретні MAC-адреси за портами (Port Security) - щоб ніхто не підключив несанкціонований пристрій у вільний порт.

Шифрування та автентифікація: при побудові бездротової мережі слід застосувати сучасні методи шифрування трафіку (стандарт WPA2-PSK або WPA3 для Wi-Fi) і надійний пароль до бездротової мережі, щоб запобігти підключенню сторонніх осіб. Внутрішні сервіси (електронна пошта, веб-доступ до внутрішньої

системи) мають використовувати захищені протоколи (HTTPS, TLS) щоб завадити перехопленню даних. Якщо співробітники підключаються віддалено, варто розгорнути VPN для шифрованого тунелю. У межах магазину VPN може й не знадобитися, але шифрування Wi-Fi - обов'язкова умова.

Політики паролів та доступу: всі мережеві пристрої (роутер, комутатор, сервер) повинні бути захищені паролями адміністратора. Паролі повинні бути складними, регулярно змінюватися. На сервері бажано розмежувати права користувачів (не давати співробітникам зайвих привілеїв), важливі файли шифрувати або принаймні робити резервні копії. Слід впровадити політику, що користувачі не підключають до мережі власні пристрої без дозволу (щоб уникнути потенційних вірусів) або хоча б сканувати такі пристрої антивірусом.

Антивірусний захист та оновлення: всі комп'ютери в мережі повинні мати оновлене антивірусне програмне забезпечення, щоб виявляти і видаляти шкідливі програми[16]. Сервер та клієнтські ПК мають регулярно отримувати оновлення операційної системи і програм - це закриває відомі уразливості, якими можуть скористатися зловмисники.

Резервне копіювання: резервні копії важливих даних - теж частина безпеки, адже в разі атаки (наприклад, шифрувальником) або збою обладнання, наявність бекапів дозволить відновити роботу. У нашому випадку серверні дані (база даних товарів, документи) будуть дублюватися на зовнішній носій або в хмарне сховище на регулярній основі (наприклад, щоденно інкрементальний бекап). Резервні копії конфігурацій маршрутизатора і комутатора також слід зберігати (можна на тому ж сервері) - щоб у разі поломки швидко налаштувати заміну.

Загалом, для мережі невеликого магазину доцільно реалізувати саме базові заходи кібербезпеки: ізоляція сегментів, міцний периметр (NAT/фаєрвол), шифрування Wi-Fi, управління доступом та резервування даних. Цих кроків достатньо, щоб значно знизити ризики несанкціонованого доступу та втрати інформації, не ускладнюючи при цьому мережу зайвими дорогими рішеннями. У практичній частині роботи наведено конкретні налаштування, що покращують безпеку спроектованої мережі магазину.

Існують також інші типи комп'ютерних мереж, такі як :

PAN - це персональна мережа, яка об'єднує персональні технологічні пристрої для зв'язку на невеликій відстані. Вона охоплює лише менше 10 метрів або 33 футів площі[17]. PAN має менше користувачів порівняно з іншими мережами, такими як LAN, WAN тощо. PAN зазвичай використовує певну форму бездротової технології. PAN передбачає передачу даних між інформаційними пристроями, такими як смартфони, персональні комп'ютери, планшетні комп'ютери тощо.

Локальна мережа (LAN) -Локальна мережа з'єднує мережеві пристрої таким чином, що персональні комп'ютери та робочі станції можуть спільно використовувати дані, інструменти та програми. Група комп'ютерів і пристроїв з'єднана між собою комутатором або стеком комутаторів, використовуючи схему приватної адресації, визначену протоколом TCP/IP. Приватні адреси є унікальними по відношенню до інших комп'ютерів у локальній мережі. Маршрутизатори знаходяться на межі локальної мережі і з'єднують її з глобальною мережею (WAN).

Дані передаються з дуже високою швидкістю, оскільки кількість підключених комп'ютерів обмежена. За визначенням, з'єднання повинні бути високошвидкісними і відносно недорогими (наприклад, концентраторами, мережевими адаптерами і кабелями Ethernet). Локальні мережі охоплюють меншу географічну територію (розмір обмежений кількома кілометрами) і перебувають у приватній власності. Її можна використовувати в офісних будівлях, будинках, лікарнях, школах тощо. Локальну мережу легко спроектувати та обслуговувати. Середовище зв'язку, що використовується в локальній мережі, має виту пару та коаксіальні кабелі. Вони покривають невеликі відстані, тому помилки та шум зводяться до мінімуму.

Глобальна мережа (WAN) - це комп'ютерна мережа, яка охоплює велику географічну територію, хоча вона може бути обмежена межами держави або країни. WAN має радіус дії понад 50 км[18]. Глобальна мережа може являти собою з'єднання локальної мережі з іншими локальними мережами за допомогою телефонних ліній і радіохвиль і може бути обмеженою підприємством

(корпорацією або організацією) або доступною для громадськості. Ця технологія є високошвидкісною і відносно дорогою.

Існує два типи WAN: комутована WAN і WAN типу «точка-точка». WAN складно проектувати і обслуговувати. Подібно до локальної мережі, відмовостійкість глобальної мережі є меншою, а перевантаження в мережі є більшим. Середовищем зв'язку, що використовується для WAN, є ТфОП (телефонна мережа загального користування) або супутниковий зв'язок. Через передачу на великі відстані, шум і помилки в глобальній мережі, як правило, більші[19].

Локальна мережа з'єднує мережеві пристрої таким чином, що персональні комп'ютери та робочі станції можуть спільно використовувати дані, інструменти та програми. Група комп'ютерів і пристроїв з'єднана між собою комутатором або стеком комутаторів, використовуючи схему приватної адресації, визначену протоколом TCP/IP[20]. Приватні адреси є унікальними по відношенню до інших комп'ютерів у локальній мережі. Маршрутизатори знаходяться на межі локальної мережі і з'єднують її з глобальною мережею (WAN).

Дані передаються з дуже високою швидкістю, оскільки кількість підключених комп'ютерів обмежена. За визначенням, з'єднання повинні бути високошвидкісними і відносно недорогими (наприклад, концентраторами, мережевими адаптерами і кабелями Ethernet). Локальні мережі охоплюють меншу географічну територію (розмір обмежений кількома кілометрами) і перебувають у приватній власності. Її можна використовувати в офісних будівлях, будинках, лікарнях, школах тощо. Локальну мережу легко спроектувати та обслуговувати. Середовище зв'язку, що використовується в локальній мережі, має виту пару та коаксіальні кабелі. Вони покривають невеликі відстані, тому помилки та шум зводяться до мінімуму.

2.4. Технічний опис об’єкта та мережеві вимоги до його обслуговування

Об’єктом проектування є локальна мережа магазину роздрібної торгівлі. Магазин розташований у приміщенні з кількома кімнатами та зонами, що відповідають різним функціональним підрозділам фірми. На основі наданої схеми приміщення магазину виділено наступні зони та відділи: виставкова зала, кімната охоронця, кімната секретаря, кабінет директора, маркетинговий відділ, відділ продажів, відділ спілкування з клієнтами (відділ підтримки клієнтів) та службове приміщення (серверна). Кожен з цих підрозділів має свої потреби в мережевих ресурсах та обладнанні.

Вітрина: містить декілька комп’ютерів або ноутбуків, призначених для демонстрації товарів клієнтам. Ці пристрої повинні мати доступ до Інтернету (для показу онлайн-ресурсів, характеристик товарів) та, можливо, до локальної бази даних товарів. Проте мережа виставкової зали має бути відокремлена від внутрішніх службових сегментів з міркувань безпеки, оскільки до цих комп’ютерів можуть мати фізичний доступ відвідувачі. Виставкова зала: містить декілька комп’ютерів або ноутбуків, призначених для демонстрації товарів клієнтам

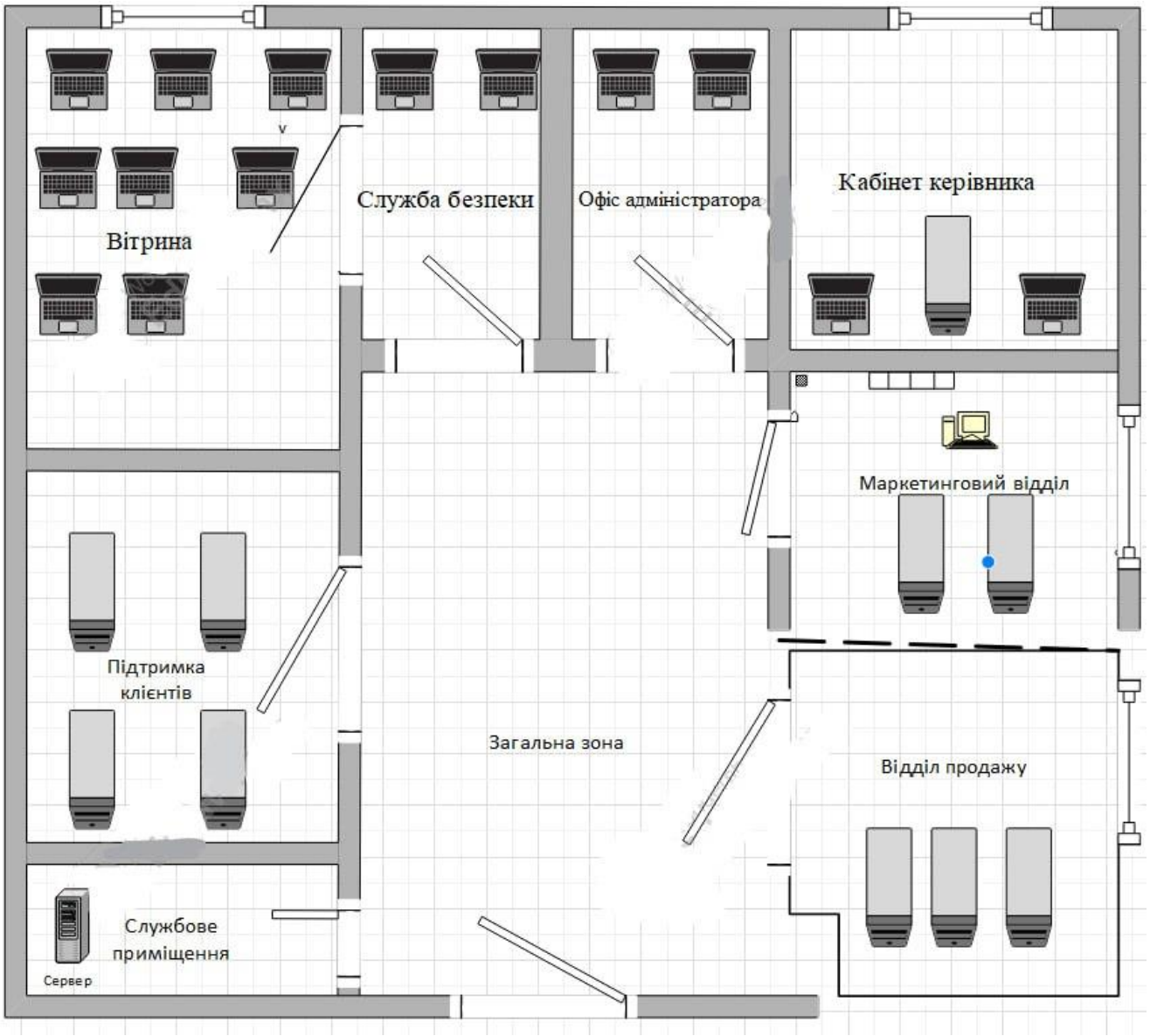


Рисунок 2.4 – План приміщення магазину [6]

Ці пристрої повинні мати доступ до Інтернету (для показу онлайн-ресурсів, характеристик товарів) та, можливо, до локальної бази даних товарів. Проте мережа виставкової зали має бути відокремлена від внутрішніх службових сегментів з міркувань безпеки, оскільки до цих комп'ютерів можуть мати фізичний доступ відвідувачі. Також у виставковій зоні доцільно забезпечити Wi-Fi для клієнтів (гостьовий доступ до Інтернету), що підвищить привабливість магазину.

Кімната охоронця характеризується тим, що у цьому приміщенні знаходиться пост безпеки. Потреби: один комп'ютер охорони, який може здійснювати моніторинг камер відеоспостереження (якщо камери IP, то трафік відео йде по

мережі), спілкування з системою сигналізації тощо. Цей ПК повинен мати стабільне дротове підключення до мережі. Доступ до Інтернету для охорони не критичний, але може знадобитися для екстреного зв’язку або передачі даних. Важливо відділити мережу охорони від інших - наприклад, камери можуть бути в окремому VLAN, доступному лише серверу запису. В нашому випадку, оскільки специфіка CCTV не детально описана, припустимо що охоронець використовує ПК для загальних задач і перегляду камер, які підключені до того ж комп’ютера або DVR.

Офіс адміністратора є першим контактом для клієнтів, тому його комп’ютер має доступ до внутрішньої бази клієнтів, до електронної пошти, CRM-системи. Він також потребує виходу в Інтернет для комунікацій. Робоче місце секретаря розташоване поруч із входом, тому підключення виконане по дроту, а не Wi-Fi, для надійності.

Кабінет директора: директорський ПК повинен мати доступ до всіх ключових ресурсів - внутрішньої бази даних, документів на сервері, статистики продажів, а також до Інтернету для аналітики та зв’язку. Як правило, для керівництва важлива безпека інформації, тому сегмент директора може бути логічно ізольований або мати додатковий захист (наприклад, доступ до деяких даних лише з його комп’ютера).

Маркетинговий відділ складається зі співробітників, що займаються рекламою, дослідженнями ринку, роботою з соцмережами. Їм потрібен вільний доступ до Інтернету (пошук інформації, робота з сайтом компанії, соцмережі), а також доступ до внутрішніх ресурсів: спільних папок на сервері, де зберігаються рекламні матеріали, клієнтські анкети, тощо. Маркетинг може знадобитися обмін великими файлами (графіка, відео), тому бажано гігабітне підключення для їхніх ПК. Їхня мережа може бути об’єднана з іншими офісними працівниками (наприклад, з продажами) або виділена окремо - це вирішимо при проектуванні VLAN.

Відділ продажу: робочі місця продавців-консультантів (можливо, менеджери з продажу, обробка замовлень). Вони активно працюють з внутрішньою базою

товарів, оформлюють продажі, тому мають доступ до серверної бази даних товарів і клієнтів. Також їм потрібна електронна пошта, обмін документами - тобто доступ до серверу файлів. Інтернет потрібен для перевірки оновлень цін, спілкування з постачальниками тощо. Стабільність і швидкодія мережі для них критична, щоб обслуговувати клієнтів без затримок (швидкий пошук інформації про товар, наявність на складі тощо).

Відділ спілкування з клієнтами, вони приймають дзвінки від клієнтів, консультують щодо товарів, статусу замовлень. Їхні ПК повинні мати доступ до тієї ж бази клієнтів і замовлень на сервері, щоб оперативно надавати інформацію. Також їм потрібен вихід в Інтернет (якщо спілкування відбувається через онлайн-чат або інші канали). Можливо використання IP-телефонів або софтфонів - тоді слід передбачити, що мережа має підтримувати і трафік VoIP (голосовий, чутливий до затримок). У нашому проекті можна припустити, що 4 комп’ютери цього відділу підключено до мережі і через них оператори здійснюють дзвінки (VoIP) або відповідають на звернення в CRM-системі. Отже, як і для продажів, якість з’єднання повинна бути високою.

Службове приміщення (серверна) вважається невеликою кімнатою, де встановлено сервер і мережеве обладнання (комутатор, маршрутизатор, патч-панель тощо). Сюди сходяться всі кабелі від робочих місць (структурована кабельна система). В серверній підтримується безпечне середовище - обмежений доступ (тільки адміністратору або директору), стабільне живлення (UPS), вентиляція/кондиціювання для серверу. Сервер, що знаходиться тут, виконує роль центрального вузла для зберігання даних та, можливо, серверу додатків. Також у цю кімнату заходить зовнішній канал Інтернет від провайдера, підключений до маршрутизатора. Усі налаштування мережі (VLAN, маршрутизація, безпека) зосереджені на обладнанні серверної.

Аналіз структури магазину показує, що мережа повинна охоплювати стаціонарні пристроїв (робочі комп’ютери та ноутбуки по відділах, сервер, охоронний ПК) і надавати бездротовий доступ для мобільних пристроїв клієнтів. У пікові години в мережі може одночасно передаватися значний обсяг даних (запити

до бази, веб-трафік маркетингу, голосовий трафік підтримки). Тому мережа має бути продуктивною (гасити можливі широкомовні «шторми», розподіляти навантаження), а також безпечною (ізолювати гостьовий трафік, захистити серверні дані).

На основі потреб підрозділів потрібно сформувати ключові вимоги до мережі магазину. Необхідно зв'язати всі комп'ютери в відділах магазину в єдину локальну мережу для забезпечення швидкого обміну даними, зокрема для доступу до спільної бази даних, файлів та інших ресурсів. Для підключення до Інтернету всіх підрозділів слід налаштувати єдиний шлюз, що дозволить доступ до зовнішніх ресурсів, електронної пошти, веб-сайтів постачальників і соціальних мереж для маркетингу. Окрім цього, потрібно виділити окрему гостьову мережу Wi-Fi для клієнтів у виставковій залі, яка повинна мати доступ тільки до Інтернету та не повинна надавати доступ до внутрішніх ресурсів магазину. Для забезпечення безпеки і кращої керованості трафіку слід реалізувати сегментацію мережі за відділами, із відокремленням адміністративного відділу від загальної мережі, а також сегментацією гостьового трафіку. Оптимальним рішенням буде використання VLAN для логічного розподілу.

Необхідно забезпечити централізоване зберігання даних на сервері, що буде доступний з усіх необхідних точок. Важливо, щоб доступ до сервера мали лише довірені сегменти мережі, такі як внутрішні VLAN, а також обмежити доступ з гостьового VLAN і зовні без використання VPN. Система повинна також забезпечувати автоматичну роздачу IP-адрес клієнтам через DHCP, що полегшує адміністрування, а також підтримувати DNS для кешування запитів або використання DNS-провайдера. При необхідності, також потрібно передбачити резервування IP-адрес за MAC-адресами для важливих пристроїв, таких як принтери чи камери.

Що стосується мережевої безпеки, то потрібно налаштувати фільтрацію трафіку між VLAN, зокрема забезпечити, щоб гостьовий VLAN не мав доступу до сервера та інших VLAN. Важливими аспектами є встановлення сильних паролів на мережевому обладнанні, використання шифрування для Wi-Fi мережі та можливе

впровадження VPN-доступу для віддаленого керування для адміністратора мережі. Також необхідно реалізувати контроль фізичного доступу до мережевого обладнання, щоб серверна була замкнена.

Для забезпечення надійності системи слід передбачити методи резервного копіювання ключових даних, таких як серверні файли і бази даних. Мережа повинна дозволяти зберігати резервні копії на зовнішньому NAS або в хмарі через Інтернет в нічний час. Враховуючи потребу в масштабованості, мережа повинна мати можливість розширення – додавання нових робочих місць, підключення мережевого принтера, POS-терміналів та інших пристроїв. Тому слід передбачити достатній запас портів на комутаторі, IP-адрес у підмережах і потужності обладнання, наприклад маршрутизатора, що витримає більшу навантаження.

З огляду на те, що магазин може не мати окремого IT-спеціаліста, мережа повинна бути простою в управлінні і підтримці. Для цього конфігурації мають бути стандартними і надійними, а обладнання має бути зручним для керування, використовуючи веб-інтерфейс або знайомий інтерфейс, наприклад Cisco IOS для професійного управління або спрощені веб-смарт пристрої. Документація щодо мережі, включаючи схеми та налаштування, має зберігатися для передачі в сервісну організацію або адміністратору за потреби.На основі цих вимог у наступних підрозділах буде здійснено вибір конкретних моделей обладнання та розроблено мережеву структуру (схему), після чого описано процес налаштування мережі згідно з поставленими цілями.

Сформуємо узагальнений перелік функціональних вимог до мережі магазину та її характеристик:

Тип мережі: локальна мережа (LAN) всередині одного приміщення (офіс + торговий зал). За територіальною класифікацією - це LAN, яка приєднується до глобальної мережі (Інтернет) через одного провайдера.

Кількість вузлів: 20 стаціонарних клієнтських пристроїв (ПК), 1 сервер, 1-2 мережевих принтери (не згадувались раніше, але припустимо, що може бути принтер/МФУ в маркетингу чи у директора), мережеві камери (можливо 2-3, якщо є система відеонагляду), 1 точка доступу Wi-Fi. Загальна кількість IP-пристроїв

може сягати 25-30 (враховуючи мобільні гаджети клієнтів при підключенні до Wi-Fi).

Топологія: фізична зірка (централізований комутатор у серверній, до нього підведені кабелі від усіх кімнат). Логічна - поділ на декілька VLAN (за функціями: наприклад, VLAN1 - управління/дирекція, VLAN2 - офіс (маркетинг, продаж), VLAN3 - клієнтська підтримка, VLAN10 - гостьовий WiFi, VLAN99 - серверний/інфраструктура). Маршрутизація між VLAN виконується на маршрутизаторі (router-on-a-stick).

Пропускна здатність: всі основні з'єднання - Gigabit Ethernet (1000 Мбіт/с). Канал до Інтернету від провайдера, припустимо, 100 Мбіт/с (симетричний або 100/50). Такої швидкості достатньо для потреб магазину (одночасний веб-серфінг, відеоконференція чи IP-телефонія, синхронізація даних тощо). Внутрішня мережа гігабітна потрібна для швидкої роботи з сервером (наприклад, відкриття великих файлів, резервне копіювання по мережі).

Адресація: використовуємо приватні IPv4 адреси. Оскільки планується розподіл на ~5 VLAN, кожному VLAN призначимо окремю підмережу класу C (маска /24). Це спрощує схему: в кожному сегменті можна мати до 254 адрес, що з надлишком покриває потреби (20-30 пристроїв). Конкретний пул адрес оберемо з діапазону 192.168.X.0/24.

Маршрутизатор матиме по одному IP в кожній підмережі (шлюз 1). Всі ці підмережі транслюватимуться через NAT на єдину публічну IP для виходу в Інтернет.

Динамічна адресація: впровадимо DHCP-сервер для автоматичної видачі адрес клієнтам у кожному VLAN. Зручніше налаштувати DHCP на самому маршрутизаторі (Cisco IOS підтримує кілька DHCP-пулів для різних інтерфейсів/VLAN). DHCP на маршрутизаторі роздаватиме IP, маску, шлюз (адресу маршрутизатора) та адреси DNS-серверів (можна вказати DNS від Google 8.8.8.8 або провайдера). Серверу, мережевим принтерам та точці доступу задаватимемо статичні адреси (щоб вони були відомі й постійні). Приклад: сервер

- 192.168.50.10, принтер - 192.168.20.100, точка доступу - 192.168.40.2 (в гостьовій підмережі).

Маршрутизація: використаємо статичну маршрутизацію на єдиний вихід. Маршрутизатор знає про всі внутрішні мережі (вони підключені як його інтерфейси). Додатково буде додано статичний маршрут “0.0.0.0/0” (default route) на інтерфейс провайдера. Якщо провайдер видає динамічну адресу, можна налаштувати отримання шлюзу через DHCP клієнт на зовнішньому інтерфейсі. Внутрішніх динамічних протоколів маршрутизації (OSPF, EIGRP) не потрібно через простоту топології.

Безпека: як обумовлено, VLAN і ACL. На маршрутизаторі: access-list, що забороняє трафік з гостьового VLAN до внутрішніх (дозволяє тільки до Інтернету). Можна це реалізувати, наприклад, через правила на інтерфейсі гостьового VLAN: permit any to internet, deny any to private ranges. Інші VLAN між собою можна не блокувати (або обмежити вибірково, якщо потрібно). Адміністративний доступ до обладнання - тільки з мережі адміністрації (директор/секретар/сервер) і по захищеному протоколу (SSH на маршрутизатор, HTTPS на комутатор). Wi-Fi гостьовий із WPA2-PSK, складним паролем, який відомий лише персоналу та надається клієнтам при потребі.

Моніторинг і управління: комутатор і маршрутизатор підтримують протокол SNMP для моніторингу (можна налаштувати якщо буде кому слідкувати). У невеликому магазині це необов’язково. Достатньо можливості зайти на обладнання через консоль/SSH для діагностики. Логи (Syslog) з маршрутизатора та комутатор

3 ПРАКТИЧНА ІМПЛЕМЕНТАЦІЯ МЕРЕЖІ

3.1 Вибір обладнання та програмного забезпечення

На основі визначених потреб потрібно визначити перелік необхідного мережевого обладнання для реалізації проекту, а також виберемо програмне забезпечення (системне і прикладне), яке буде задіяне. Основні критерії вибору - відповідність вимогам по продуктивності, надійності, сумісність, а також вартість, оскільки для магазину важливо залишатися в межах виділеного бюджету на IT та потрібне обласднання для мережі.

Комутатор (Switch). Потрібен керований комутатор рівня 2 з підтримкою VLAN і бажано Gigabit Ethernet на всіх портах. Орієнтовна кількість портів - 24 (виходимо з 20 активних пристроїв + запас на розширення і підключення точок доступу, камер тощо). Оптимальним вибором є, наприклад, Cisco Catalyst 2960 на 24 порти 10/100/1000 або його аналог із серії Cisco Business (SG300/350) для малого бізнесу. Такі комутатори підтримують VLAN, мають просте управління через web або CLI, надійні у роботі. Альтернативно можна розглянути моделі від TP-Link (серія JetStream), D-Link (DES-1210) або MikroTik CRS - вони можуть бути дешевшими, але для уніфікації беремо Cisco, адже і маршрутизатор планується Cisco (що спростить налаштування у Packet Tracer і є стандартом де-факто). 24-портовий комутатор дозволить підключити всі пристрої в одну «зірку». Гігабітна швидкість забезпечить швидку передачу між сервером та клієнтами. Керованість потрібна для налаштування VLAN. Комутатор встановимо в серверній шафі, недалеко від серверу і маршрутизатора.

Маршрутизатор (Router). Необхідний маршрутизатор для підключення LAN до Інтернету і маршрутизації між VLAN. У Cisco Packet Tracer доступні моделі ISR (Integrated Services Router) серій 1841, 2811, 2911, тощо. Для наших потреб достатньо 2-4 портового маршрутизатора з підтримкою NAT, ACL і інтерфейсом FastEthernet або краще GigabitEthernet для підключення до комутатора. Візьмемо, наприклад, Cisco 2811 ISR: він має два вбудованих FastEthernet порти, які можна

використати як «LAN» і «WAN». Якщо потрібні додаткові підінтерфейси для VLAN, 2811 підтримує субінтерфейси 802.1Q на порті (router-on-a-stick). WAN-порт підключимо до модему провайдера (припустимо Ethernet до DHCP). LAN-порт trunk до комутатора. Також 2811 може виступати DHCP-сервером. Альтернативно міг би бути сучасніший маршрутизатор, але навіть старий 2811 (до 100 тис. пакетів/с) впорається з навантаженням малого офісу.

Маршрутизатори Cisco забезпечують надійну роботу, гнучке налаштування. На ньому реалізуємо NAT/PAT, щоб локальна мережа виходила в Інтернет під одним зовнішнім IP. Маршрутизатор також дозволить впровадити базові правила брандмауера (ACL) між VLAN та зовнішньою мережею.

Точка доступу Wi-Fi. Вибираємо точку доступу стандарту не нижче 802.11n (краще ac Wave2, щоб підтримувати сучасні пристрої і більшу швидкість). З огляду на невелику площу магазину, достатньо 1 точки доступу, встановленої у центрі виставкової зали на стелі. Наприклад, Cisco Aironet 1830 чи Cisco WAP150 (серія для малого бізнесу) з підтримкою кількох SSID/VLAN. Вони можуть працювати автономно (standalone AP). Інший варіант - точка доступу від Ubiquiti (UniFi AP) або TP-Link EAP, які теж дають потрібний функціонал. Ми розглядаємо Cisco для узгодженості.

Одна точка доступу з радіусом дії 30 м покриє виставкову залу і, можливо, прилеглі офіси. Якщо сигнала не вистачить до далеких кімнат (на кшталт серверної), це несуттєво, бо там Wi-Fi не потрібен. Гостьова мережа Wi-Fi буде транслюватися з цієї точки доступу, ізольовано (налаштуємо VLAN для SSID). Пропускної здатності точки (до 300 Мбіт/с для 802.11n або до 1.3 Гбіт/с для 802.11ac) вистачить для одночасних підключень клієнтів (навіть якщо 10 клієнтів, кожен зможе отримати декілька десятків Мбіт/с).

Можливими варіантами серверу є брендований сервер рівня HPE ProLiant ML30 (вежовий сервер початкового рівня) або збірка на базі продуктивного ПК (наприклад, процесор Intel Xeon E3 або Core i7, 16 GB RAM, 2×HDD 4TB у RAID1 для надійності, ОС Windows Server 2019 Standard або Ubuntu Server). Сервер підключається до мережі через гігабітний порт .

Сервер виконуватиме роль центрального сховища даних та, можливо, серверу додатків. Якщо встановити Windows Server, на ньому можуть працювати служби: Active Directory (якщо потрібно централізоване управління користувачами), файл-сервер (папки для різних відділів), SQL Server (для бази даних товарів/клієнтів), DHCP і DNS (альтернатива реалізації на маршрутизаторі). Оскільки маршрутизатор Cisco також може роздавати DHCP, остаточне рішення - що саме робить сервер, а що - маршрутизатор - приймається з міркувань зручності. У малих мережах часто роутер займається мережею (DHCP/NAT), а сервер - лише даними.

Модем/ONU провайдера: якщо Інтернет надається по оптоволокну чи xDSL, знадобиться відповідний модем/медіаконвертер від провайдера. Він підключається до WAN-порту маршрутизатора. В нашій схемі цей елемент є, але він поза сферою налаштування (налаштований провайдером). У Cisco Packet Tracer для спрощення використовується символ Cloud (хмара) або модуль Serial0/ADSL для з'єднання з іншим роутером-симуляцією інтернет.

Джерело безперебійного живлення (UPS): не мережевий пристрій, але важливо, що в серверну кімнату ставиться UPS, до якого підключено сервер, комутатор, маршрутизатор. Це забезпечить 10-15 хвилин роботи при зникненні електрики, дасть змогу коректно вимкнути сервер і збереже роботу мережі при коротких збоях.

Структурована кабельна система: UTP кат.6 кабелі від кожної кімнати до серверної, патч-панель, комутаційні шнури. Для ~20 підключень буде одна 24-портова патч-панель, з'єднана з комутатором. Кабелі прокладаються в коробах або під підлогою/над стелею. Максимальна довжина кабелю до найдальшої точки (можливо, виставкова зала) 50 м, що в межах норми Ethernet.

ОС і серверні служби: на сервері встановлено Windows Server 2019. Налаштовано роль файлового сервера (спільні папки з правами доступу по відділах), можливо роль DHCP-сервера (альтернативно роутер, як вирішено), DNS-сервер (кешуючий або для локального домену, якщо впроваджено AD). Якщо використовується база даних - Microsoft SQL Server Express (для невеликої бази).

Для резервного копіювання - штатні засоби Windows Server Backup або стороння утиліта (Acronis, Veeam).

Клієнтські ОС: Windows 10/11 на робочих ПК, відповідно. На них стандартний набір програм: офісний пакет, клієнт електронної пошти, веб-браузер, ПО для доступу до корпоративної БД (якщо є окремий додаток). Також встановлено антивірус.

Мережеве ПЗ: на маршрутизаторі - Cisco IOS 15.x (в симуляції Packet Tracer доступний інтерфейс команд). Для управління комутатором - теж Cisco IOS (через командний рядок або простий web-інтерфейс). Адміністрування може виконуватися через Telnet/SSH (налаштуємо SSH на маршрутизаторі).

Cisco Packet Tracer: використовується в рамках виконання дипломної роботи для віртуального моделювання мережі. Версія PT 8.2 (умовно). Всі скриншоти та схеми далі отримані саме з цього симулятора.

Вибране апаратне та програмне забезпечення задовольняє вимоги магазину. У наступних підрозділах буде представлено схема мережі та детальний опис її конфігурування.

3.2 Підбір оптимального обладнання відповідно до потреб магазину

На цьому етапі проектування створюється фізична схема мережі: розташування пристроїв у приміщеннях та кабельні з’єднання між ними. За основу беремо план приміщення (рис. 3.1) і накладаємо на нього мережеві підключення: кожна кімната обладнана як мінімум одним мережевим портом (RJ-45 розеткою), який з’єднаний кабелем категорії 6 зі шкафом в серверній кімнаті. У серверній встановлено комутаційний щит (патч-панель) та 24-портовий комутатор. Всі кабелі від розеток заведені на патч-панель і короткими патч-кордами підключені до портів комутатора. Маршрутизатор розташований поруч з комутатором і з’єднаний з ним одним патч-кордом (т.зв. uplink від LAN-порту маршрутизатора до порту комутатора; цей порт комутатора буде налаштований як trunk для VLAN). Інший інтерфейс маршрутизатора підключено до пристрою провайдера (модему) - цей

кабель йде до вводу інтернет-лінії. Точка доступу Wi-Fi закріплена на стелі виставкової зали, до неї прокладений кабель, що також підключений до комутатора (на окремий порт, конфігурований як trunk або access у VLAN гостьової мережі - залежно від моделі ТД). Сервер підключений безпосередньо до комутатора патч-кордом (його розетка може бути теж заведена на патч-панель або він стоїть близько і кабель йде прямо).

Отримана фізична топологія - зірка з одним комутатором у центрі. Така структура відповідає стандартній архітектурі Ethernet LAN у межах одного поверху/будівлі. Для наочності на рис. 3.1 нижче наведено логічну схема мережі, відображену в Cisco Packet Tracer:

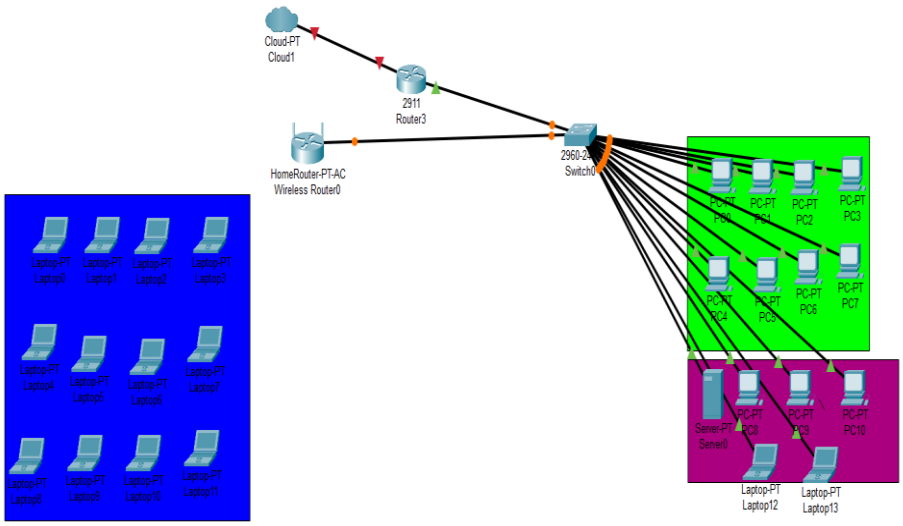


Рис. 3.1. Логічна схема мережі магазину

Маршрутизатор з’єднаний з «хмарою» (Cloud) або інтернет-мережею для забезпечення зовнішнього зв’язку. Кожен сегмент має власну IP-підмережу (192.168.1.0, 192.168.2.0 і т.д. на прикладі), що аналогічно запланованим нами 192.168.10.0/20.0/30.0/40.0 мережам.

На рис.3.1 видно, що кожен відділ підключений до окремого порту (або групи портів) комутатора, і їх трафік розділено на рівні VLAN. Фізично всі ці пристрої

з’єднані одним комутатором, але завдяки VLAN ізольовані в різних широкомовних доменах. Маршрутизатор (позначений як R1) має по одному логічному інтерфейсу на кожен VLAN (в Packet Tracer вони відображаються як sub-interface, напр. Fa0/0.1, Fa0/0.2 і т.д., або як окремі інтерфейси якщо б були порти). Саме маршрутизатор зв’язує ці VLAN між собою і з Інтернетом.

Розміщення обладнання в приміщенні магазину:

Серверна (службове приміщення): тут встановлено комутатор маршрутизатор, сервер, UPS, патч-панель. Бажано використати закриту телекомунікаційну шафу для безпеки і порядку. Усі з’єднання сконцентровані тут.

Виставкова зала: комп’ютери, що стоять на вітрині, підключені кабелями до найближчих розеток. Точка доступу Wi-Fi прикріплена на стелю, кабель від неї йде теж до розетки. Якщо комп’ютери виставкової зали планується переключати між різними демонстраційними режимами, їх теж можна підключити по Wi-Fi, але краще провідь для стабільності (отже, 1-2 розетки на зал, з можливістю підключити по черзі різні ноутбуки).

Кабінети директора, секретаря, відділи: в кожному кімнаті зазвичай 1-2 розетки, до яких підключені ПК, IP-телефон або принтер. Якщо пристроїв кілька, можна поставити маленький некерований свіч на 5 портів локально, але це небажано (краще протягнути окремі лінії на кожне робоче місце). Припустимо, що зроблено якісно - тобто кожен ПК має пряме підключення до головного комутатора.

Охорона: 1 розетка для ПК охоронця, 1 для можливої IP-камери (або камера живиться PoE від комутатора - тоді потрібен PoE комутатор або інжектор). В специфікаціях комутатор Cisco 2960 може мати PoE версію 2960-24PC, що забезпечує живлення PoE на 8-12 портів - це вирішило б питання камер і точки доступу. Додамо припущення, що модель комутатора підтримує PoE, щоб уникнути окремих інжекторів.

Принтери: мережевий принтер, наприклад, в маркетинговому відділі - теж через локальну розетку в тій кімнаті. Йому призначено IP і він доступний іншим по мережі.

Кабельні траси: невеликий офіс, укладено кабель-канали вздовж стін, через які проходять кабелі UTP. Виставкова зала до серверної - відстань ~15-20 м, інші кімнати ще менше. Перешкод для прокладки немає.

Така фізична і логічна прив’язка забезпечує, що кожен відділ потрапляє у свій VLAN автоматично через порт. У разі перестановки відділів (наприклад, маркетинг переїде в іншу кімнату), достатньо переналаштувати відповідні порти комутатора під потрібний VLAN.

Підсумовуючи, фізична схема реалізована гнучко і з запасом. Наступним кроком є детальніше описати логічну структуру мережі - тобто як саме розподілені адреси між VLAN, які мережеві налаштування зроблені.

3.3 Логічна структура мережі (адресація, VLAN, маршрутизація)

Логічна структура описує, як мережа поділена на сегменти і як організовано взаємодію між ними. У нашому проекті логічна структура складається з декількох віртуальних локальних мереж (VLAN) та відповідних їм IP-підмереж.

Маршрутизатор забезпечує маршрутизацію між цими підмережами та вихід у глобальну мережу.

Як зазначено раніше, виділяються такі VLAN і мережі:

Таблиця 3.1 - Відповідність назви vlan до номеру

Назва Vlan	Номер Vlan
Pc-pc	2
laptop	3
pc	4

Таблиця 3.2 – Належність портів до Vlan

Назва пристроїв	Порти	Vlan

Switch0	Fa0/1, Fa0/2, Fa0/3, Fa0/4, Fa0/5, Fa0/6, Fa0/7, Fa0/8, Fa0/9, Fa0/10, Fa0/11, Fa0/12, Fa0/13, Fa0/15	cameras
	Fa0/14	pc
Switch1	Fa0/1, Fa0/2, Fa0/3, Fa0/4, Fa0/5	cameras
	Fa0/6, Fa0/7	cashregisters
Wireless Router0	Fa0/1, Wireless, Wireless	guests

DHCP тут не потрібний, оскільки 1 сервери завжди статичні. Цей VLAN може використовуватись суто для ізоляції сервера. Можливо, ми могли б об’єднати сервер із VLAN10 (адмін) без великого ризику, але виділення окремо дозволяє чітко керувати доступом до сервера.

Така адресна схема узгоджується: мережі розрізняються у третьому октеті (10,20,30,40,50). Маска 255.255.255.0 (/24) у кожній дає до 254 хостів, що з надлишком покриває потреби (використовуємо <10% простору кожної). Перевага окремих мереж - можна легко писати ACL, наприклад “permit 192.168.10.0/24 to 192.168.50.10 tcp 1433” (доступ адмін-сегменту до SQL-сервера), або “deny 192.168.40.0/24 to any 192.168.0.0/16” (блок гостьового до всіх приватних).

DHCP-налаштування: На маршрутизаторі Cisco (R1) створюються пули DHCP для кожної внутрішньої мережі.

```
Router>
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int g0/0
Router(config-if)#ip add 192.168.1.1 255.255.255.0
Router(config-if)#no shut
Router(config-if)#exit
Router(config)#ip dhcp pool MY_STORE
Router(dhcp-config)#network 192.168.1.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.1.1
Router(dhcp-config)#dns-server 192.168.1.1
Router(dhcp-config)#
```

Рисунок 3.1 - Налаштування DHCP на роутері

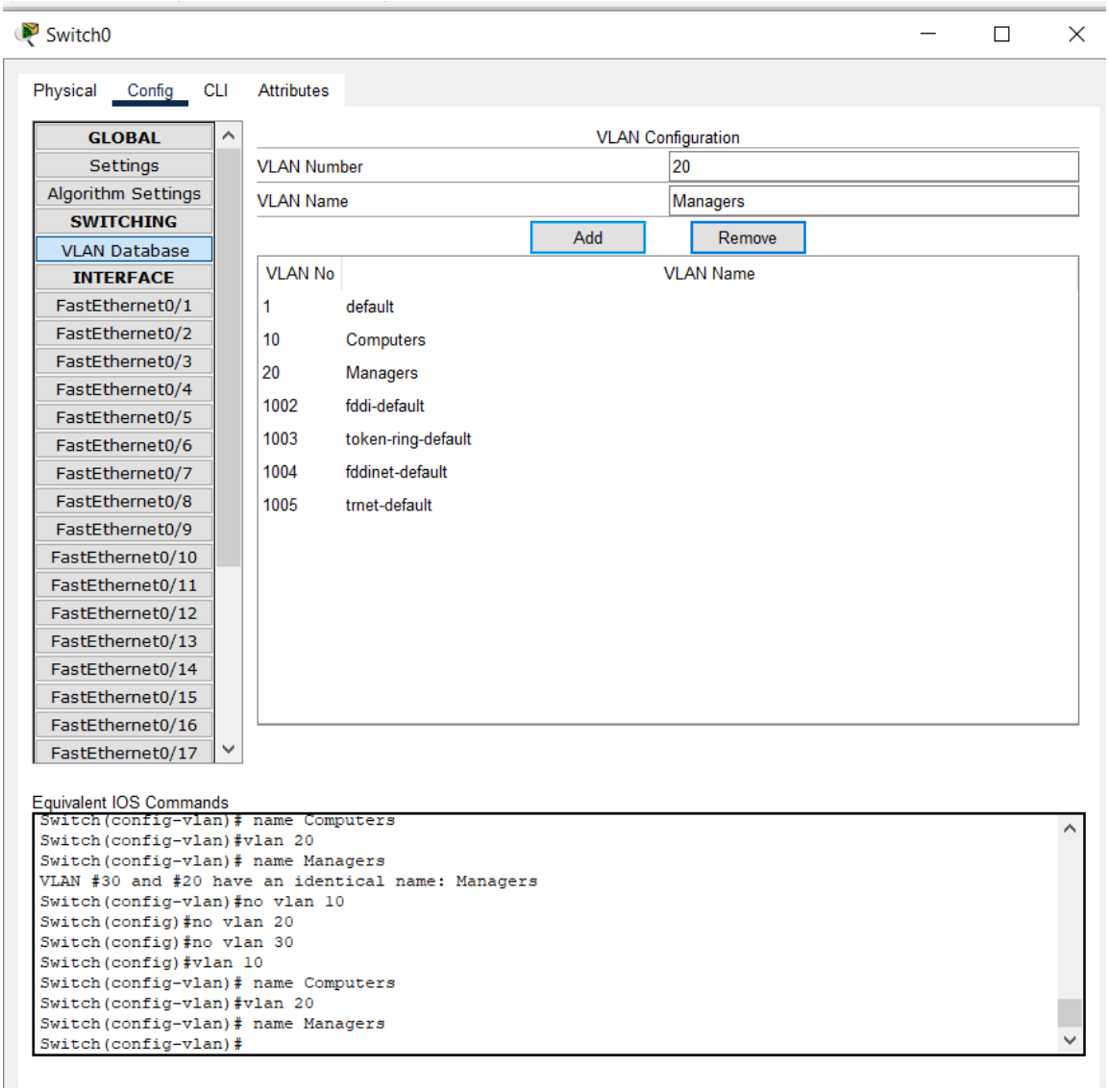


Рисунок 3.2 - Створення VLAN

Цим забезпечимо, що всі підрозділи ходять у Інтернет під однією IP. Зовні ініційовані з’єднання відхиляються, якщо немає відповідного rule (а у нас немає, тому зовні ніхто не достукається до внутрішніх - це плюс безпеки). Якщо потрібно, наприклад, дозволити директору з дому зайти на сервер - довелося б налаштувати VPN або статичний NAT для RDP-порту, але в рамках задачі не потрібно.

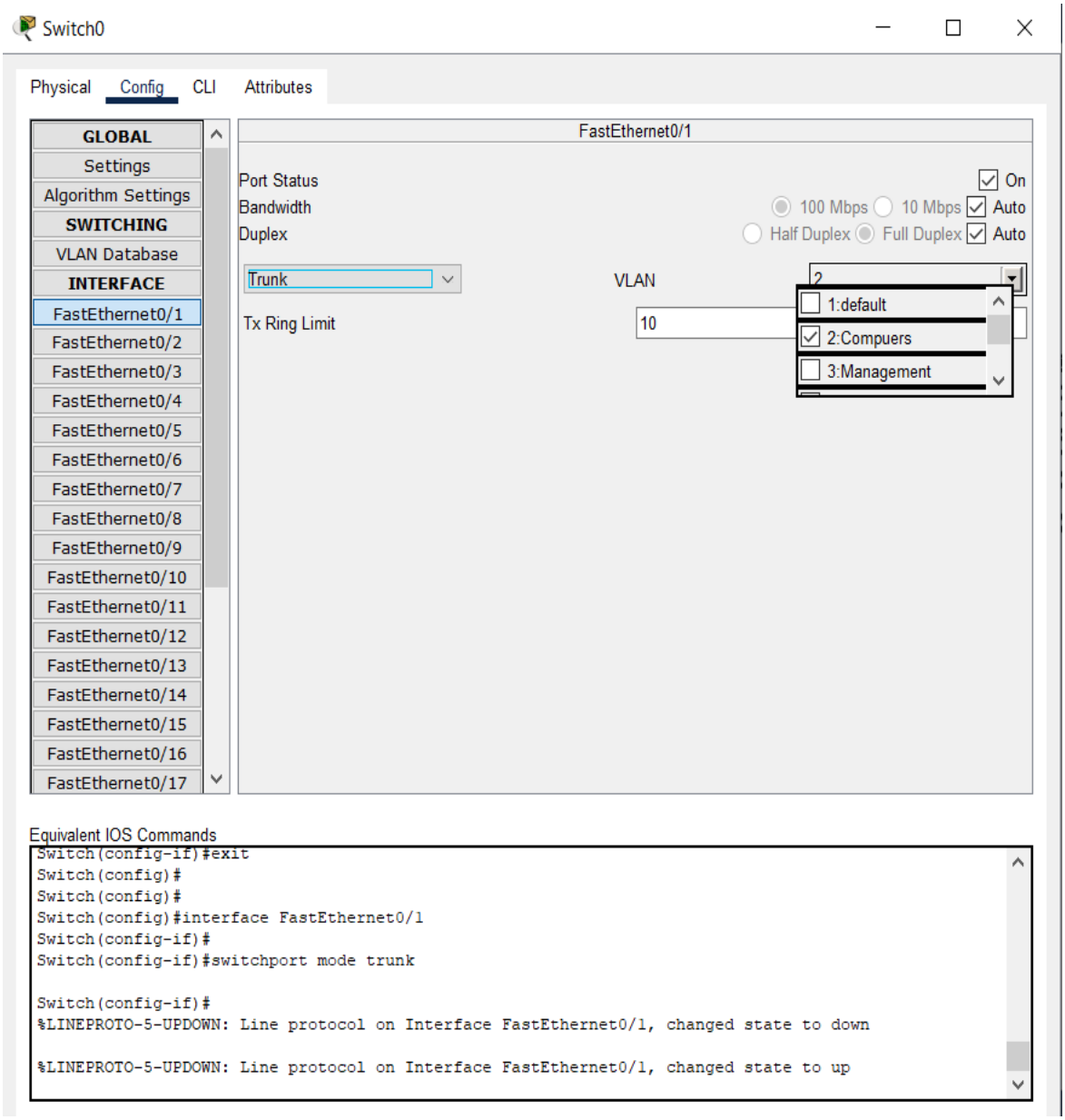


Рисунок 3.3 - Підключення портів до VLAN

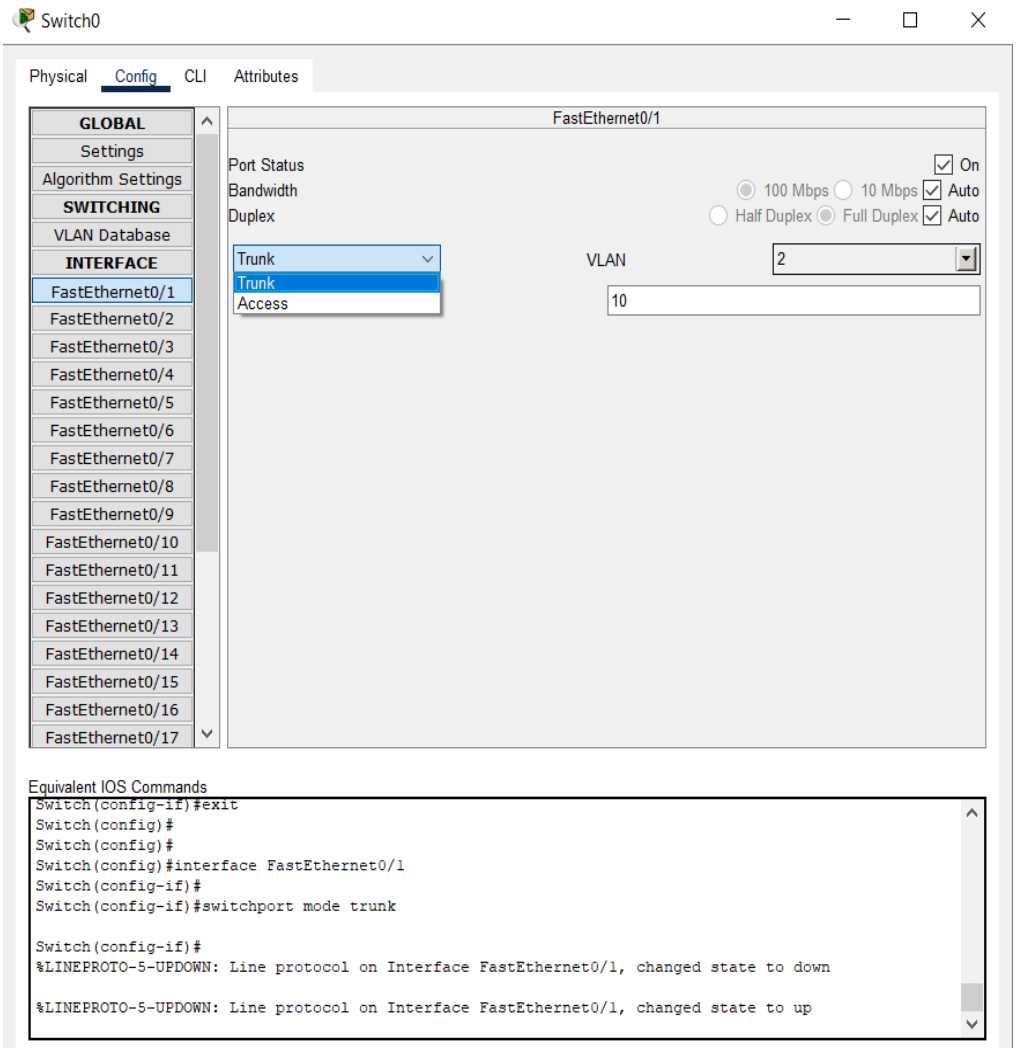


Рисунок 3.4 – Встановлення типу каналу

Більшість ПК будуть отримувати IP автоматично (DHCP). В Packet Tracer за замовчуванням вони DHCP запит зроблять, якщо у них в config стоїть DHCP.

На кожному PC заходимо Desktop > IP Configuration > Set DHCP. Відбувається DHCP Discover, і якщо все ок - вони отримують належний IP, маску, шлюз, DNS.

Потрібно переконатися, що кожен ПК опинився у своїй мережі. Напр., PC-Dir повинен отримати 192.168.10.x, PC-Marketing - 192.168.20.x, тощо. У разі неправильного VLAN, DHCP може не відповісти. Це спосіб перевірки VLAN: якщо ПК отримав IP, значить VLAN assignment порту вірний.

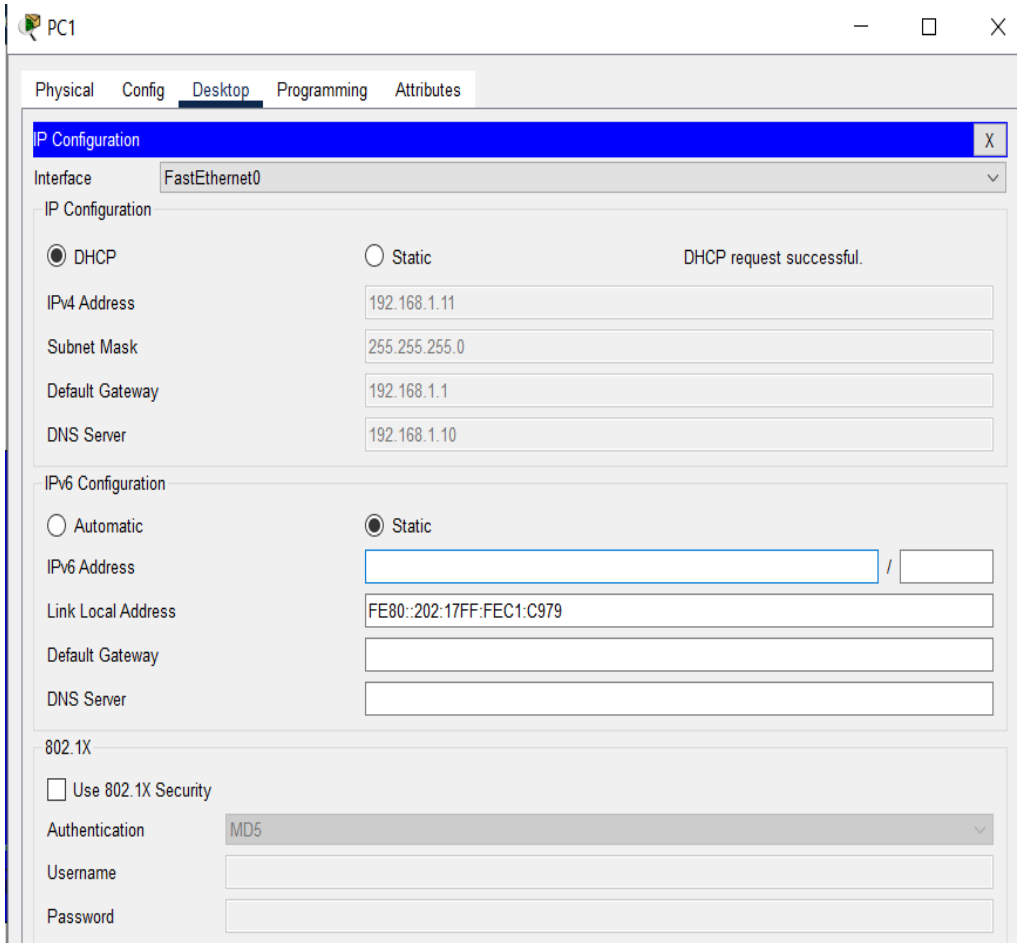


Рисунок 3.5 – Використання DHCP адреси для камери відеоспостереження

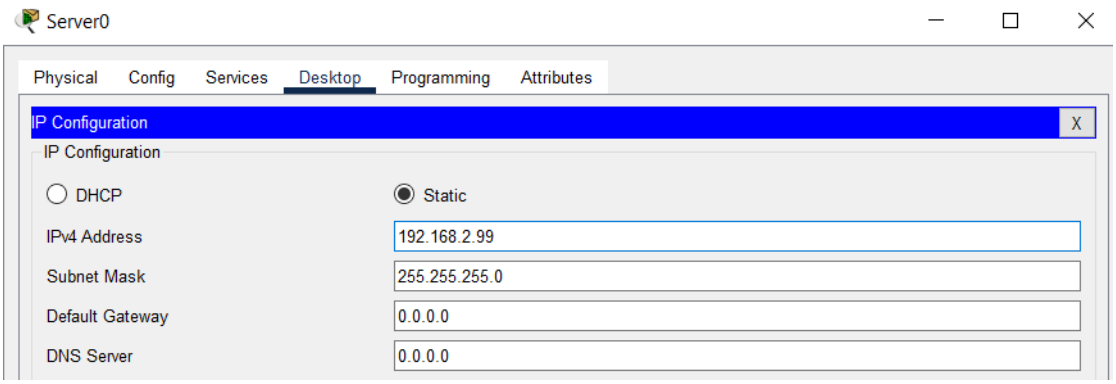


Рисунок 3.6 – Використання статичної адреси сервером

Для важливих (директор) - можна вручну задати IP (192.168.10.2). Але поки що не критично, хай буде DHCP.

Щоб налаштувати маршрутизатор (див. рисунок 3.7) для коректної роботи в мережі, спочатку необхідно призначити IP-адреси його фізичним інтерфейсам. Для цього в режимі глобальної конфігурації виконується перехід до відповідного порту

за допомогою команди interface, після чого вказується назва інтерфейсу та його номер (наприклад, GigabitEthernet0/1). Далі задається IP-адреса та маска підмережі командою ip address, і завершальним етапом є активація інтерфейсу через no shutdown.

У випадку, коли на одному фізичному інтерфейсі необхідно організувати кілька логічних підключень наприклад, для підтримки різних VLAN створюються сабінтерфейси. Для цього використовується команда interface із зазначенням інтерфейсу та логічного номера сабінтерфейсу, наприклад: GigabitEthernet0/1.10. Далі на сабінтерфейсі виконується прив'язка до VLAN за допомогою команди encapsulation dot1Q, де вказується відповідний ідентифікатор VLAN.

Після виконання налаштувань важливо чітко розподілити ролі кожного інтерфейсу: одні з них будуть слугувати для з'єднання з локальною мережею (внутрішні інтерфейси), інші — для підключення до зовнішніх мереж, наприклад, до Інтернету. Такий поділ забезпечує коректну маршрутизацію трафіку та послідовне функціонування всієї мережевої структури.Крок 10: Тестування мережі в симуляції.

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int g0/0.20
Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip address 192.168.20.1 255.255.255.0
Router(config-subif)#no shut
Router(config-subif)#
```

Рисунок 3.7 – Увімкнення портів на маршрутизаторі, встановлення IP-адреси

Після повної конфігурації проводимо тестування основних функцій:

Перевірка IP-зв'язності всередині LAN: спробуємо "ping" між кількома вузлами різних VLAN. Наприклад, з ПК маркетингу (192.168.20.x) запінгувати сервер 192.168.50.10 - повинно бути успішно (у ACL нічого не блокує це). З ПК маркетингу пінгувати ПК підтримки (192.168.30.x) - теж мало б працювати (якщо не ввели ніяких deny для внутрішніх). З ПК гостя (192.168.40.x) спробувати пінг 192.168.50.10 - має не проходити (timeout), оскільки ACL.

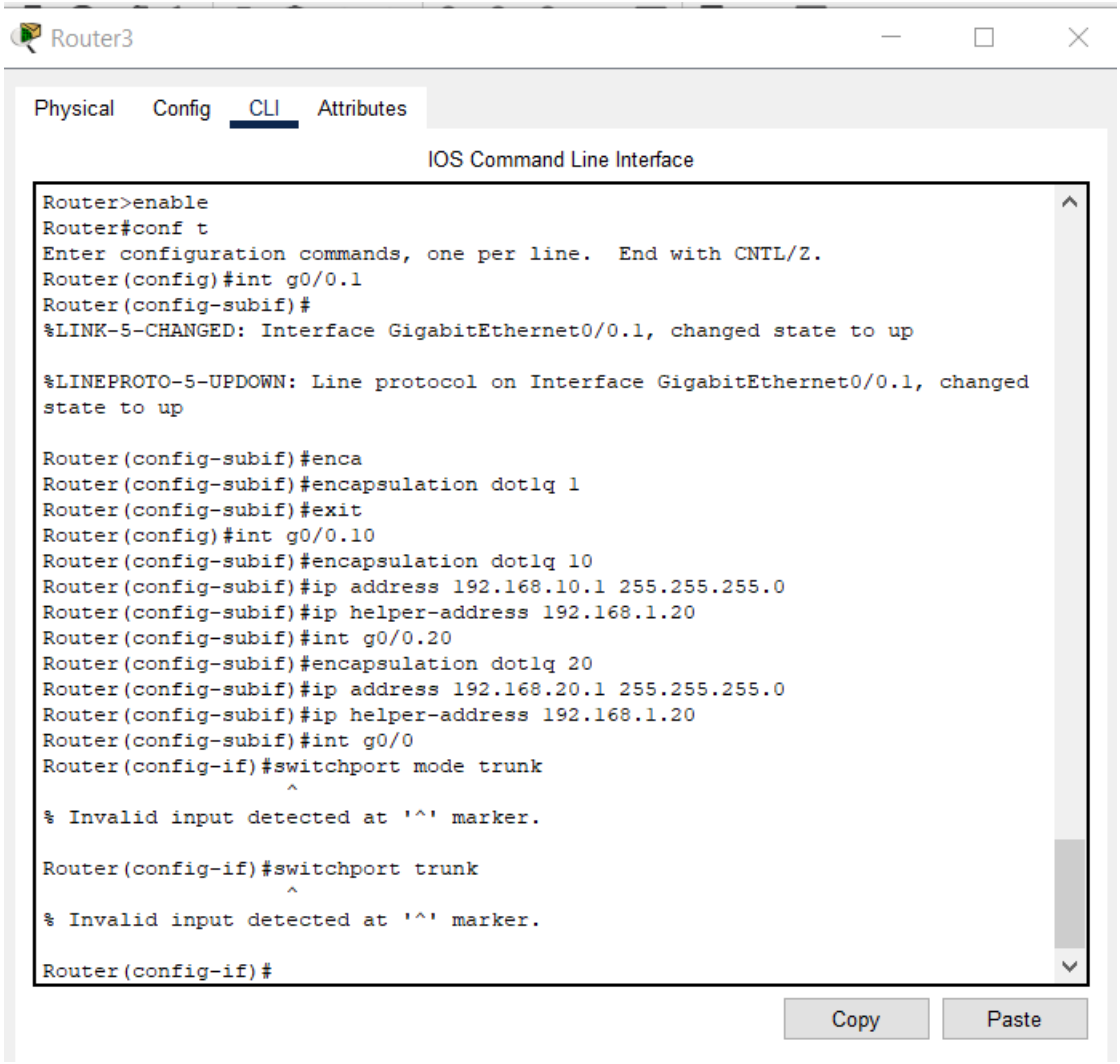


Рисунок 3.8 – Створення сабінтерфейсів

Перевірка виходу в Інтернет: з якого-небудь ПК (скажімо маркетинг) пінгуємо адресу на боці провайдера. У нашій схемі ISP-Router Fa0/0 = 200.200.200.1. Тому з PC-Marketing: ping 8.8.8.8. В Packet Tracer, якщо немає реального інтернет, можна зробити так: на ISP-Router налаштуємо Loopback interface 8.8.8.8 255.255.255.255 (для імітації DNS-сервера).

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int g0/0
Router(config-if)#no ip add
Router(config-if)#no shut
Router(config-if)#int g0/0.10
Router(config-subif)#encapsulation dot1q 10
Router(config-subif)#ip add 192.168.10.1 255.255.255.0
Router(config-subif)#description vlan10
Router(config-subif)#int g0/0.20
Router(config-subif)#encapsulation do1q 20\
                                    ^
% Invalid input detected at '^' marker.

Router(config-subif)#encapsulation dot1q 20\
                                        ^
% Invalid input detected at '^' marker.

Router(config-subif)#encapsulation dot1q 20
Router(config-subif)#ip add 192.168.20.1 255.255.255.0
Router(config-subif)#description vlan20
Router(config-subif)#int g0/0.30
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.30, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.30, changed state to up
encapsulation dot1q 30
Router(config-subif)#ip add 192.168.30.1 255.255.255.0
Router(config-subif)#description vlan30
Router(config-subif)#
```

Рисунок 3.9 – Налаштування підмереж та IP-адрес на роутері

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name Support
Switch(config-vlan)#vlan 20
Switch(config-vlan)#name Managers
Switch(config-vlan)#vlan 30
Switch(config-vlan)#name Exhibition
Switch(config-vlan)#exit
Switch(config)#
```

Рисунок 3.10 – Визначення VLAN

У Packet Tracer всі налаштування можна зберегти у .pkt файл (ми це зробимо). В реальній мережі - виконуємо copy run start на кожному Cisco пристрої, щоб при перезавантаженні налаштування не зникли. Сервер і ПК не потребують спец. збереження (їх конфіги статичні).

```
Switch(config)#int g0/1
Switch(config-if)#sw mode trunk

Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

Switch(config-if)#int range f0/1-8
Switch(config-if-range)#sw mode access
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#int range f0/10-14
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 20
Switch(config-if-range)#int g0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 30
Switch(config-if)#
```

Рисунок 3.11 – Налаштування trunk режиму для обробки трафіку з декількох VLAN та присвоювання портів на до інтерфейсів

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip dhcp pool vlan10
Router(dhcp-config)#network 192.168.10.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.10.1
Router(dhcp-config)#dns-server 8.8.8.8
Router(dhcp-config)#exit
Router(config)#ip dhcp excluded-address 192.168.10.1
Router(config)#ip dhcp excluded-address 192.168.10.255
Router(config)#ip dhcp pool vlan20
Router(dhcp-config)#network 192.168.20.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.20.1
Router(dhcp-config)#dns-server 8.8.8.8
Router(dhcp-config)#exit
Router(config)#ip dhcp excluded-address 192.168.20.1
Router(config)#ip dhcp excluded-address 192.168.20.255
Router(config)#ip dhcp excluded-address 192.168.20.100
Router(config)#ip dhcp pool vlan30
Router(dhcp-config)#network 192.168.30.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.30.1
Router(dhcp-config)#dns-server 8.8.8.8
Router(dhcp-config)#exit
Router(config)#
Router(config)#ip dhcp excluded-address 192.168.30.1
Router(config)#ip dhcp excluded-address 192.168.30.2
Router(config)#ip dhcp excluded-address 192.168.30.255
Router(config)#
```

Рисунок 3.12 – Налаштування dhcp для VLAN на роутері

Рисунок 3.13 демонструє успішну перевірку отримання IP-адреси клієнтським комп’ютером у VLAN через DHCP. Виведено конфігурацію мережевого інтерфейсу, яка підтверджує, що IP-адреса, маска підмережі та шлюз були призначені автоматично з відповідного DHCP-пулу. Це свідчить про

правильну роботу служби DHCP та коректне функціонування VLAN. Наявність VLAN дозволяє не лише оптимізувати трафік, але й підвищити рівень безпеки за рахунок логічного розмежування доступу. Кожен VLAN може мати власні політики безпеки та фільтрування, що знижує ризик несанкціонованого доступу до чутливої інформації. У поєднанні з міжмережевою маршрутизацією це створює надійну архітектуру.

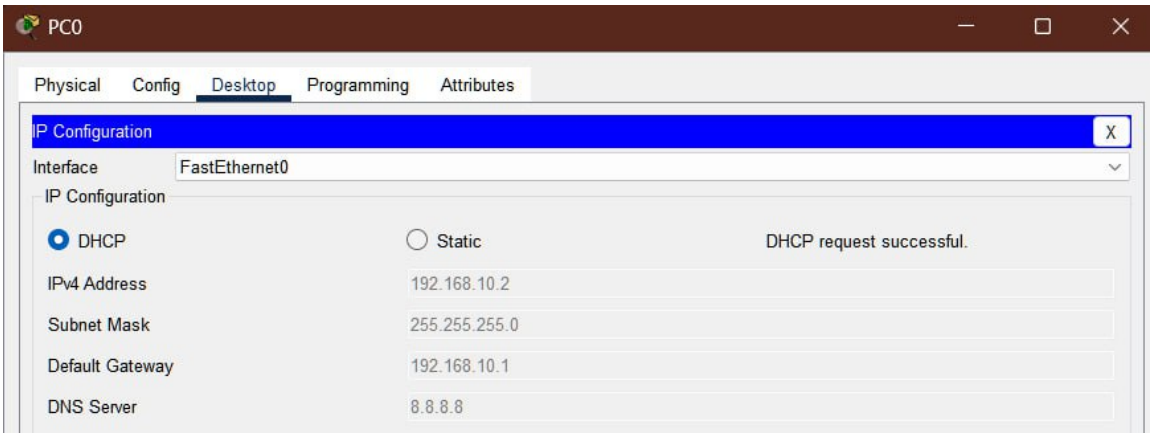


Рисунок 3.13 Перевірка отримання IP-адреси за DHCP

На рисунку 3.14 представлено конфігурацію сервера зі статично призначеною IP-адресою. У параметрах мережевого інтерфейсу задано IP-адресу, маску підмережі, шлюз за замовчуванням та DNS-сервер. Статична адресація є доцільною для серверів, до яких необхідно мати постійний доступ з інших частин мережі, оскільки вона забезпечує стабільність з'єднання та спрощує адміністрування мережевої інфраструктури.

Призначення статичної IP-адреси серверу є важливим кроком у процесі організації стабільної та передбачуваної інфраструктури, оскільки сервери зазвичай надають постійні послуги (наприклад, файловий доступ, бази даних, внутрішній веб-сайт тощо), і їхня адреса має залишатися незмінною для всіх клієнтів. Крім того, це дозволяє адміністратору мережі ефективно налаштовувати правила маршрутизації, NAT, фаєрволи та інші сервіси без ризику, що IP-адреса зміниться після перезавантаження або збою.

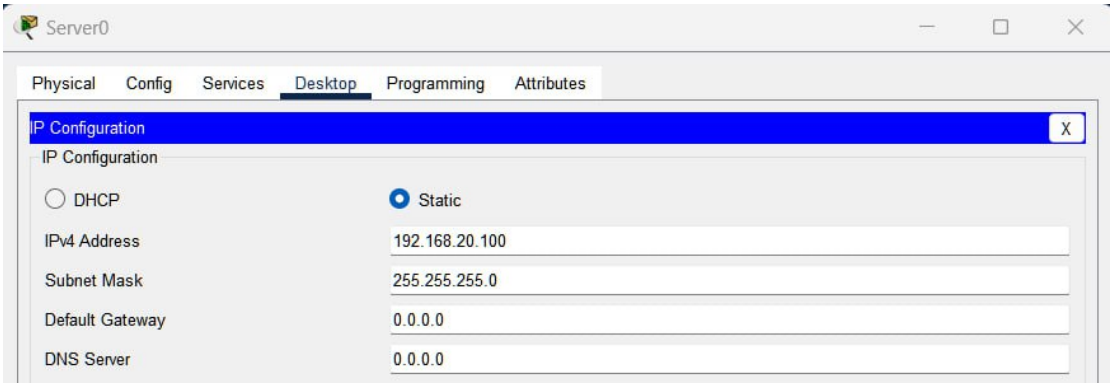


Рисунок 3.14 – Налаштування сервера зі статичною IP-адресою

На рисунку 3.15 показано процес додавання сервера до певної підмережі. Сервер отримує IP-адресу з відповідного діапазону, що відповідає налаштованому VLAN або логічному сегменту. Це дозволяє забезпечити логічну організацію мережі, ізоляцію трафіку та централізований доступ до серверних ресурсів.

Розміщення сервера в окремій підмережі дає змогу досягти вищого рівня організації мережевого середовища. Такий підхід відповідає принципам сегментації трафіку та дотримання принципів безпеки мережі. Серверна підмережа ізольована від інших VLAN, у яких можуть перебувати, наприклад, робочі станції користувачів або пристрої IoT. Завдяки цьому зменшується ризик несанкціонованого доступу або поширення шкідливого трафіку між сегментами.

```
Switch(config)#int f0/9
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
```

Рисунок 3.15 – Додавання сервера у підмережу

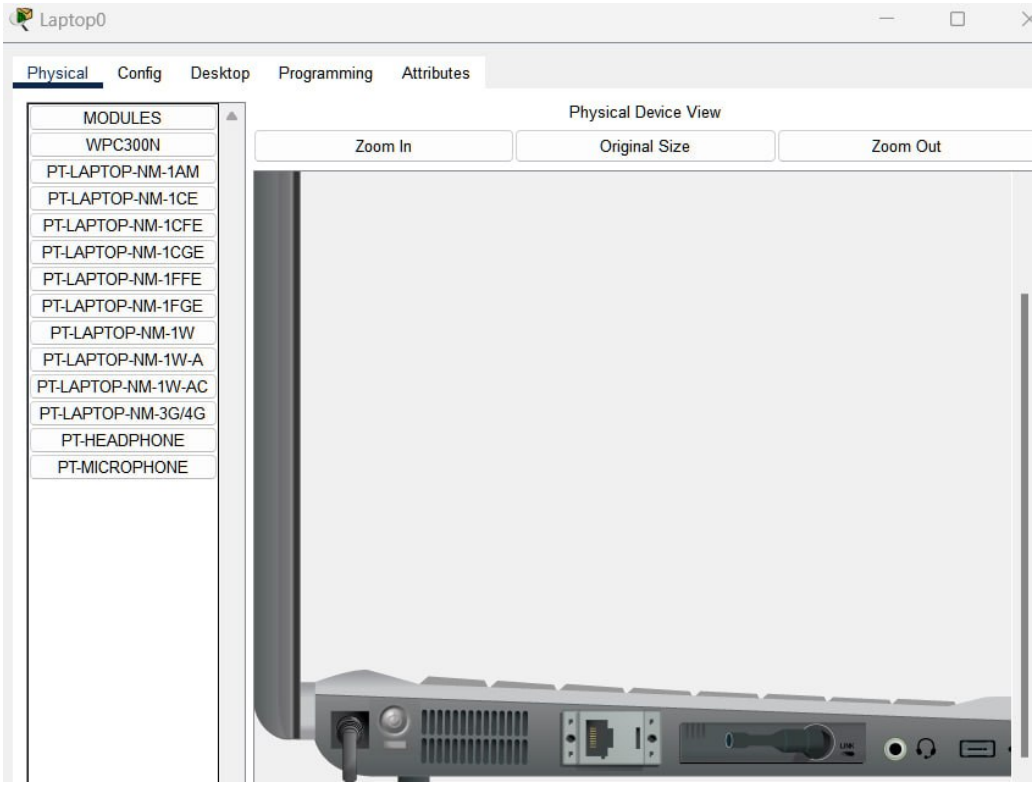


Рисунок 3.16 – На ноутбуці замінюємо модуль на бездротовий інтернет

Рисунок 3.17 повторно ілюструє налаштування NAT (Network Address Translation) для трансляції локальних IP-адрес у глобальну адресу. Це забезпечує вихід пристроїв з внутрішньої мережі в Інтернет і є важливим етапом при створенні повноцінного мережевого середовища.

Після налаштування DNS-сервера та NAT було виконано перевірку їх працездатності. Клієнтський пристрій здійснив запит до доменного імені, і DNS-сервер успішно перетворив його на IP-адресу. Подальша маршрутизація через NAT підтвердила можливість виходу в Інтернет з внутрішньої адреси. Це свідчить про правильну інтеграцію мережевих сервісів. Окрім раціонального використання адресного простору, NAT також дозволяє підвищити керованість трафіку, забезпечити фільтрацію та моніторинг з'єднань. У разі необхідності, можна легко налаштувати правила переадресації портів (port forwarding), що дозволяє доступ ззовні до внутрішніх ресурсів, таких як веб-сервер або FTP. Таким чином, NAT не лише виконує роль "перекладача" адрес, але й виступає гнучким інструментом адміністрування. Оскільки за NAT-перетворенням внутрішні адреси недоступні для зовнішнього спостерігача, зловмиснику буде складно виявити внутрішню

топологію мережі. Таким чином, NAT виступає своєрідним бар'єром, що ускладнює здійснення несанкціонованого доступу та спроб злому

```
Router(config)#int g0/0
Router(config-if)#ip nat inside
Router(config-if)#int g0/1
Router(config-if)#ip nat outside
Router(config-if)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#sh ip nat stat
Total translations: 0 (0 static, 0 dynamic, 0 extended)
Outside Interfaces: GigabitEthernet0/1
Inside Interfaces: GigabitEthernet0/0
Hits: 0  Misses: 0
Expired translations: 0
Dynamic mappings:
Router#show ip nat translations
Router#show ip nat translations
Router#sh ip nat stat
Total translations: 0 (0 static, 0 dynamic, 0 extended)
Outside Interfaces: GigabitEthernet0/1
Inside Interfaces: GigabitEthernet0/0
Hits: 0  Misses: 4
Expired translations: 0
Dynamic mappings:
Router#show ip nat translations
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip nat inside source static 192.168.10.2 89.203.12.47
Router(config)#
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
---  89.203.12.47      192.168.10.2       ---                ---

Router#sh ip nat stat
Total translations: 1 (1 static, 0 dynamic, 0 extended)
Outside Interfaces: GigabitEthernet0/1
Inside Interfaces: GigabitEthernet0/0
```

Рисунок 3.17-NAT

Далі налаштування зовнішнього інтерфейсу маршрутизатора, який з'єднано з глобальною мережею (Інтернетом), що забражено на рисунку 3.18. Зазначено публічну IP-адресу, маску та шлюз, через які здійснюється вихід за межі локальної мережі.

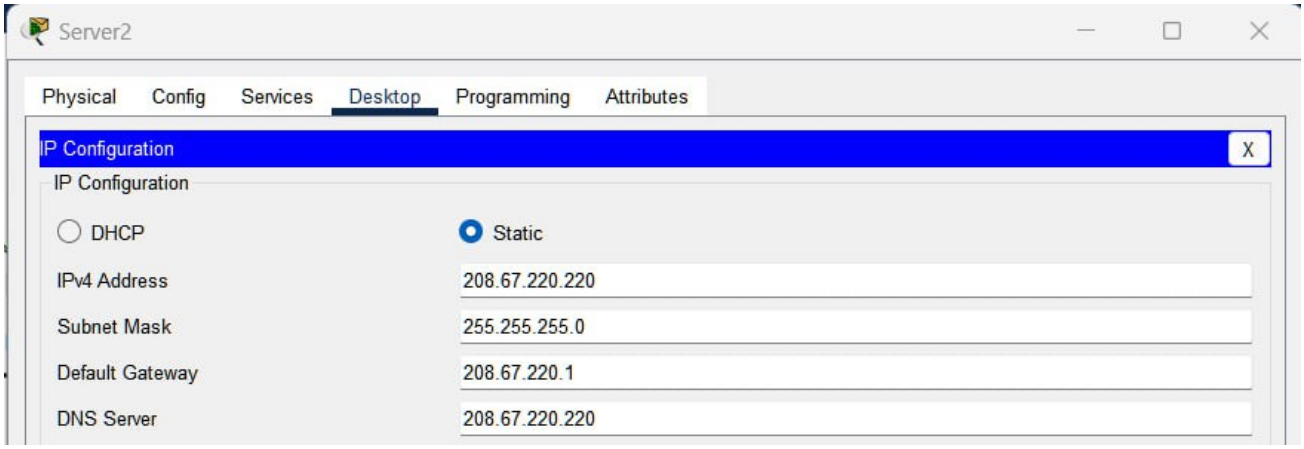


Рисунок 3.18- Зовнішній сервер роутера

Рисунок 3.19 ілюструє процес тестування з'єднання з локального ПК (з IP-адресою 192.168.10.2) до зовнішнього або внутрішнього сервера. Використано утиліту ping, що підтверджує доступність сервера, правильну роботу маршрутизатора, NAT та інших мережевих служб.

```
C:\>ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:

Reply from 192.168.10.2: bytes=32 time=53ms TTL=127
Reply from 192.168.10.2: bytes=32 time=13ms TTL=127
Reply from 192.168.10.2: bytes=32 time=14ms TTL=127
Reply from 192.168.10.2: bytes=32 time=27ms TTL=127

Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 13ms, Maximum = 53ms, Average = 26ms
```

Рисунок 3.20- Перевірка з'єднання з ПК (192.168.10.2) до сервера

Налаштування мережі завершено.

3.4 Висновки

У практичній частині роботи виконано детальний проект локальної мережі магазину та впроваджено його модель у Cisco Packet Tracer. Було прийнято ряд рішень, які підтвердили свою ефективність при перевірці:

1. Мережа сегментована на декілька VLAN відповідно до підрозділів магазину, що дозволило ізолювати трафік і підвищити безпеку без втрати зручності обміну даними.

2. Обране мережеве обладнання (керований комутатор і маршрутизатор Cisco) забезпечило гнучке налаштування і надійну роботу. У симуляції підтверджено коректність конфігурації VLAN, міжвланової маршрутизації, DHCP та NAT.

3. Розроблено схему IP-адресації приватного простору, яка спрощує адміністрування (логічні групи адрес по відділах) та легко масштабується у разі розширення мережі.

4. Налаштовано необхідні мережеві служби: DHCP автоматизує налаштування робочих станцій, DNS забезпечує іменування (в реалі може бути реалізовано на сервері), NAT дає всім вузлам доступ в Інтернет через єдиний зовнішній IP.

5. Реалізовано основні заходи безпеки: шифрування Wi-Fi (WPA2), фільтрація трафіку між сегментами (ACL на маршрутизаторі), закриття невикористаних портів комутатора, встановлення паролів на мережеве обладнання. Це зменшує ризики як зовнішніх вторгнень, так і внутрішніх витоків.

6. Передбачено резервне копіювання важливих даних на сервері та використання UPS для захисту від перебоїв живлення, що підвищує стійкість IT-інфраструктури магазину.

Проєкт мережі був успішно перевірений на відповідність поставленим вимогам шляхом тестування в Packet Tracer. Отримані результати показують, що запропонована мережева інфраструктура забезпечить ефективну роботу інформаційних систем магазину, швидкий доступ до потрібних ресурсів для

персоналу, а також безпечний доступ до Інтернету для відвідувачів. У наступному розділі (висновках) узагальнюються підсумки виконаної дипломної роботи та визначаються можливі напрямки подальшого вдосконалення мережі.

ВИСНОВКИ

В дипломній роботі вирішено комплекс завдань з розробки комп’ютерної мережі магазину. На підставі аналізу діяльності підприємства і планування приміщень було визначено вимоги до мережі: необхідність об’єднати кілька відділів в єдину інфраструктуру, забезпечити доступ до Інтернету, захистити внутрішні інформаційні ресурси та організувати гостьовий доступ.

В теоретичній частині узагальнено принципи побудови локальних мереж, розглянуто сучасні технології і обладнання, які використовуються для їх реалізації. Було описано моделі мережевої взаємодії, типи топологій, функції основних пристроїв (комутаторів, маршрутизаторів, точок доступу), а також засоби забезпечення мережевої безпеки. Ці відомості дозволили обґрунтовано підійти до вибору рішень для практичної реалізації.

У практичному розділі на основі теоретичних знань спроектовано локальну мережу магазину “Погляд” із використанням обладнання Cisco. Розроблено структурну схему мережі, згідно з якою всі комп’ютери підключено до центрального комутатора в серверній кімнаті, а маршрутизатор виконує роль шлюзу до Інтернету та контролює обмін даними між сегментами. Впроваджено поділ на VLAN відповідно до відділів магазину, що підвищує продуктивність і безпеку мережі. Налаштовано IP-адресацію приватного діапазону для кожного сегменту, конфігуровано протоколи і служби (DHCP, NAT, VLAN, SSH), необхідні для автоматизації і захисту мережевих з’єднань.

Модель мережі перевірена в середовищі Cisco Packet Tracer: результати тестування підтвердили правильність роботи всіх компонентів. Співробітники магазину мають доступ до спільного серверу з мінімальними затримками, а відвідувачі можуть підключатися до Wi-Fi, не ризикуючи цілісністю внутрішніх даних. Мережа здатна масштабуватися, тому що за необхідності можна додавати нові робочі місця або навіть нові відділи (VLAN) з мінімальними змінами в конфігурації.

Одним з важливих аспектів проекту є забезпечення безпеки: у роботі досягнуто баланс між відкритістю мережі для бізнес-потреб (вільний доступ співробітників до ресурсів, Інтернет-зв'язок) та захищеністю (ізоляція критичних сегментів, шифрування, контроль доступу). Також реалізовано базові заходи відмовостійкості, таких як резервне копіювання та аварійне живлення, що свідчить про надійність спроектованої інфраструктури.

Практична цінність роботи полягає в тому, що отриманий проект мережі може бути безпосередньо застосований або адаптований для реального магазину середнього розміру.

Наукова новизна дипломної роботи полягає у комплексному підході до побудови мережі малого підприємства з використанням сучасних технологій сегментації і безпеки, що зазвичай притаманні більшим корпоративним мережам. Показано, що навіть в умовах обмежених ресурсів можна впровадити рішення (VLAN, VLAN Routing, WPA2, ACL), які забезпечать високий рівень захищеності інформації.

Підсумовуючи, поставлену мету досягнуто, спроєктовано і протестовано локальну комп'ютерну мережу магазину, яка відповідає всім заданим вимогам щодо функціональності, продуктивності та безпеки. Розробка містить необхідні матеріали для її практичної реалізації. У ході виконання дипломної роботи автор поглибив знання з комп'ютерних мереж, навчився застосовувати теоретичні концепції (моделі, протоколи) у реальних конфігураціях, отримав навички роботи з мережевим обладнанням Cisco.

Проєкт може бути базою для подальшого вдосконалення мережі: впровадження засобів моніторингу трафіку, системи запобігання вторгнень (IPS/IDS), переходу на IPv6, використання хмарних сервісів для резервування тощо. Таким чином, дипломна робота робить внесок у розв'язання практичноїзадачі IT-інфраструктури малого бізнесу та демонструє можливості сучасних мережевих технологій у цьому сегменті.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Азаров О., Захарченко С., Кадук О. Комп’ютерні мережі: підручник. ВНТУ, 2020. 378 с.
2. Kurose J., Ross K. Computer Networking: A Top Down Approach. Pearson, 2017. 852 p.
3. Kumar P., Misra S. Computer Networks: Principles, Protocols and Architecture. Chapman \& Hall/CRC, 2020. 648 p.
4. Stallings W. Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud. Addison Wesley, 2020. 480 p.
5. Forouzan B. Data Communications and Networking. McGraw Hill Education, 2022. 656 p.
6. Krishnamurthi R. Computer Communication Networks. Elsevier, 2021. 492 p.
7. Kumar P., Misra S. Computer Networks: Principles, Protocols and Architecture. Chapman \& Hall/CRC, 2020. 648 p.
8. Kurose J., Ross K. Computer Networking: A Top Down Approach. Pearson, 2017. 852 p.
9. Peterson L., Davie B. Computer Networks: A Systems Approach. Morgan Kaufmann, 2021. 976 p.
10. Peterson L., Davie B. Computer Networks: A Systems Approach. Morgan Kaufmann, 2021. 976 p.
11. Lanza C., Moretti E. IPv6 and Next Generation Networking (2nd Edition). Springer, 2020. 312 p.
12. Т.С. Теорія комп’ютерних мереж: від основ до практики. Дніпро: ДНУ, 2021. 342 с.
13. Верещака С.І. Інформаційні мережі та системи зв’язку. — Одеса: ОНУ, 2020. 240 с.
14. Береза П.В. Побудова безпечних корпоративних мереж. Київ: КНУТД, 2022. 223 с.

15. Соловей О.П. Основи маршрутизації в комп’ютерних мережах. Вінниця: ВНТУ, 2021. 284 с.

16. Ільчук М.О. Адміністрування та моніторинг мереж. м Харків: ХНУ, 2020. 260 с.

17. Федорук О.М. Захист інформації в комп’ютерних мережах. Чернівці: ЧНУ, 2023. 276 с.

18. Горбач В.Л. Архітектура телекомунікаційних мереж. Київ: НУ “КПІ”, 2021. 348 с.

19. Ліщинський Р.П. Цифрові комунікації та комп’ютерні мережі. Львів: ЛНТУ, 2020. 267 с.

20. Коломієць Т.С. Моделювання мережі з використанням Cisco Packet Tracer. Запоріжжя: ЗНУ, 2022. 196 с.

21. Hagen S. Cloud Networking: Understanding Cloud-based Data Center Networks (2nd Edition). Wiley, 2020. 400 p.

22. McGrew D. Security in Computing and Networking (2nd Edition). – Truman University Press, 2021. 280 p.

23. Duato J., Yalman Ö., Gómez-Luna J., Shin K.-G. On Chip Communication Networks (2nd Edition). Morgan Kaufmann, 2020. 726 p.

24. Li Z., Mahapatra R., Agrawal B. 5G Mobile and Wireless Communications Technology. – Cambridge University Press, 2021. 676 p.

25. Steel B., Nagappan A. Network Performance and Security: Testing and Hardening Wireless and Ethernet Networks. SAMS, 2021. 524 p.

26. Behringer M., Roessler R. Understanding IPv6 (5th Edition). Prentice-Hall, 2022. 592 p.

27. Comer D. Internetworking with TCP/IP Volume One (6th Edition). Pearson, 2021. 936 p.

28. Abdullah A.F., Bassilious F. Wi-Fi 6 & Next Generation Wireless Networks. Wiley, 2023. 328 p.

29. Oppenheimer P. Top-Down Network Design (3rd Edition). Cisco Press, 2020. 494 p.

30. Dawkins G., Spurlin R., George C. Wireless Communications & Networking (3rd Edition). Elsevier, 2021. 570 p.

31. Antón A., Bowen P. Security for System-on-Chip Designs: Foundational Concepts and Practical Applications. Springer, 2020. 450 p.

32. Hicks R., Newell D. IPv6 Essentials (3rd Edition). O'Reilly, 2022. 240 p.

33. Northcutt S., Novak J. Network Intrusion Detection (Forward). Cisco Press, 2023. 304 p.

34. White C., Stallings W. Network Security Essentials: Applications and Standards (7th Ed.). Pearson, 2022. 456 p.

35. Johnson S., Ross K. Next-Generation Internet: Performance, Architecture, and Applications. Springer, 2021. 384 p.

36. Gupta B., Perez M. Machine Learning for Computer and Cyber Security Applications. CRC Press, 2022. 312 p.

37. Tucker J., Nelson B. Routing TCP/IP (Volume 1, 3rd Ed.). Cisco Press, 2023. 832 p.

38. Tan R., Wang Y. Cloud Networking: Principles and Practice. Wiley, 2021. 416 p.

39. Li L., Geng X. AI-Driven Network Security: Models and Practices. – Springer, 2022. 378 p

40. Anderson R., Kumar V. Fundamentals of Wireless Communication. – Cambridge University Press, 2020. 592 p.

41. Costa M., Sobrinho J. Topology Control in Wireless Ad Hoc and Sensor Networks. – Springer, 2021. 298 p.

42. Sivalingam K.M., Barolli L. 5G for Future Wireless Networks. Springer, 2022. 472 p.

43. Patterson D., Bhatti N. Modern Network Design and Management. Morgan Kaufmann, 2021. 351 p.

44. Oppenheimer P. Cisco SD-WAN: Advanced Design and Deployment. Cisco Press, 2023. 514 p.

45. Taylor C., Beck J. Essential Computer Networking (2nd Ed.). – McGraw-Hill, 2020. 422 p.

46. Minoli D. Designing, Developing, and Deploying Systems and Applications for Cloud and Beyond. Wiley, 2021. 448 p.

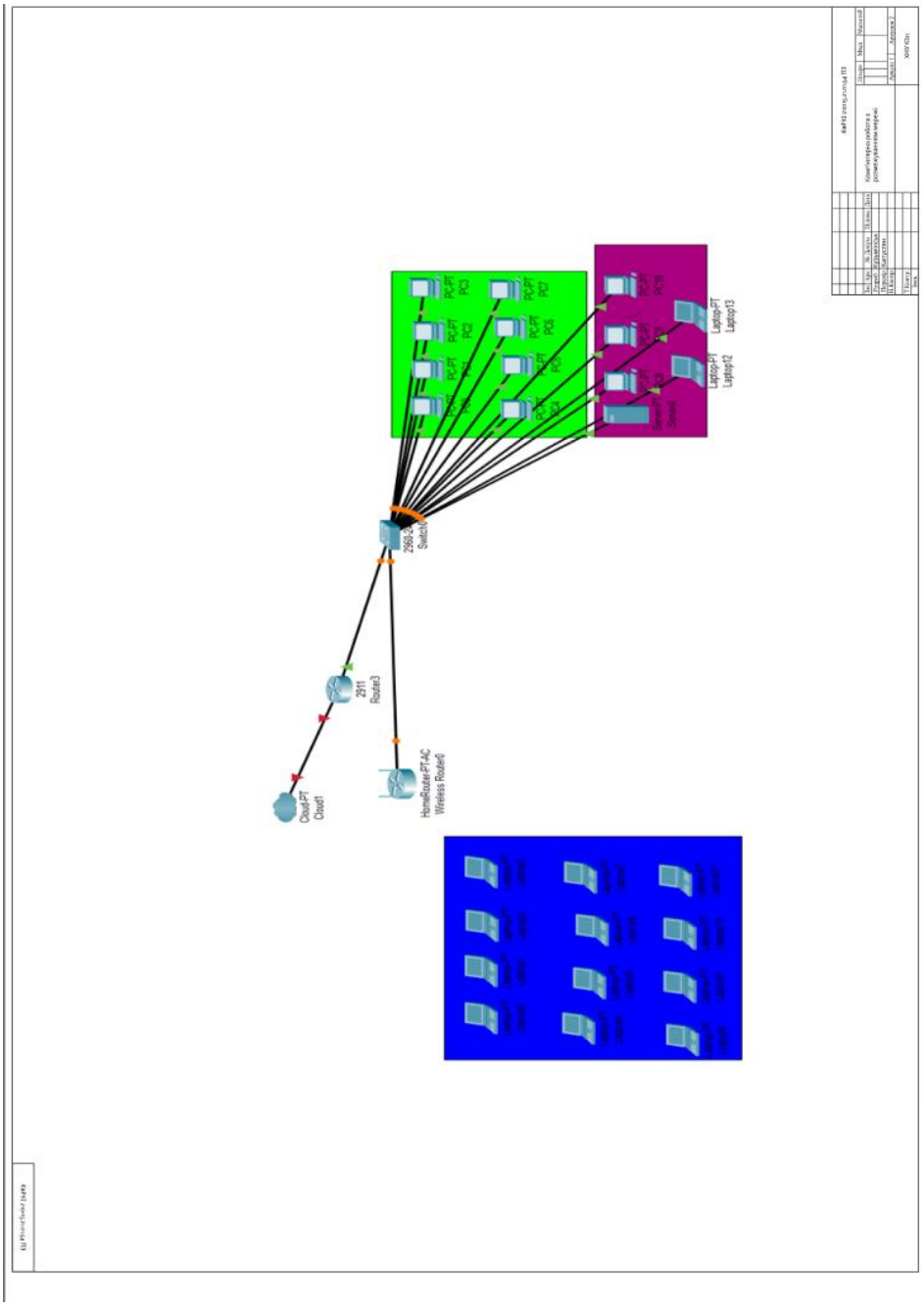
47. Song H., Rawat D.B. Cyber-Physical Systems: Foundations, Principles and Applications. Elsevier, 2022. 390 p.

48. Жукова Н.А. Інформаційні системи в комп’ютерних мережах. Суми: СумДУ, 2023. – 312 с.

Додаток А

(обов’язковий)

КОПІЯ КРЕСЛЕННЯ «СТРУКРУРНА СХЕМА МЕРЕЖІ»



Додаток Б

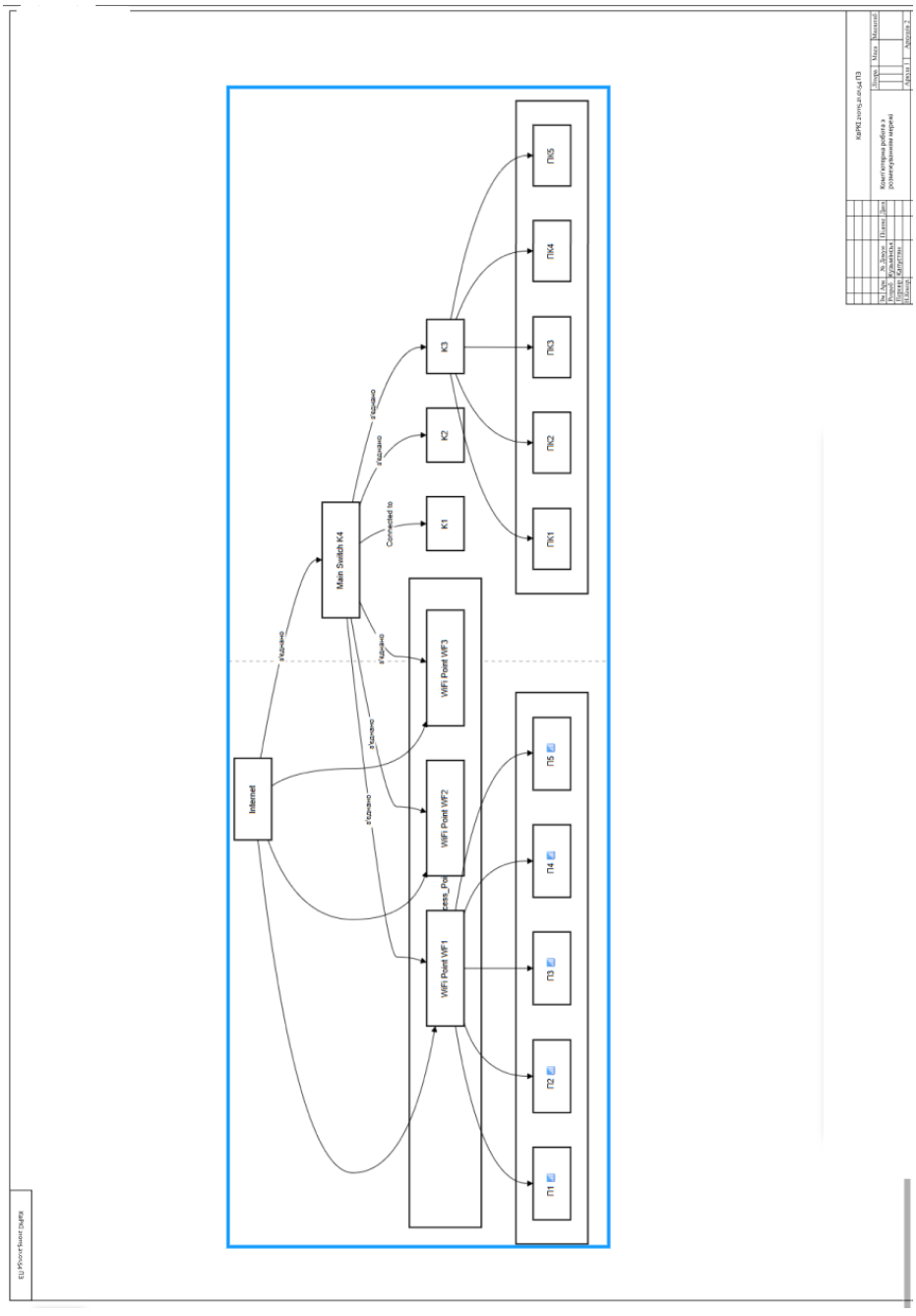
(обов’язковий)

КОПІЯ КРЕСЛЕННЯ «ФУНКЦІОНАЛЬНА СХЕМА МЕРЕЖІ»

Додаток В

(обов’язковий)

КОПІЯ КРЕСЛЕННЯ «КАРТА КОМП’ЮТЕРНОЇ МЕРЕЖІ»



Завідувачу кафедри КІІС
д-р. філософії, доц. Ользі ПАВЛОВІЙ

Інни КУЗЬМІНСЬКОЇ
ПІБ здобувача вищої освіти

ФІТ, 4 курсу, групи КІ2-21-1

ЗАЯВА

З правилами чинного Положення «Про систему забезпечення академічної доброчесності у Хмельницькому національному університеті» від 01.07.2022, згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений (а). Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат оповіщений(а) та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-технічних засобів (Strike-Plagiarism та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

16 червня 2025 року

РІШЕННЯ ЕКСПЕРТНОЇ КОМІСІЇ
КАФЕДРИ КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА ІНФОРМАЦІЙНИХ СИСТЕМ
ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: Комп'ютерна мережа з розмежуванням доступу

Автор: Інна КУЗЬМІНСЬКА

Спеціальність: 123– Комп'ютерна інженерія

Освітня програма: освітньо-професійна

Науковий керівник: Марія КАПУСТЯН, к.т.н, доцент

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом. Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв`язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	

Підтвердження:

Запозичення, виявлені в роботі, є законними і не є плагіатом, оскільки:

1) Запозичення розміщені в розділах аналізу існуючих аналогів та прототипів, що є загальним оглядом літератури та не стосуються безпосередньо авторського дослідження чи оригінальних результатів роботи.
2) Усі запозичення є фрагментарними та належним чином оформлені відповідно до академічних вимог, з наданням точних посилань на джерела, з яких вони були отримані.
3) Окремі збіги, зафіксовані системою, є загальновживаними фразами або термінами, що часто використовуються в галузі, про що свідчить численні збіги з 10-40 джерелами на один фрагмент тексту. Такі фрази не є результатом авторського плагіату, оскільки належать до загальновизнаних термінів.
4) В окремих випадках система зафіксувала послідовності чотиризначних двійкових кодів, що є типовими вхідними даними для множини задач, і не можуть розглядатися як об'єкт авторських прав, оскільки ці послідовності є стандартними елементами для математичних чи технічних розрахунків.
5) Всі зафіксовані системою ознаки модифікації тексту пов'язані з комбінуванням латинських символів зі скороченнями українських індексів у формулах. Це не є модифікацією змісту, оскільки такі скорочення є стандартною практикою в математичній та технічній літературі і не порушують авторських прав.

Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ ідентичності/схожості StrikePlagiarism, складає 2% і адресується до 401 першоджерела; та системою Anti-Plagiarism складає 1%, що, з урахуванням наведених обгрунтувань, відповідає характеру наукового дослідження і свідчить на користь кваліфікаційної роботи.

Керівник роботи _____ Марія КАПУСТЯН

Гарант ОП _____ Андрій Нічепорук

Завідувач кафедри КІС _____ Ольга ПАВЛОВА

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

Дипломник: Кузьмінська Інна Валеріївна

Тема: Комп'ютерна мережа магазину з розмежуванням доступу.

Спеціальність: 123 «Комп'ютерна інженерія»

Обсяг кваліфікаційної роботи:

Кількість листів креслень ___3___ Кількість сторінок записки ___55___

1. Короткий зміст роботи та прийнятих рішень: Метою кваліфікаційної роботи є створення системи моніторингу закриття вікон і дверей у приміщенні.

2. Висновок про відповідність роботи дипломному завданню: Дипломний проект у повній мірі відповідає поставленому завданню як в теоретичній, так і в практичній частині даного проекту.

3. Характеристика виконання кожного розділу, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У першому розділі роботи здійснено детальний аналіз існуючих аналогів і підходів до побудови мереж для комерційних об'єктів, що дозволило визначити оптимальні технології і методи для забезпечення безпеки, продуктивності та надійності мережі. У наступному розділі було обґрунтовано вибір програмних і апаратних засобів для реалізації проекту. Для цього було враховано не тільки технічні характеристики обладнання, але й можливість інтеграції в існуючу інфраструктуру магазину, а також перспективи масштабування мережі в майбутньому. Основна частина роботи була присвячена детальному опису реалізації запропонованих рішень. Описано алгоритми роботи мережі, принципи налаштування IP-адресації та VLAN, а також методи забезпечення безпеки мережі, що включають налаштування фаєрволів та контроль доступу.. Загалом, дипломна робота відповідає всім вимогам і містить сучасні методи та підходи до вирішення завдань побудови та обслуговування комп'ютерних мереж, що дозволяє застосувати отримані результати в реальних умовах для підвищення ефективності роботи магазину.

4. Позитивні сторони роботи: Дипломна робота має високу практичну цінність, оскільки розроблена система комп'ютерної мережі для магазину дозволяє забезпечити стабільну, безпечну та ефективну роботу всіх інфраструктурних елементів. Проєкт враховує можливість подальшого розширення і масштабування, що дозволяє зростати бізнесу разом з розвитком мережі, а також адаптувати мережу до нових технологічних вимог.

5. Негативні сторони роботи: Недостатньо висвітлені питання гостьового доступу та питання вартості побудови мережі.

6. Оцінка графічного оформлення та пояснювальної записки роботи: Пояснювальна записка оформлена коректно, згідно діючих стандартів оформлення документації.

7. Відгук про роботу в цілому: Робота виконана на належному науково-технічному рівні.

8. Інші зауваження: _____

9. Оцінка дипломної роботи: Розглянувши позитивні та негативні сторони представленої дипломної роботи вважаю, що робота заслуговує оцінки «добре», 3.75 (С).

Рецензент (прізвище, ім'я, по батькові, посада, місце роботи) Оксенчук Оксана Григорівна, к. пед. наук, доцент каф. ІПЗ, УжНУ

"16" 06 2025 р. _____ (підпис)

Протокол аналізу звіту подібності експертом

Заявляю, що я ознайомився (-лась) з Повним звітом подібності, який був згенерований Системою виявлення і запобігання плагіату щодо роботи:

Автор: Інна КУЗЬМІНСЬКА

Співавтор:

Назва: Кузьмінська_Комп'ютерна мережа магазину з розмежуванням доступу

Експерт:

Підрозділ: Кафедра комп'ютерної інженерії та інформаційних систем

Коефіцієнт подібності 1:2%

Коефіцієнт подібності 2:0.6%

Мікропробіли: 26

Заміна букв: 1

Інтервали: 0

Білі знаки: 0

Дата створення звіту: 2025-06-13 07:07:42.0

Після аналізу Звіту подібності констатую наступне:

☒ **Запозичення, виявлені в роботі є законними і не є плагіатом. Рівень подібності не перевищує допустимої межі. Таким чином робота незалежна і приймається.**

☐ **Запозичення не є плагіатом, але перевищено граничне значення рівня подібностей. Таким чином робота повертається на доопрацювання.**

☐ **Виявлено запозичення і плагіат або навмисні текстові спотворення (маніпуляції), як передбачувані спроби укриття плагіату, які роблять роботу невідповідною вимогам законодавства (Ст. 32. ЗУ Про вищу освіту, пункт 3.1, Ст. 42. ЗУ Про освіту) та вимог НАЗЯВО (Критерій 5), а також кодексу етики і процедурам. Таким чином робота не приймається.**

Обгрунтування:

2025-06-13 Доцент Андрій Нічепорук

Дата експерт

Anti-Plagiarism (UA) v-15.281 Educational

The maximum coincidence with one document 1.0%

Dictionaries check: en_US, ru_RU, ua_UA. **Errors in the documents: 12%**

	Document		Sum coincidence on the DB	
ID: 245510 Title: БКР Комп'ютерна мережа магазину з розмежуванням доступу Added in a DB: 2025-06-13 Authors: Інна КУЗЬМІНСЬКА Heads: Марія КАПУСТЯН Consultants: Opponents:	Symbols	Lexemes	Symbols	Lexemes
	82801	656	1222 (1%)	20 (3%)

Plagiarism sources

ID	Description	Plagiarism presence in the document	
		Symbols	Lexemes