Міністерство освіти і науки України

Луцький національний технічний університет
(повне найменування закладу вищої освіти)

Факультет комп'ютерних та інформаційних технологій
(повне найменування факультету)

Кафедра комп'ютерної інженерії та безпеки
(повне найменування кафедри)

КВАЛІФІКАЦІЙНА РОБОТА ЗА СТУПЕНЕМ ВИЩОЇ ОСВІТИ «БАКАЛАВР»

КОРПОРАТИВНА МЕРЕЖА КОМПАНІЇ DODAY

CORPORATE NETWORK OF DODAY COMPANY

спеціальність 123 Комп'ютерна інженерія
(шифр і назва спеціальності)

освітня програма Комп'ютерна інженерія
(назва освітньої програми)

Виконав: здобувач вищої освіти
групи КІ-41
Чичелюк Олеся Андріївна

(підпис)

Керівник:
к.т.н., доцент
Багнюк Наталія Володимирівна

(підпис)

Кваліфікаційну роботу
допущено до захисту
« 04 » червня 2025 р.
Гарант освітньої програми:
к.т.н., доцент
Лавренчук Світлана Василівна

(підпис)

Луцьк – 2025 року

ЛУЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Факультет *комп'ютерних та інформаційних технологій*
Кафедра *комп'ютерної інженерії та безпеки*
Ступінь вищої освіти: *бакалавр*
Галузь знань: *12 Інформаційні технології*
Спеціальність: *123 Комп'ютерна інженерія*
Освітня програма: *«Комп'ютерна інженерія»*

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ доц. Т. ТЕРЛЕЦЬКИЙ
« 10 » 01 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ ЗДОБУВАЧУ ВИЩОЇ ОСВІТИ

Чичелюк Олесі Андріївни
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи *Корпоративна мережа компанії DoDay*

Керівник роботи *к.т.н., доцент Багнюк Наталія Володимирівна*

затверджені наказом закладу вищої освіти від «04» січня 2025 року № 11/01-02
2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 10.06.2025р.

3. Вихідні дані до роботи *джерелом розробки є науково-технічна література та публікації в періодичних виданнях з даного питання, опубліковані зарубіжні та вітчизняні роботи в даній області та різні інтернет-ресурси технічного спрямування.*

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити):
Вступ
Теоретичні основи проєктування корпоративних мереж
Проєктування корпоративної мережі компанії DoDay
Реалізація та налаштування корпоративної мережі
Висновки

5. Перелік графічного (ілюстративного) матеріалу:

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис	
		завдання видав	завдання прийняв
Теоретичні основи проєктування корпоративних мереж	*Багнюк Н.В., доцент*		
Проєктування корпоративної мережі компанії DoDay	*Багнюк Н.В., доцент*		
Реалізація та налаштування корпоративної мережі	*Багнюк Н.В., доцент*		
Нормоконтроль	*Багнюк Н.В., доцент*		
Гарант ОП	*Лавренчук С.В., доцент*		
Показник запозичень тексту	***___%***		
Академічна доброчесність	*Міскевич О.І.,ст.викладач*		

7. Дата видачі завдання 10.01.2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	*Огляд літератури із досліджуваної проблеми, аналіз предметної області та наявних рішень*	до 10.02.2025 р.	Виконано
2.	*Теоретичні основи проєктування корпоративних мереж*	до 02.03.2025 р.	Виконано
3.	*Проєктування, реалізація та налаштування корпоративної мережі*	до 02.04.2025 р.	Виконано
4.	*Висновки та пропозиції*	до 10.04.2025 р.	Виконано
5.	*Формування списку використаних джерел*	до 15.04.2025 р.	Виконано
6.	*Формування додатків*	до 02.05.2025 р.	Виконано
7.	*Оформлення ілюстративного матеріалу*	до 10.05.2025 р.	Виконано
8.	*Представлення остаточного варіанту кваліфікаційної роботи керівникові*	до 15.05.2025 р.	Виконано
9.	*Нормоконтроль*	до 30.05.2025 р.	Виконано
10	*Інструментальна перевірка на академічний плагіат*	до 03.06.2025 р	Виконано
11.	*Здача кваліфікаційної роботи та всіх супровідних документів на кафедру*	до 10.06.2025 р.	Виконано

Здобувач вищої освіти _____ (підпис) Чичелюк О.А. (прізвище, ініціали)

Керівник кваліфікаційної роботи _____ (підпис) Багнюк Н.В. (прізвище, ініціали)

АНОТАЦІЯ

Чичелюк О. А. Корпоративна мережа компанії DoDay. Рукопис.

Кваліфікаційна робота бакалавра ОП «Комп'ютерна інженерія» спеціальності 123 Комп'ютерна інженерія. Луцький національний технічний університет. Луцьк, 2025.

Кваліфікаційна робота складається зі вступу, трьох розділів, висновків, списку використаних джерел та додатків.

У першому розділі представлено теоретичні основи проєктування корпоративних мереж, наведено поняття корпоративної мережі, основні етапи її проєктування, типову структуру та топологію, розглянуто канали зв'язку, VLAN, використання технологій Інтернету речей (IoT) та принципи адміністрування й контролю доступу.

У другому розділі виконано проєктування корпоративної мережі компанії DoDay. Проаналізовано вимоги до мережі, розроблено її фізичну й логічну структуру, обґрунтовано вибір мережевого обладнання, зокрема маршрутизаторів, комутаторів, точок доступу, серверів і периферійних пристроїв.

У третьому розділі реалізовано налаштування мережі в середовищі Cisco Packet Tracer. Здійснено конфігурацію маршрутизаторів і комутаторів, побудовано схему логічної адресації, організовано VLAN та маршрутизацію між ними, налаштовано DHCP, Wi-Fi, VPN-з'єднання з віддаленими офісами, реалізовано елементи мережевої безпеки – списки контролю доступу (ACL), шифрування, SNMP-моніторинг.

Ключові слова: корпоративна мережа, VLAN, VPN, OSPF, Cisco Packet Tracer, IoT, DHCP, ACL, NAT.

ANNOTATION

Chycheliuk O. Corporate network of DoDay company. Manuscript.

Bachelor's qualification thesis in the educational program Computer Engineering, specialty 123 Computer Engineering. Lutsk National Technical University. Lutsk, 2025.

The bachelor's thesis consists of an introduction, three chapters, conclusions, a list of references, and appendices.

The first chapter presents the theoretical foundations of corporate network design, including the concept of a corporate network, the main stages of its development, typical structure and topology, communication channels, VLAN configuration, the use of Internet of Things (IoT) technologies, and principles of administration and access control.

The second chapter describes the design of the DoDay company's corporate network. The network requirements are analyzed, its physical and logical structure is developed, and the choice of network equipment is justified – including routers, switches, access points, servers, and peripheral devices.

The third chapter focuses on the network configuration in the Cisco Packet Tracer environment. It includes the setup of routers and switches, development of IP addressing schemes, implementation of VLAN and inter-VLAN routing, configuration of DHCP, Wi-Fi, VPN connections to remote offices, and implementation of network security features – access control lists (ACL), encryption, and SNMP monitoring.

Keywords: corporate network, VLAN, VPN, OSPF, Cisco Packet Tracer, IoT, DHCP, ACL, NAT.

ЗМІСТ

ВСТУП

У сучасних умовах динамічного розвитку інформаційних технологій ефективність роботи будь-якої компанії значною мірою залежить від якості організації її корпоративної мережі. Особливо актуальним це стає для підприємств, які мають численні структурні підрозділи, віддалені офіси та потребують інтеграції новітніх технологій для автоматизації та моніторингу робочих процесів. Компанія DoDay, що розширює свій бізнес, гостро відчуває необхідність у створенні надійної, масштабованої та безпечної мережевої інфраструктури, яка б забезпечувала безперебійний обмін даними між відділами, а також підтримувала підключення Інтернету речей (IoT), зокрема систем відеоспостереження.

Актуальність теми обумовлена тим, що сучасні корпоративні мережі повинні відповідати високим вимогам щодо продуктивності, безпеки та гнучкості. Особливо це стосується мереж, які інтегрують IoT-пристрої та об’єднують кілька географічно розподілених офісів. Ефективне проєктування такої мережі дозволить компанії DoDay оптимізувати бізнес-процеси, покращити захист інформації і забезпечити комфортні умови роботи для співробітників.

Метою роботи є розробка корпоративної мережі компанії DoDay з урахуванням сучасних технологій, що передбачає організацію локальної мережі, інтеграцію IoT-пристроїв, налаштування міжмережевої маршрутизації та забезпечення безпеки при обміні даними.

Об’єктом дослідження є корпоративна комп’ютерна мережа компанії DoDay, її архітектура, складові елементи та методи організації.

Предметом дослідження є корпоративна мережа офісу компанії DoDay з підтримкою IoT-пристроїв (камер відеоспостереження) та організацією зв’язку з віддаленими офісами.

Для реалізації поставленої мети необхідно вирішити низку ключових завдань, які дозволять створити сучасну, ефективну та безпечну корпоративну мережу компанії DoDay. Зокрема, необхідно:

– проаналізувати структуру компанії DoDay та сформулювати основні вимоги до мережевої інфраструктури з урахуванням використання IoT-пристроїв, відеоспостереження та наявності віддалених офісів;

– вибрати логічну топологію корпоративної мережі, яка забезпечить масштабованість, централізоване керування та гнучкість при подальшому розвитку мережі;

– впровадити схему логічної IP-адресації для усіх сегментів мережі, включно з відокремленими VLAN, офісними приміщеннями та віддаленими підрозділами компанії;

– розробити структуру віртуальних локальних мереж (VLAN) з урахуванням функціонального поділу компанії, що дозволить ізолювати трафік, обмежити доступ і підвищити рівень безпеки;

– налаштувати маршрутизацію між VLAN за допомогою протоколу OSPF, забезпечити динамічне оновлення маршрутів і зменшити час затримки при передачі даних;

– розробити та візуалізувати топологію корпоративної мережі, що відображатиме як фізичні, так і логічні зв’язки між компонентами інфраструктури;

– обґрунтувати та здійснити вибір мережевого обладнання: маршрутизаторів, комутаторів, точок доступу, серверів, периферійних пристроїв відповідно до потреб компанії щодо безпеки, продуктивності та масштабованості;

– реалізувати проєкт у середовищі Cisco Packet Tracer, змоделювати налаштування пристроїв, портів, підмереж, серверів, VLAN та VPN-з’єднань;

– налаштувати основні мережеві сервіси, зокрема DHCP, організувати VPN-зв’язок з філіями в інших містах та NAT;

– забезпечити мережеву безпеку через списки контролю доступу (ACL), авторизацію;

– виконати тестування мережі: перевірити доступність між VLAN, коректність DHCP, роботу VPN, взаємодію між віддаленими офісами й основною інфраструктурою.

Апробація: практична значимість основних результатів дослідження підтвердженна на Міжнародній науково-практичній конференції молодих вчених та студентів «Програмне та апаратне забезпечення в інформаційних технологіях» (6 травня 2025 р., м. Луцьк) [1].

РОЗДІЛ 1
ТЕОРЕТИЧНІ ОСНОВИ ПРОЕКТУВАННЯ КОРПОРАТИВНИХ МЕРЕЖ

1.1 Поняття корпоративної мережі

Корпоративна мережа – це комплекс інформаційно-технологічних засобів, які об’єднують комп’ютерні пристрої, сервери, мережеве обладнання та інші ресурси в межах однієї організації для забезпечення ефективного обміну даними, доступу до спільних сервісів і ресурсів [2]. Основна мета корпоративної мережі полягає у створенні єдиного інформаційного простору, який дозволяє співробітникам організації швидко та безпечно обмінюватись інформацією незалежно від їхнього фізичного розташування.

Сучасні корпоративні мережі зазвичай мають складну архітектуру і охоплюють кілька підмереж, які відповідають різним структурним підрозділам компанії. Вони можуть включати як локальні мережі (LAN), що об’єднують пристрої в межах одного офісу, так і глобальні мережі (WAN), що з’єднують розподілені географічно офіси або віддалені робочі місця [3].

Корпоративна мережа забезпечує взаємодію між різними відділами організації, такими як керівництво, маркетинг, підтримка клієнтів, навчальні класи, ІТ-відділ, бухгалтерія, юридичний відділ, а також між офісами у різних містах. Враховуючи сучасні потреби, до мережі часто підключаються IoT-пристрої, зокрема камери відеоспостереження, що підвищує рівень безпеки офісних приміщень.

Важливими характеристиками корпоративної мережі є:

– надійність і стабільність роботи – мережа повинна забезпечувати безперервний доступ до ресурсів підприємства;

– безпека – запобігання несанкціонованому доступу, захист від атак і витоку інформації;

– масштабованість – можливість розширення мережі без значних змін у її архітектурі;

– гнучкість – адаптація під потреби різних відділів, підтримка різних типів пристроїв, включно з IoT.

Таким чином, корпоративна мережа є комплексною системою, яка забезпечує ефективну, безпечну і зручну організацію обміну даними, об’єднує локальні і віддалені підрозділи та підтримує сучасні технологічні рішення.

1.2 Основні етапи проєктування корпоративної мережі

Проєктування корпоративної мережі – це комплексний процес, який включає технічне, логічне та організаційне планування з метою створення надійної, безпечної та масштабованої інфраструктури передачі даних [4]. На початковому етапі здійснюється аналіз потреб організації, специфіки її діяльності, кількості підрозділів, географічного розташування офісів, а також оцінка навантаження, яке мережа має витримувати.

Важливою частиною проєктування є формування логічної структури мережі. Це передбачає вибір топології мережі, що найкраще відповідає вимогам бізнесу – наприклад, зіркоподібної схеми, а також організацію мережі на логічні сегменти за допомогою VLAN. Кожен підрозділ отримує власну віртуальну мережу, що підвищує безпеку, оптимізує трафік і спрощує адміністрування. Для забезпечення маршрутизації між VLAN застосовують протоколи динамічної маршрутизації, такі як OSPF, які дозволяють ефективно обмінюватися маршрутною інформацією між пристроями.

На фізичному рівні проєктування передбачає вибір та розміщення мережевого обладнання маршрутизаторів, комутаторів, серверів, точок бездротового доступу. Зазвичай для великих офісних приміщень або кількох поверхів виділяють окремі маршрутизатори та комутатори, інколи розподіляючи їх за функціональним призначенням, наприклад, окремо для IoT-пристроїв (камери відеоспостереження, датчики) і окремо для користувацьких пристроїв (ПК, ноутбуки). Централізоване розміщення серверів забезпечує ефективне управління мережевими ресурсами.

Наступним кроком є налаштування мережевих сервісів, таких як протоколи динамічної маршрутизації, DHCP-сервери для автоматичного призначення IP-адрес в межах VLAN, а також впровадження заходів безпеки фільтрація трафіку за допомогою списків контролю доступу (ACL), забезпечення захищеного віддаленого доступу через VPN. Ці заходи гарантують конфіденційність, цілісність і доступність інформації в межах корпоративної мережі.

Заключним етапом проєктування є тестування та документування. Після впровадження налаштувань здійснюється перевірка працездатності мережі за допомогою діагностичних інструментів, таких як ping і traceroute, що дозволяє виявити та усунути можливі несправності. Одночасно створюється детальна технічна документація – схеми мережі, таблиці адресації, конфігурації мережевого обладнання, політики безпеки. Така документація значно полегшує подальшу підтримку і масштабування мережі.

Отже, проєктування корпоративної мережі вимагає комплексного і послідовного підходу, що охоплює всі рівні її структури від планування до впровадження. Дотримання цих етапів забезпечує створення стабільної, масштабованої та безпечної інфраструктури, яка відповідає сучасним потребам організації.

1.3 Структура корпоративної мережі

Структура корпоративної мережі є основою для забезпечення ефективної взаємодії між усіма інформаційними системами організації. Вона включає фізичне та логічне компонування мережевого середовища – комп’ютери, сервери, комутатори, маршрутизатори, точки доступу та мережеві сервіси. Від правильного проєктування структури залежить не лише продуктивність мережі, але й її безпека, надійність і масштабованість [5].

Зазвичай корпоративна мережа має ієрархічну архітектуру, що складається з кількох основних рівнів:

– ядро мережі (core layer) – відповідає за високошвидкісну маршрутизацію між ключовими сегментами мережі;

– рівень розподілу (distribution layer) – обробляє трафік між VLAN, реалізує політики безпеки, фільтрацію та маршрутизацію;

– рівень доступу (access layer) – забезпечує підключення кінцевих пристроїв до мережі.

Інфраструктура корпоративної мережі може включати як дротові, так і бездротові компоненти, які працюють як єдина система. До неї також можуть входити віддалені офіси, підключені через захищені VPN-канали, хмарні сервіси, камери відеоспостереження та інші периферійні пристрої. Структура мережі має бути гнучкою, адаптивною до змін і простою в адмініструванні.

У процесі проєктування корпоративної мережі часто застосовується багаторівнева модель із виділенням окремих сегментів для користувацьких пристроїв, IoT-компонентів (зокрема, камер відеоспостереження, серверів та віддалених офісів. Такий підхід відповідає сучасним стандартам побудови корпоративних мереж і дозволяє забезпечити високу ефективність, безпеку та керованість мережевої інфраструктури.

1.4 Вибір топології та методи підключення підмереж

Проєктування корпоративної мережі передбачає ретельний вибір топології, яка визначає спосіб організації зв’язків між мережевими пристроями. Правильно обрана топологія забезпечує ефективний обмін даними, високу надійність, гнучкість при масштабуванні та спрощує адміністрування мережі. Серед найпоширеніших варіантів – зіркоподібна, шинна, кільцева та комбіновані топології [6]. У сучасних корпоративних мережах найбільшу популярність має ієрархічна зіркоподібна топологія, що дозволяє централізовано контролювати трафік та розподіляти навантаження.

Ієрархічна модель передбачає розподіл мережі на три основні рівні: ядро, агрегацію (рівень розподілу) та доступ. Ключовими елементами на цих рівнях є

комутатори і маршрутизатори, що дає змогу створювати ізольовані логічні сегменти (VLAN), впроваджувати політики безпеки і ефективно управляти доступом до мережевих ресурсів. Ця модель підтримує як дротові Ethernet-з’єднання, так і бездротові точки доступу Wi-Fi у зонах, де потрібна мобільність користувачів.

Для маршрутизації трафіку між VLAN, підмережами та зовнішніми мережами застосовуються маршрутизатори. Особливо важливою є організація захищеного зв’язку з віддаленими офісами за допомогою VPN-технологій, що дозволяє інтегрувати географічно розподілені підрозділи в єдину корпоративну мережу із дотриманням високих стандартів безпеки.

У межах розроблюваної мережі обрана зіркоподібна топологія, що забезпечує стабільну роботу різних служб підприємства, враховуючи підключення дротових і бездротових пристроїв, IoT-компонентів (зокрема IP-камер), а також захищені канали зв’язку з віддаленими офісами. Такий підхід гарантує масштабованість, гнучкість та надійність корпоративної IT-інфраструктури.

1.5 Канали зв’язку корпоративної мережі

Канали зв’язку відіграють ключову роль у функціонуванні корпоративної мережі, оскільки саме вони забезпечують фізичну або логічну передачу даних між мережевими пристроями, відділами та віддаленими офісами. До основних характеристик каналів належать пропускна здатність, надійність, затримка, тип середовища передавання (мідь, оптика, бездротовий сигнал) та захищеність переданої інформації [7].

У корпоративному середовищі найчастіше застосовуються дротові канали зв’язку на основі мідного кабелю категорії 5e або 6 (Ethernet), а також оптоволоконні лінії, які забезпечують високу швидкість та більшу стійкість до електромагнітних завад, особливо на великих відстанях або для магістральних підключень. Для покриття окремих зон офісу, зокрема публічних або мобільних

робочих місць, часто впроваджуються бездротові канали зв’язку за технологією Wi-Fi.

Крім внутрішніх каналів, корпоративна мережа може включати зовнішні канали зв’язку, зокрема для підключення до Інтернету або встановлення захищених тунелів з віддаленими офісами. У таких випадках використовуються VPN (Virtual Private Network) – технологія, яка дозволяє створити зашифроване з’єднання через публічні мережі, зберігаючи конфіденційність та цілісність даних.

У межах проєкту корпоративної мережі для компанії DoDay було враховано різні типи каналів: дротове з’єднання для основних підрозділів, бездротовий доступ у загальних зонах, а також захищений VPN-канал для з’єднання з віддаленими офісами. Такий підхід забезпечує комплексне покриття потреб підприємства, балансуючи між швидкістю, надійністю та безпекою переданих даних.

1.6 Віртуальні локальні мережі (VLAN)

У сучасних корпоративних мережах важливу роль відіграє логічне розділення інфраструктури за допомогою віртуальних локальних мереж (VLAN). Технологія VLAN дозволяє об’єднувати пристрої в окремі логічні сегменти мережі незалежно від їхнього фізичного розташування. Це дає змогу підвищити продуктивність, спростити адміністрування, посилити безпеку та ізолювати трафік між окремими відділами або службами.

Завдяки VLAN можна створити окремі підмережі для кожного підрозділу організації – наприклад, для керівництва, бухгалтерії, технічної підтримки, IoT-пристроїв або публічних зон. Це дозволяє застосовувати до кожної VLAN власні правила маршрутизації, фільтрації трафіку, політики доступу та пріоритети обробки даних.

Для забезпечення взаємодії між VLAN зазвичай використовується маршрутизація між VLAN (Inter-VLAN Routing), яка реалізується за допомогою

маршрутизатора або комутатора третього рівня. Такий підхід дозволяє зберігати логічну ізольованість сегментів, водночас забезпечуючи обмін даними за потреби.

У корпоративних мережах також важливо забезпечити масштабованість VLAN – можливість легко додавати нові сегменти без зміни фізичної структури мережі, що особливо актуально для організацій із динамічною структурою.

У межах розробленої мережі для компанії DoDay VLAN використовуються для розмежування підрозділів на кожному поверсі, ізоляції IoT-пристроїв (зокрема відеокамер), а також для створення окремої VLAN для загальних сервісів, зокрема принтерів та точок доступу. Така структура дозволяє ефективно керувати трафіком, забезпечити контроль доступу та підвищити загальний рівень кібербезпеки корпоративної мережі.

1.7 Інтернет речей (IoT) у корпоративних мережах

Інтернет речей (Internet of Things, IoT) є однією з провідних технологій, що змінюють сучасні корпоративні мережі. В її основі лежить об’єднання фізичних пристроїв, які здатні автоматично передавати дані через мережу без участі користувачів. Це відкриває широкі можливості для автоматизації бізнес-процесів, моніторингу, контролю та забезпечення безпеки.

У корпоративному середовищі IoT найчастіше застосовується для реалізації систем відеоспостереження, розумного освітлення, управління кліматом, контролю доступу та інших компонентів «розумного» офісу. Завдяки постійному збору та аналізу даних у режимі реального часу підприємства можуть приймати більш обґрунтовані рішення, оперативно реагувати на події і підвищувати загальну ефективність роботи.

Водночас інтеграція IoT-пристроїв у корпоративну мережу вимагає ретельного підходу до проєктування. Особливу увагу слід приділяти безпеці, ізоляції трафіку, оптимізації пропускної здатності та централізованому управлінню. Одним із важливих рішень є виділення окремої VLAN для

IoT-пристроїв, що дозволяє логічно ізолювати їх від основної мережі та обмежити доступ.

У проєкті корпоративної мережі компанії DoDay до IoT включено, передусім, камери відеоспостереження, встановлені у всіх ключових зонах офісів. Вони підключені через спеціалізоване мережеве обладнання та працюють у межах окремої підмережі, що підвищує рівень безпеки та спрощує адміністрування системи.

1.8 Основи адміністрування та контролю доступу

Ефективне адміністрування корпоративної мережі є ключовою умовою для забезпечення її стабільної роботи, безпеки та гнучкого управління інформаційними потоками. Сучасний підхід до адміністрування охоплює не лише технічне обслуговування мережевого обладнання, а й впровадження політик доступу, моніторинг трафіку, керування правами користувачів та ведення журналів подій.

Важливим елементом управління мережею є контроль доступу, який реалізується за допомогою списків контролю доступу (ACL), протоколів шифрування і автентифікації, а також логічного сегментування мережі. Це дозволяє обмежувати або надавати доступ до ресурсів на основі IP-адрес, VLAN, типу пристрою чи ролі користувача.

Застосування таких методів забезпечує надійний захист від внутрішніх та зовнішніх загроз, а також дає змогу гнучко розмежовувати доступ між різними підрозділами компанії. У великих або розподілених корпоративних мережах адміністрування також включає централізований моніторинг за допомогою протоколів, таких як SNMP, безпечне керування через SSH, а також регулярне оновлення політик безпеки.

У мережі компанії DoDay особлива увага приділена обмеженню доступу між VLAN, захисту інтерфейсів управління маршрутизаторів і комутаторів, а також впровадженню VPN для безпечного підключення віддалених офісів через

виділений маршрутизатор. Такі рішення забезпечують ефективне адміністрування мережевої інфраструктури та підтримання її цілісності в умовах динамічного середовища.

РОЗДІЛ 2
ПРОЄКТУВАННЯ КОРПОРАТИВНОЇ МЕРЕЖІ КОМПАНІЇ DODAY

2.1 Аналіз вимог до корпоративної мережі

Проєктування корпоративної мережі для компанії DoDay має враховувати особливості роботи організації, її потреби у стабільному та безпечному доступі до різноманітних ресурсів, а також вимоги до ефективної роботи віддалених офісів. Мережа повинна забезпечити не тільки стабільний зв’язок між підрозділами, а й оптимізовану роботу з даними, відеоспостереженням, а також з різними системами автоматизації. Зокрема, важливим аспектом є інтеграція камер відеоспостереження як частини IoT-системи, що мають забезпечити моніторинг безпеки на всіх поверхах офісу [8].

Одним із основних критеріїв є висока надійність і відмовостійкість мережі. Компанія активно використовує різноманітні онлайн-системи для обміну інформацією, CRM-системи для обслуговування клієнтів і спільної роботи, а також проводить відеоконференції. Тому збої в мережі можуть серйозно вплинути на продуктивність і призвести до втрати важливих даних. Для забезпечення безперебійної роботи необхідно враховувати резервування з’єднань, ефективну маршрутизацію трафіку та оптимальні способи його моніторингу [9].

Враховуючи наявність різноманітних відділів і пристроїв, важливо організувати логічну сегментацію мережі через використання VLAN. Це дозволить не лише зменшити навантаження на мережу, а й підвищити її безпеку, адже кожен відділ та група пристроїв (наприклад, IoT-система з камерами відеоспостереження) будуть працювати в окремому сегменті мережі [10]. Для підвищення контролю над трафіком кожен сегмент буде мати свою окрему VLAN, що дозволить ізолювати дані різних відділів та пристроїв, а також забезпечити легше адміністрування мережі.

Ще одним важливим аспектом є питання інформаційної безпеки. Компанія має справу з конфіденційними даними клієнтів і партнерів, фінансовою

інформацією та внутрішньою документацією. Тому впровадження засобів захисту даних, таких як ACL (списки контролю доступу), а також використання безпечних каналів зв’язку через SSH для адміністрування мережевих пристроїв і SNMP для моніторингу мережевих подій, є надзвичайно важливими для забезпечення цілісності та безпеки інформації [11].

Мережа повинна також підтримувати систему підключення до віддалених офісів через VPN. Оскільки компанія має кілька віддалених офісів у Львові та Харкові, важливо організувати безпечний і надійний обмін даними між головним офісом і віддаленими локаціями. Для цього буде використано шифрування даних і протоколи автентифікації, що забезпечать захищений доступ до ресурсів компанії.

Що стосується бездротового доступу, компанія планує впровадити Wi-Fi 6 у зонах загального користування, таких як рецепція і конференц-зал. Wi-Fi 6 забезпечить високу швидкість передачі даних, що дозволить одночасно підтримувати роботу великої кількості пристроїв без втрати якості з’єднання.

Таким чином, основні вимоги до корпоративної мережі включають високий рівень безпеки, ефективну сегментацію трафіку за допомогою VLAN, надійне резервування та відмовостійкість, безпечний доступ до віддалених офісів через VPN, а також підтримку сучасних стандартів бездротового доступу.

2.2 Фізична структура мережі

Фізична структура корпоративної мережі компанії DoDay є важливим етапом у забезпеченні ефективної роботи офісу та віддалених локацій. Структура мережі повинна бути оптимізованою для швидкої передачі даних, забезпечення безпеки і стабільної роботи всіх підрозділів, зокрема в умовах інтеграції IoT-пристроїв, таких як камери відеоспостереження.

Фізична структура мережі компанії DoDay має на меті забезпечити підключення всіх пристроїв, що працюють в офісі та віддалених локаціях.

Офісна мережа складається з двох поверхів, на кожному з яких розміщено різні відділи та технічне обладнання.

На першому поверсі розташовано кілька основних підрозділів: відділ маркетингу, відділ підтримки клієнтів, IT-відділ і рецепція. Для забезпечення ефективної роботи на цьому поверсі мережеві пристрої (комп'ютери, камери відеоспостереження, точка доступу Wi-Fi) підключаються через комутатори, які обробляють локальний трафік. Відповідно до схеми першого поверху (рис. 2.1), підключення до мережі буде організовано через комутатори, що дозволяє зручно розділяти трафік між різними відділами та підключенням до сервера. Для камер відеоспостереження використано окремі комутатори на обох поверхах.

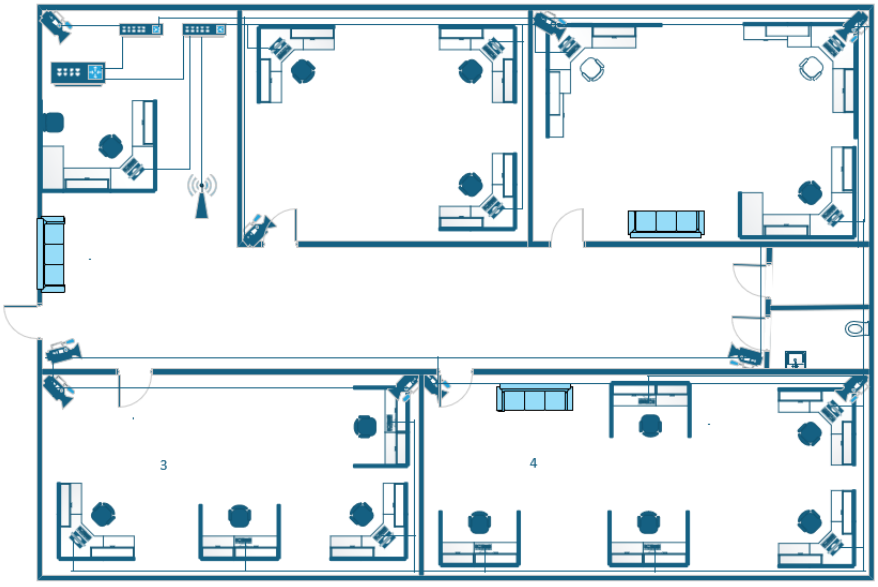

Рисунок 2.1 – План мережі першого поверху

На другому поверсі знаходиться кабінет керівника, бухгалтерія, юридичний відділ, навчальний клас та конференц-зал. Крім того, на цьому поверсі розташовані камери відеоспостереження, серверне обладнання та інші критично важливі пристрої. Логічне підключення цього поверху також здійснюється через комутатори, що дозволяє організувати ефективну маршрутизацію між відділами і забезпечити безперебійний доступ до корпоративних ресурсів. Відповідно до схеми другого поверху (рис. 2.2), всі

пристрої з’єднані через окремі порти комутаторів, що відповідають за трафік кожного відділу.

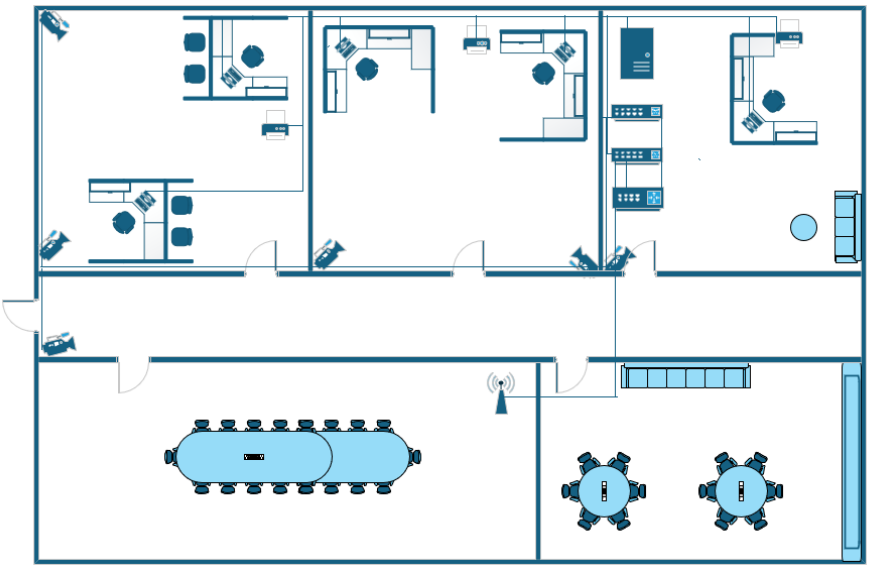

Рисунок 2.2 – План мережі другого поверху

Крім того, для зв’язку між поверхами використовуються високошвидкісні оптоволоконні лінії, що забезпечують необхідну швидкість передачі даних. Спеціальні маршрутизатори на кожному з поверхів здійснюють маршрутизацію трафіку між мережевими сегментами і підключаються до основного маршрутизатора в серверній кімнаті, що розташована на другому поверсі.

Окрім центрального офісу, корпоративна мережа компанії DoDay включає три віддалені офіси, що розташовані в містах Київ, Львів та Харків. Кожен з цих офісів має власну локальну мережу, інтегровану до загальної корпоративної інфраструктури через захищені VPN-з’єднання. Основна мета фізичної організації мережі у віддалених локаціях – забезпечити стабільне підключення працівників до ресурсів головного офісу.

Фізична структура кожного з віддалених офісів є спрощеною, оскільки передбачає лише підключення персональних комп’ютерів співробітників. Усі ПК об’єднані за допомогою комутатора, який підключено до маршрутизатора з налаштованим VPN-тунелем до центрального офісу. Такий підхід дозволяє

забезпечити базову функціональність, необхідну для віддаленої роботи та обміну даними з головною мережею компанії.

На фізичних схемах мережі для кожного офісу (рис. 2.3-2.5) відображено розташування обладнання та особливості підключення.

У Києві (рис. 2.3) ПК працівників підключено до комутатора, який зв’язується з маршрутизатором, що забезпечує захищений VPN-зв’язок із центральним офісом.

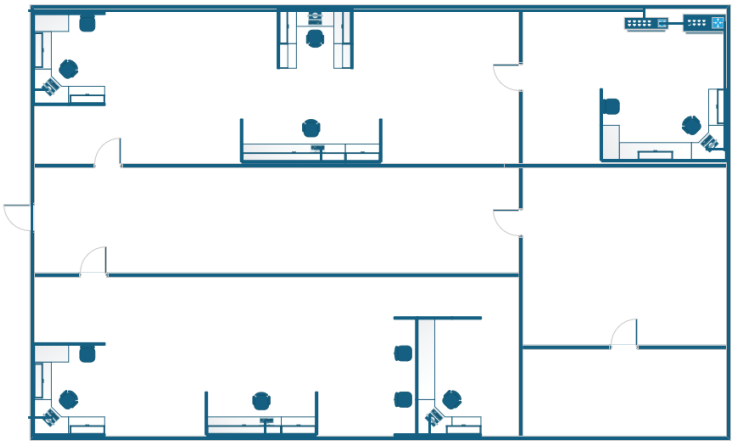

Рисунок 2.3 – План мережі віддаленого офісу в Києві

У Львові (рис. 2.4) реалізовано аналогічну структуру: ПК об’єднані через комутатор, підключений до маршрутизатора з тунельним з’єднанням до центрального маршрутизатора компанії.

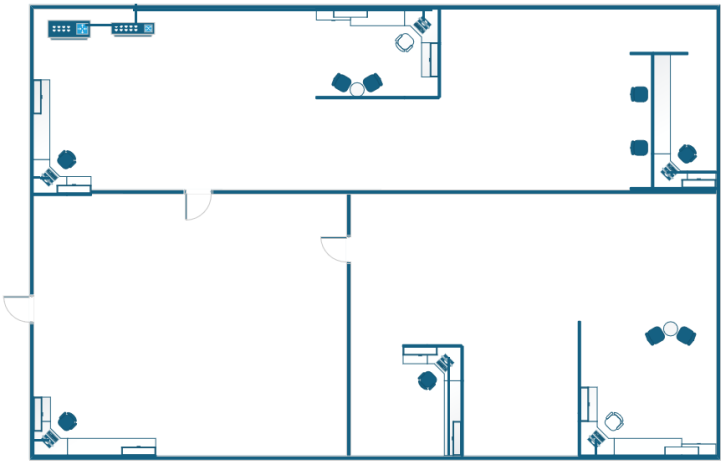

Рисунок 2.4 – План мережі віддаленого офісу в Львові

У Харкові (рис. 2.5) структура ідентична – ПК підключені до локального комутатора, з’єднаного з маршрутизатором, через який здійснюється VPN-зв’язок із центральним офісом.

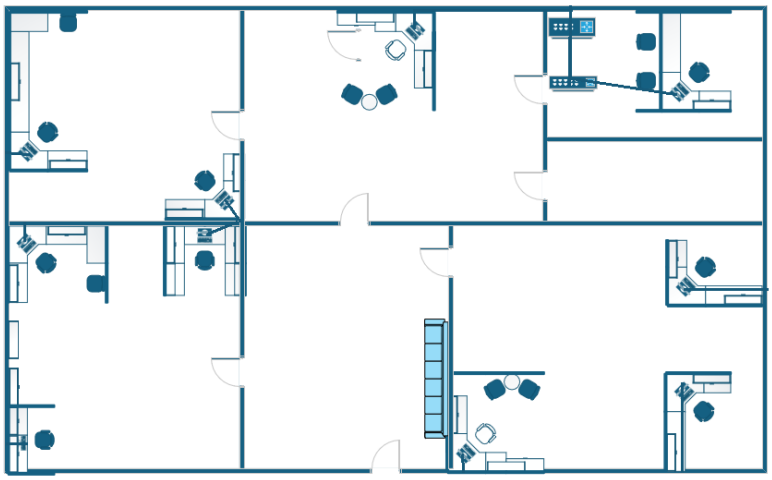

Рисунок 2.5 – План мережі віддаленого офісу в Харкові

Фізична організація мережі в цих офісах дозволяє зберігати єдину логіку побудови інфраструктури, спрощує адміністрування та підвищує надійність доступу до корпоративних сервісів незалежно від місця розташування працівників.

2.3 Вибір мережевого обладнання

Процес вибору мережевого обладнання є одним із ключових етапів у проєктуванні корпоративної мережі, адже саме він визначає стабільність, надійність, безпеку, ефективність і можливість масштабування інформаційної інфраструктури компанії. Вибір технічних засобів здійснюється з урахуванням кількості користувачів, типу та площі приміщень, необхідної пропускної здатності каналів, потреби в сегментації трафіку за допомогою VLAN, підтримки сучасних протоколів маршрутизації (зокрема OSPF), централізованого моніторингу мережі та засобів безпеки, включаючи шифрування, автентифікацію та контроль доступу.

У типовому корпоративному середовищі використовується комбінація керованих комутаторів другого та третього рівнів, маршрутизаторів із підтримкою VPN і динамічної маршрутизації, серверного обладнання, бездротових точок доступу, периферійних пристроїв і систем відеонагляду. В умовах стрімкого розвитку Інтернету речей та кіберзагроз пріоритет надається обладнанню з підтримкою захищеного віддаленого керування, шифрування даних, ізоляції трафіку та швидкої реакції на інциденти.

Для реалізації корпоративної мережі компанії DoDay було обрано обладнання, що відповідає сучасним вимогам щодо продуктивності, безпеки, сумісності з різними протоколами та подальшого масштабування. В головному офісі використано маршрутизатори різних виробників, кожен з яких виконує власну роль у мережевій структурі.

Центральним елементом є маршрутизатор Cisco ISR 4331 (рис. 2.6), який відповідає за маршрутизацію між VLAN усередині головного офісу, а також підтримує динамічний протокол OSPF. Він обладнаний вбудованими модулями шифрування, підтримує масштабування обчислювальної потужності та забезпечує продуктивність до 300 Мбіт/с, що є цілком достатнім для навантаження всіх відділів офісу.

Рисунок 2.6 – Маршрутизатор Cisco ISR 4331 [12]

Другий маршрутизатор MikroTik CCR1009-7G-1C-1S+ (рис. 2.7) відповідає за маршрутизацію на другому поверсі головного офісу, де розміщені критично важливі підрозділи: керівництво, бухгалтерія, юридичний відділ. Завдяки

потужному процесору Tilera Tile-Gx9, великій кількості гігабітних інтерфейсів і підтримці апаратного шифрування IPsec цей маршрутизатор дозволяє забезпечити швидку та безперебійну маршрутизацію VLAN-трафіку, не створюючи додаткового навантаження на центральний маршрутизатор.

Рисунок 2.7 – Маршрутизатор MikroTik CCR1009-7G-1C-1S+ [13]

Третій та четвертий маршрутизатори Ubiquiti EdgeRouter 4 (рис. 2.8) використовуються виключно для створення VPN-з’єднань із віддаленими офісами компанії в інших містах, зокрема у Львові, Харкові та Києві. Він підтримує сучасні VPN-протоколи, включаючи GRE, що дозволяє створити захищені канали для передавання даних між офісами. Завдяки чотириядерному процесору EdgeRouter 4 здатен ефективно обробляти трафік без шкоди для продуктивності основної мережі, а його інтерфейс EdgeOS дозволяє зручно керувати конфігурацією пристрою.

Рисунок 2.8 – Маршрутизатор Ubiquiti EdgeRouter 4 [14]

Комутатори в головному офісі також відрізняються залежно від завдань. Для комп’ютерів та точок доступу використовуються Cisco Catalyst 2960X (рис. 2.9), які мають підтримку Gigabit Ethernet, VLAN, STP, PoE, SNMP, що забезпечує надійну та гнучку організацію локального доступу.

Рисунок 2.9 – Комутатор Cisco Catalyst 2960X [15]

Для підключення IP-камер обрано окремі комутатори з підтримкою PoE, зокрема моделі TP-Link TL-SG2428P (рис. 2.10), що дозволяють не тільки передавати дані, але й живити камери відеоспостереження, зменшуючи потребу в додатковому електроживленні.

Рисунок 2.10 – Комутатор TP-Link TL-SG2428P [16]

У ролі бездротових точок доступу обрано Cisco Aironet 1832i (рис. 2.11), які забезпечують стабільне з’єднання за стандартом Wi-Fi 802.11ac Wave 2, підтримують MU-MIMO та здатні обслуговувати велику кількість пристроїв у конференц-залі та рецепції.

Рисунок 2.11 – Бездротова точока доступу Cisco Aironet 1832i [17]

У мережі використовуються IP-камери Ubiquiti UniFi G3 (рис. 2.12), які встановлені як на першому, так і на другому поверхах. Ці камери забезпечують високу роздільну здатність відео, інтеграцію з мережею, централізоване керування та запис на сервер. Загалом у проєкті використано 17 камер – 10 на першому поверсі (включаючи рецепцію, маркетинг, підтримку клієнтів, IT-відділ, навчальний клас) і 7 на другому поверсі (включаючи кабінет керівника, бухгалтерію, юридичний відділ та загальні зони поверху).

Рисунок 2.12 – IP-камера Ubiquiti UniFi G3 [18]

Сервер HP ProLiant ML350 Gen10 (рис. 2.13), розміщено в кабінеті керівника. Він виконує роль DHCP-сервера, а також забезпечує функції HTTP/FTP-сервера для зберігання відеозаписів із камер. У майбутньому сервер може бути використаний як файловий або резервний сервер для розміщення критичних даних компанії.

Рисунок 2.13 – Сервер HP ProLiant ML350 [19]

Віддалені офіси компанії в містах Львів, Харків та Київ. У кожному з них встановлено маршрутизатор Ubiquiti EdgeRouter X (рис. 2.14), комутатор TP-Link TL-SG2210P (рис. 2.15), для підключення комп’ютерного обладнання, а також базове периферійне обладнання.

Таке уніфіковане рішення дозволяє значно спростити налаштування, забезпечити централізоване адміністрування та легкість масштабування в разі відкриття нових філій.

Рисунок 2.14 – Маршрутизатор Ubiquiti EdgeRouter X [20]

Рисунок 2.15 – Комутатор TP-Link TL-SG2210P [21]

Обрана апаратна конфігурація дозволяє реалізувати безпечну, стабільну й масштабовану корпоративну мережу для компанії DoDay, яка забезпечує ефективну взаємодію між усіма відділами головного офісу та віддаленими підрозділами.

РОЗДІЛ 3
РЕАЛІЗАЦІЯ ТА НАЛАШТУВАННЯ КОРПОРАТИВНОЇ МЕРЕЖІ

3.1 Розробка логічної структури мережі

Логічна структура корпоративної мережі компанії DoDay охоплює головний офіс (двоповерхову будівлю) та три віддалені офіси, з’єднані захищеними VPN-тунелями.

Мережа розроблена з урахуванням вимог до безпеки, масштабованості та ефективного управління. Вона побудована з використанням VLAN, OSPF-маршрутизації, NAT, ізоляції IoT-пристроїв (камер спостереження) та централізованого зберігання даних на сервері.

3.1.1 Логічна схема мережі

Мережа побудована за ієрархічною структурою з поділом на логічні сегменти відповідно до відділів компанії. Для кожного підрозділу головного офісу створено окрему VLAN, що забезпечує ізоляцію трафіку та контроль доступу.

У головному офісі встановлено два маршрутизатори (по одному на поверх), які забезпечують локальну маршрутизацію через OSPF.

Центральним вузлом виступає Router3, який також забезпечує VPN-з’єднання з віддаленими офісами (Київ, Львів, Харків).

IoT-пристрої (камери спостереження) виділені в окремі VLAN та підключені через окремі комутатори. Усі відеопотоки надсилаються на сервер із підтримкою HTTP/FTP.

Віддалені офіси мають власні локальні мережі та підключені до центрального маршрутизатора через VPN. Реалізовано NAT для забезпечення взаємодії з сервером і внутрішніми ресурсами.

Загальну логічну структуру представлено на рисунку 3.1.

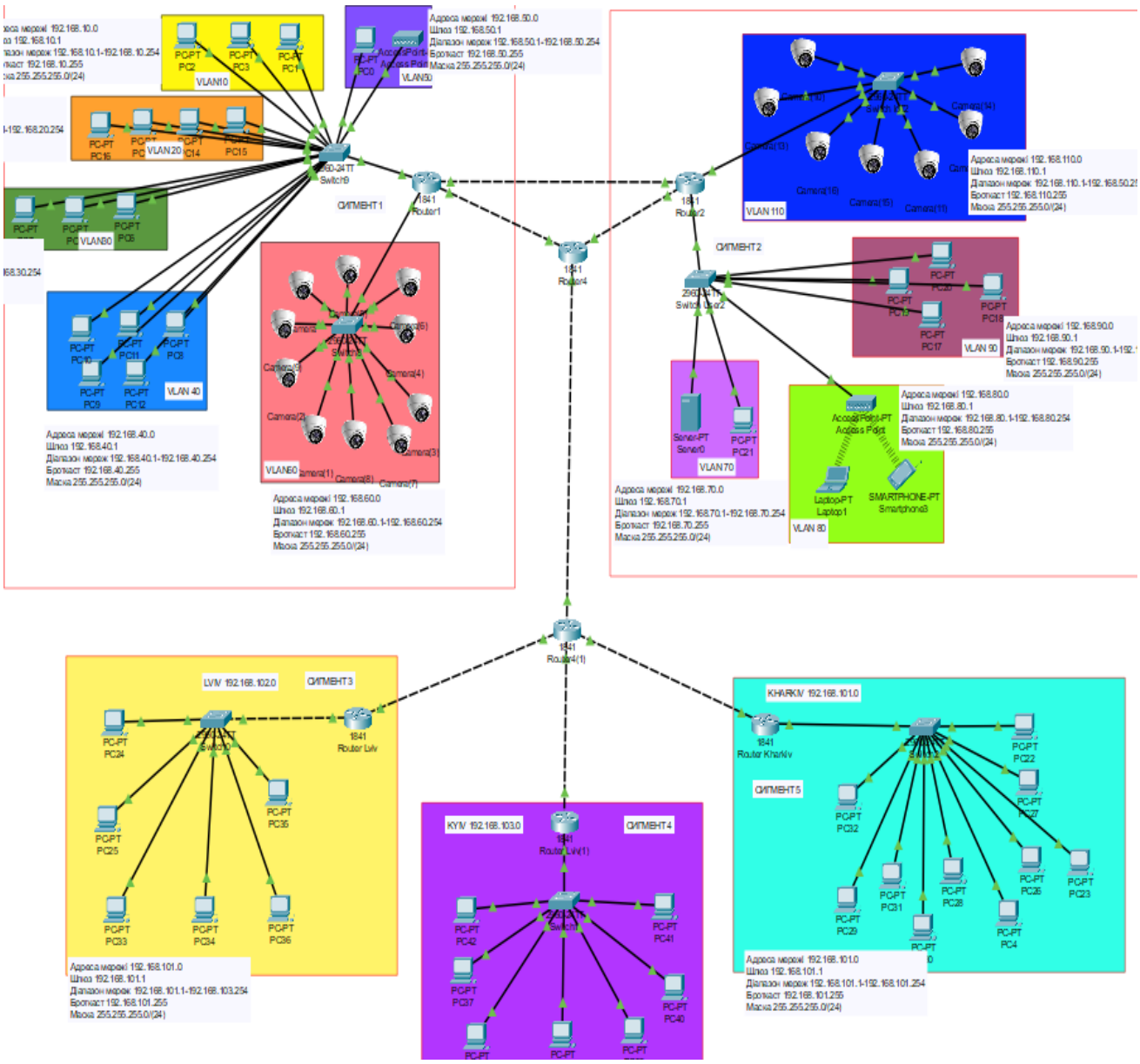

Рисунок 3.1 – Логічна схема мережі

Перший поверх головного офісу поділений на VLAN для відділів маркетингу, підтримки клієнтів, IT, рецепції та навчального класу. Камери спостереження підключені в окремий VLAN IoT, що забезпечує ізоляцію трафіку. Безпроводові точки доступу також виділені в окремий VLAN.

Загальну логічну структуру першого поверху (сегмент 1) представлено на рисунку 3.2

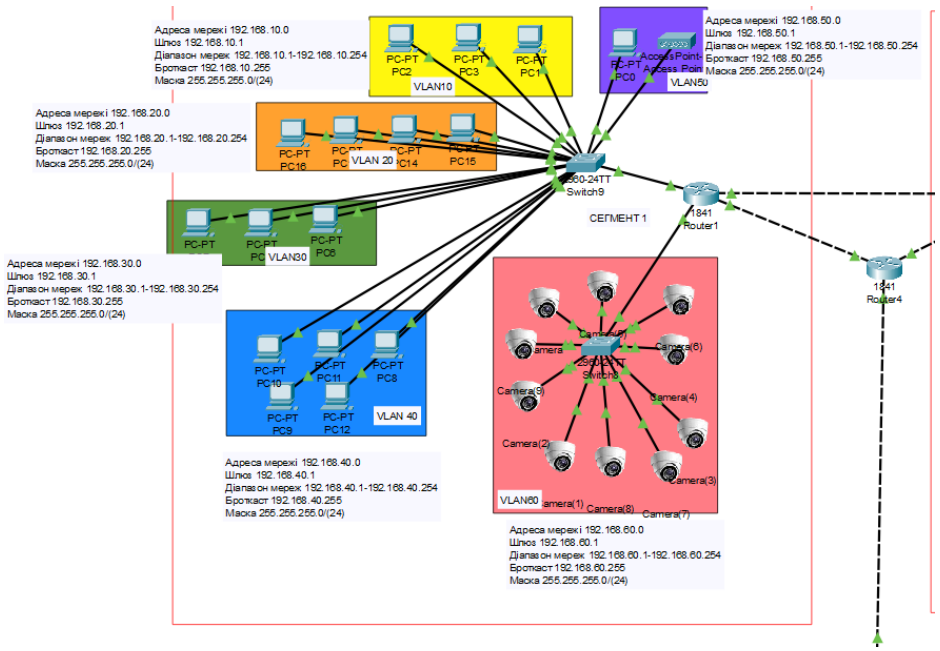

Рисунок 3.2 – Логічна схема мережі першого поверху

Другий поверх містить VLAN для кабінету керівника, бухгалтерії, юридичного відділу та конференц-залу. Сервер із статичною IP-адресою розташований у VLAN керівництва. Камери і бездротові точки доступу мають власні VLAN. Всі пристрої взаємодіють через OSPF. Топологія другого поверху відображена на рисунку 3.3.

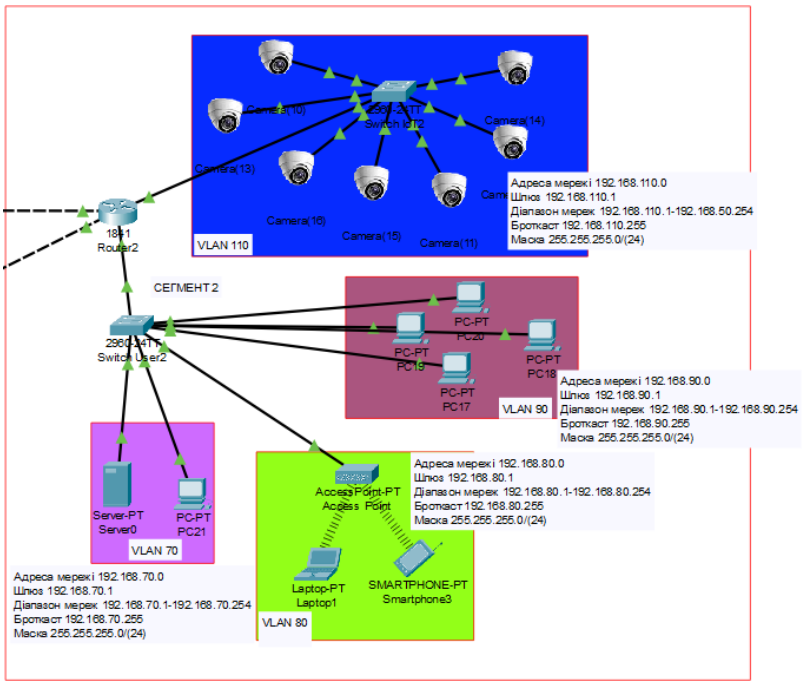

Рисунок 3.3 – Логічна схема мережі другого поверху

Віддалені офіси в Києві, Львові та Харкові підключені до головної мережі через захищені VPN-тунелі. У кожному офісі локальна мережа організована за принципом VLAN-сегментації, що виділяє робочі станції та бездротовий доступ, із відповідними заходами безпеки, включаючи ACL і шифрування тунелів. Логічні схеми віддалених офісів наведені відповідно на рисунках 3.4, 3.5 та 3.6

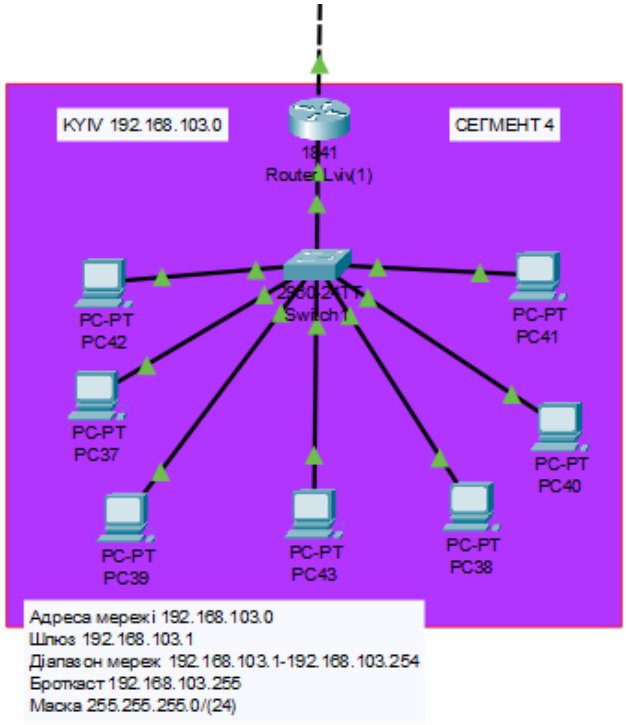

Рисунок 3.4 – Логічна схема мережі віддаленого офісу в Києві

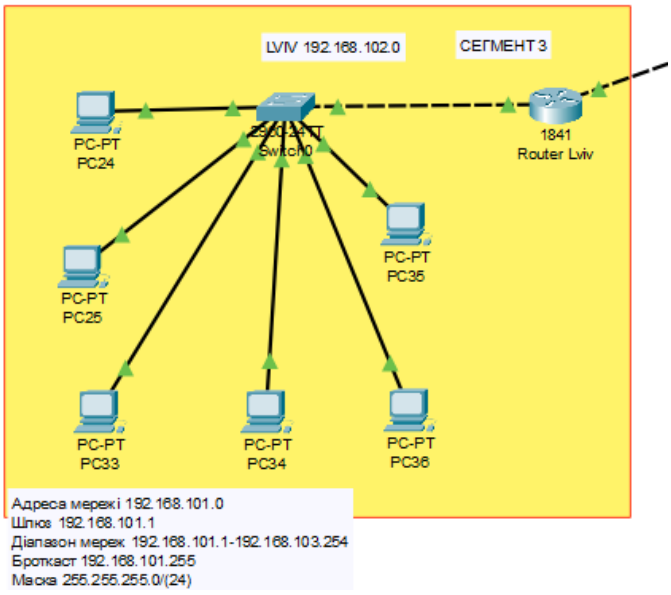

Рисунок 3.5 – Логічна схема мережі віддаленого офісу в Львові

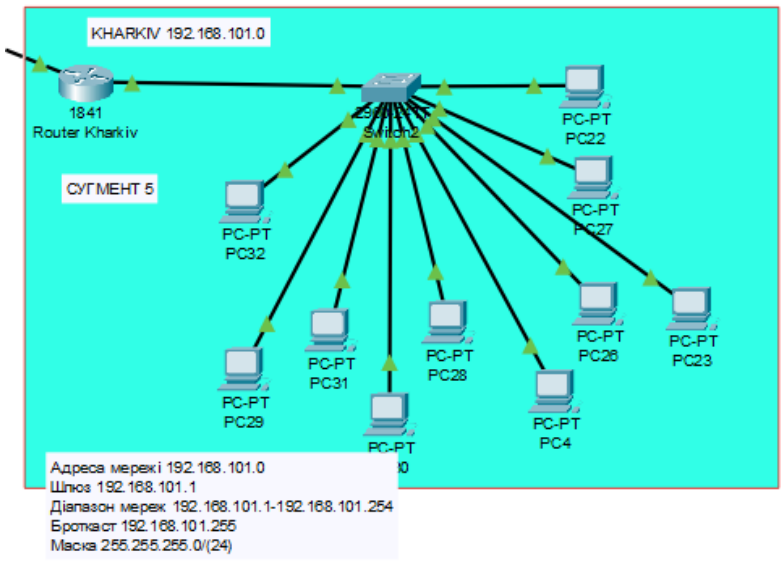

Рисунок 3.6 – Логічна схема мережі віддаленого офісу в Харкові

3.1.2 Розрахунок логічної адресації

Для ефективної організації мережі було здійснено ретельний розрахунок логічної адресації з метою оптимального використання IP-простору та забезпечення коректної маршрутизації між різними VLAN. В основі планування IP-адрес лежить приватний діапазон IPv4, який відповідає стандарту RFC 1918. Для кожного VLAN виділено окрему підмережу з відповідною маскою, що дозволяє розмежувати трафік, підвищити безпеку і спростити адміністрування.

Нижче наведена таблиця 3.1, у якій деталізовано VLAN, їх призначення, підмережі, маски, шлюзи за замовчуванням та діапазони IP-адрес, що використовуються у мережі компанії DoDay.

Таблиця 3.1 – VLAN з підмережами, шлюзами та IP-адресами

VLAN / Офіс	Підмережа	Маска	Шлюз за замовчуванням	DHCP пул	Призначення
VLAN 10 Marketing	192.168.10.0	255.255.255.0	192.168.10.1	192.168.10.100-254	ПК відділу маркетингу
VLAN 20 Support	192.168.20.0	255.255.255.0	192.168.20.1	192.168.20.100-254	ПК відділу підтримки
VLAN 30 IT	192.168.30.0	255.255.255.0	192.168.30.1	192.168.30.100-254	ПК IT-відділу

Продовження таблиці 3.1

VLAN / Офіс	Підмережа	Маска	Шлюз за замовчуванням	DHCP пул	Призначення
VLAN 40 Student	192.168.40.0	255.255.255.0	192.168.40.1	192.168.40.100-254	Навчальні класи
VLAN 50 Reception	192.168.50.0	255.255.255.0	192.168.50.1	192.168.50.100-254	Рецепція
VLAN 60 IoT	192.168.60.0	255.255.255.0	192.168.60.1	192.168.60.100-254	IoT-пристрої
VLAN 70 Management	192.168.70.0	255.255.255.0	192.168.70.1	192.168.70.100-254	Керівництво
VLAN 80 Accounting	192.168.80.0	255.255.255.0	192.168.80.1	192.168.80.100-254	Бухгалтерія
VLAN 90 Legal	192.168.90.0	255.255.255.0	192.168.90.1	192.168.90.100-254	Юридичний відділ
VLAN 110 Conference	192.168.110.0	255.255.255.0	192.168.110.1	192.168.110.100-254	Конференц-зал
VLAN 120 IoT	192.168.120.0	255.255.255.0	192.168.120.1	192.168.120.100-254	IoT-пристрої
Server Network	192.168.70.10	255.255.255.0	192.168.70.1	-	HTTP/FTP сервер у VLAN 70
Kharkiv	192.168.101.0	255.255.255.0	192.168.101.1	192.168.101.100-254	Віддалений офіс Харків
Lviv	192.168.102.0	255.255.255.0	192.168.102.1	192.168.102.100-254	Віддалений офіс Львів
Kyiv	192.168.103.0	255.255.255.0	192.168.103.1	192.168.103.100-254	Віддалений офіс Київ

Для кожного VLAN і віддаленого офісу налаштовані DHCP-пули, які забезпечують автоматичне призначення IP-адрес кінцевим пристроям. Використання таких пулів дозволяє централізовано керувати видачею адрес і уникнути конфліктів у мережі. Статична IP-адреса 192.168.70.10 виділена для HTTP/FTP сервера, що розміщений у VLAN 70, для забезпечення стабільного доступу до серверних ресурсів.

3.2 Налаштування мережевого обладнання

На першому етапі створення корпоративної мережі компанії DoDay виконується налаштування основного мережевого обладнання. До складу інфраструктури входять маршрутизатори, керовані комутатори другого рівня, а також сервер, який виступає в ролі файлового сховища. Всі пристрої попередньо розміщуються у Cisco Packet Tracer, після чого здійснюється конфігурація відповідно до заданої топології та логічної адресації (табл. 3.1).

Налаштування починається з базових параметрів маршрутизаторів та комутаторів. Під час віртуального моделювання мережі використовується Cisco Packet Tracer, в реальному проєкті передбачено обладнання різних брендів. Для зручності адміністрування задаються імена пристроїв, вимикається автоматичне визначення швидкості портів, налаштовуються паролі доступу, а також активуються необхідні інтерфейси. Приклад налаштування наведено на рисунку 3.7.

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R2_doday
R2_doday(config)#interface GigabitEthernet0/0/0
R2_doday(config-if)#ip address 192.168.2.1 255.255.255.0
R2_doday(config-if)#no shutdown

R2_doday(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0, changed state to up
exit
R2_doday(config)#interface GigabitEthernet0/0/1
R2_doday(config-if)#ip address 192.168.12.1 255.255.255.0
R2_doday(config-if)#no shutdown

R2_doday(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1, changed state to up
exit
R2_doday(config)#enable secret doday123
R2_doday(config)#line console 0
R2_doday(config-line)#password doday2025
R2_doday(config-line)#login
R2_doday(config-line)#exit
R2_doday(config)#line vty 0 4
R2_doday(config-line)#password dodayvty
R2_doday(config-line)#login
R2_doday(config-line)#exit
R2_doday(config)#end
R2_doday#
%SYS-5-CONFIG_I: Configured from console by console
write memory
Building configuration...
[OK]
R2 doday#
```

Рисунок 3.7 – Конфігурація базових налаштувань маршрутизатора R1_doday

Аналогічні команди застосовуються до інших маршрутизаторів і комутаторів (Router2, Router3, Switch1 тощо), з індивідуальними назвами.

Для забезпечення взаємодії з різними сегментами мережі використовується підінтерфейсна маршрутизація. Кожному підінтерфейсу призначається IP-адреса, що виступає шлюзом для відповідної підмережі (рис. 3.8).

```
R1_doday(config)#interface FastEthernet0/0.10
R1_doday(config-subif)# encapsulation dot1Q 10
R1_doday(config-subif)# ip address 192.168.10.1 255.255.255.0
R1_doday(config-subif)#interface FastEthernet0/0.20
R1_doday(config-subif)# encapsulation dot1Q 20
R1_doday(config-subif)# ip address 192.168.20.1 255.255.255.0
```

Рисунок 3.8 – Приклад налаштування підінтерфейсів

Таким чином, маршрутизатор забезпечує доступність мережевих ресурсів для окремих сегментів.

На комутаторах створюються базові VLAN (рис. 3.9) (їх створення та прив’язка портів описується в іншому розділі), а порти переводяться в потрібний режим.

```
Switch1>enable
Switch1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch1(config)#vlan 10
Switch1(config-vlan)#name Marketing
Switch1(config-vlan)#exit
Switch1(config)#interface fastEthernet 0/1
Switch1(config-if)#switchport mode access
Switch1(config-if)#switchport access vlan 10
```

Рисунок 3.9 – Створення VLAN

Для того щоб пристрої в мережі автоматично отримували IP-адреси, на маршрутизаторі налаштовується DHCP-сервер. Спочатку виключаємо частину адрес, які призначені для шлюзів або серверів (наприклад, 192.168.10.1 – 192.168.10.10), щоб уникнути конфліктів.

Після цього створюються окремі DHCP-пули для кожної VLAN. У кожному пулі вказується, яка мережа використовується, маска, шлюз за замовчуванням і DNS-сервер. Приклад для VLAN10 наведено на рисунку 3.10.

```
R1_doday(config)#ip dhcp excluded-address 192.168.10.1 192.168.10.10
R1_doday(config)#ip dhcp pool VLAN10
R1_doday(dhcp-config)#network 192.168.10.0 255.255.255.0
R1_doday(dhcp-config)#default-router 192.168.10.1
R1_doday(dhcp-config)#dns-server 8.8.8.8
```

Рисунок 3.10 – Створення DHCP-пулів

Аналогічно налаштовуються пули для інших VLAN.

Коли DHCP активний, будь-який пристрій у відповідній VLAN, який має ввімкнений режим «отримати IP автоматично», після підключення до мережі отримає IP-адресу, маску, шлюз і DNS автоматично. Наприклад, комп'ютер, підключений до VLAN10, може отримати адресу 192.168.10.13, якщо вона вільна.

У Cisco Packet Tracer це перевіряється через вкладку IP Configuration на пристрої –потрібно вибрати режим DHCP і через кілька секунд адреса з'явиться автоматично, якщо налаштування правильні (рис. 3.11).

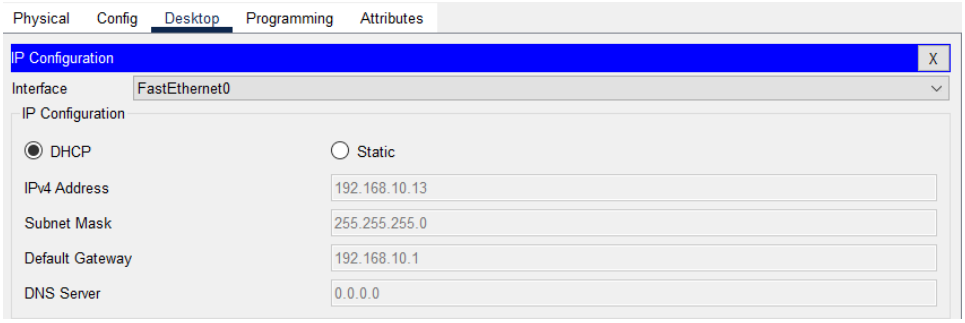

Рисунок 3.11 – DHCP налаштування на одному з ПК

Після підключення сервера до комутатора керівництва на другому поверсі, переходимо до його налаштування. У вікні IP Configuration на вкладці Desktop вказуємо IP-адресу вручну, оскільки цей сервер має працювати з постійною адресою. Встановлюємо IP: 192.168.70.10, маску підмережі 255.255.255.0,

а шлюзом за замовчуванням виступає адреса інтерфейсу маршрутизатора VLAN 70 – 192.168.70.1 (рис. 3.12).

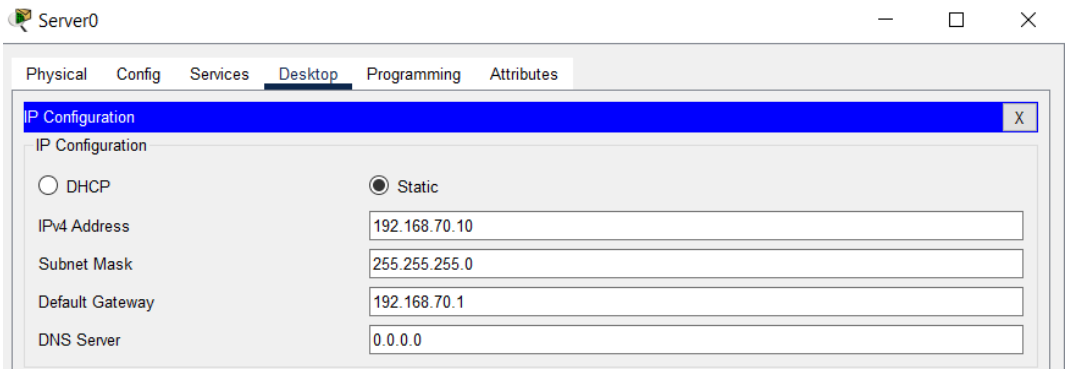

Рисунок 3.12 – Налаштування статичної IP- адреси для сервера

Далі активуємо потрібні служби сервера. У вкладці Services обираємо розділ HTTP і переконуємось, що сервер увімкнено (відмітка ON). Це дозволить іншим пристроям мережі, зокрема комп'ютерам працівників, отримувати доступ до веб-ресурсів, що будуть розміщені на сервері. Вмикаємо веб-сервер, переконуємося, що опція активна, та редагуємо HTML-код сторінки, яка відображатиметься користувачам при зверненні до IP-адреси сервера через браузер. Додаємо заголовок із назвою компанії DoDay та повідомлення про те, що це сервер для зберігання відео із камер спостереження (рис. 3.13).

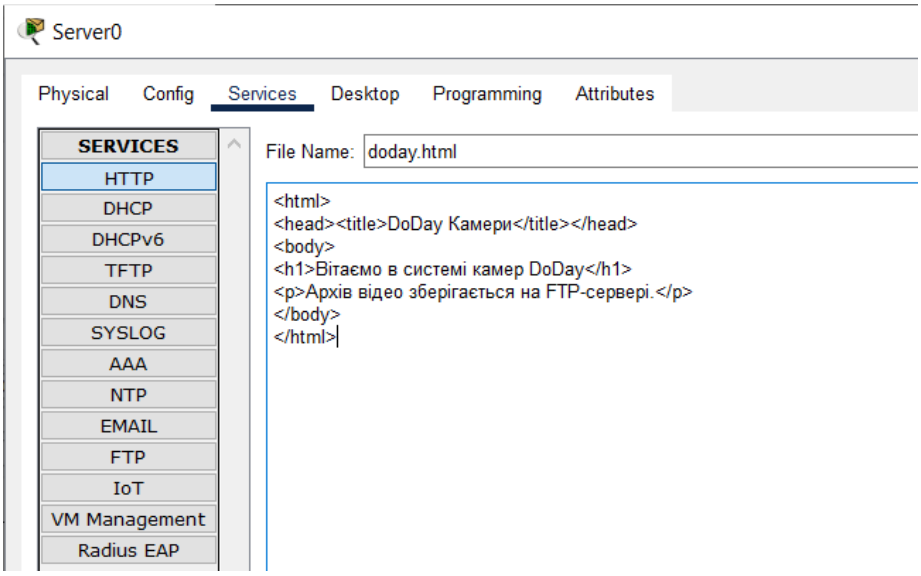

Рисунок 3.13 – Налаштування HTML-коду

Одразу ж у тій же вкладці переходимо до розділу FTP та активуємо службу обміну файлами, що необхідна для прийому відео з камер. Створюємо окремий обліковий запис: ім’я користувача camera_doday, пароль doday2025 (рис. 3.14). Саме через цей акаунт IP-камери будуть авторизуватись на сервері для надсилання файлів

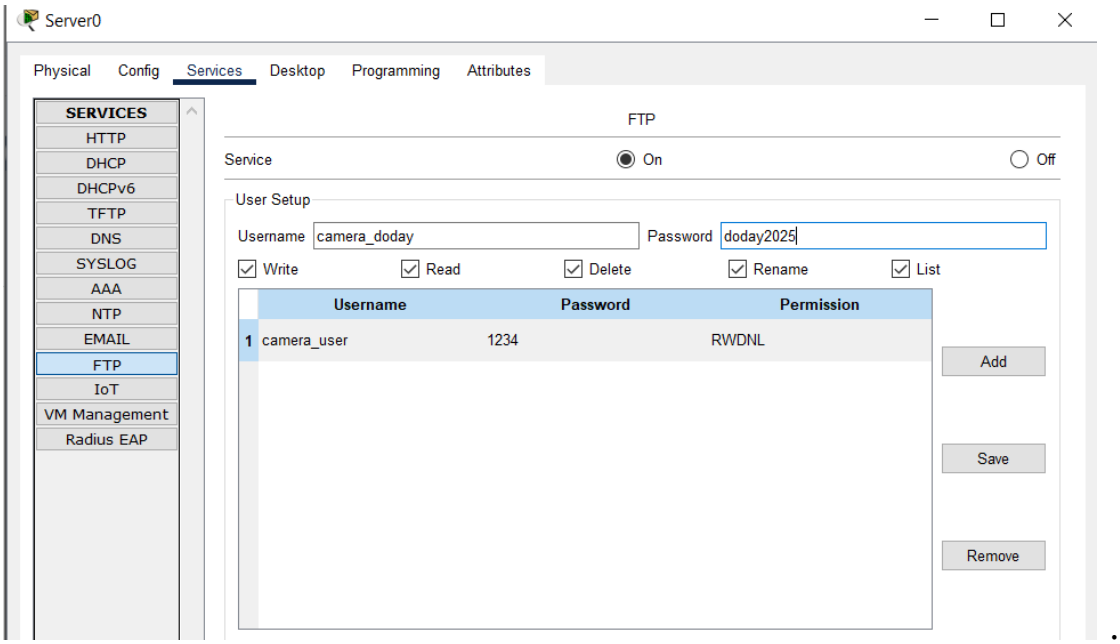

Рисунок 3.14 – Налаштування FTP

Після завершення налаштувань перевіряємо коректність роботи сервера. Відкриваємо браузер на будь-якому пристрої в мережі й переходимо за адресою http://192.168.70.10 – має відображатись підготовлена HTML-сторінка (рис. 3.15).

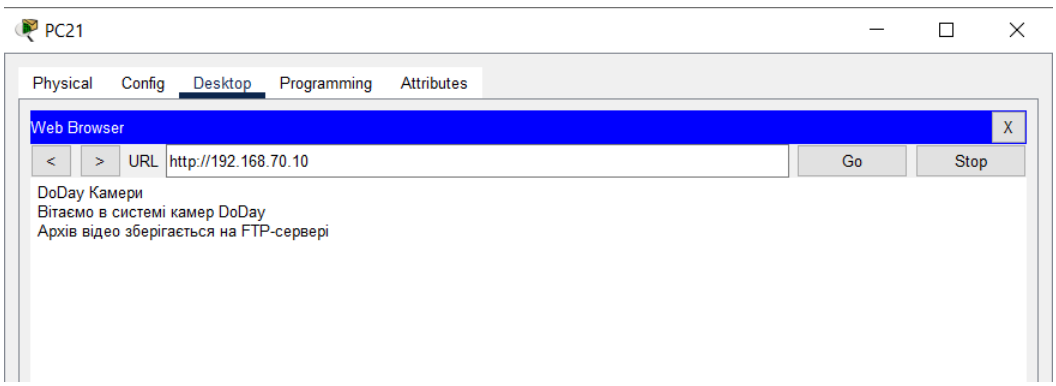

Рисунок 3.15 – HTTP запит до серверу

Для перевірки FTP-з’єднання можна використати інший пристрій у мережі: вводимо IP-адресу сервера в Command Prompt, авторизуємось через camera_doday / doday2025 та перевіряємо доступ до створеної теки (рис. 3.16). Якщо все виконано вірно – сервер успішно виконує роль центра зберігання відео з камер і надає веб-доступ до інформації.

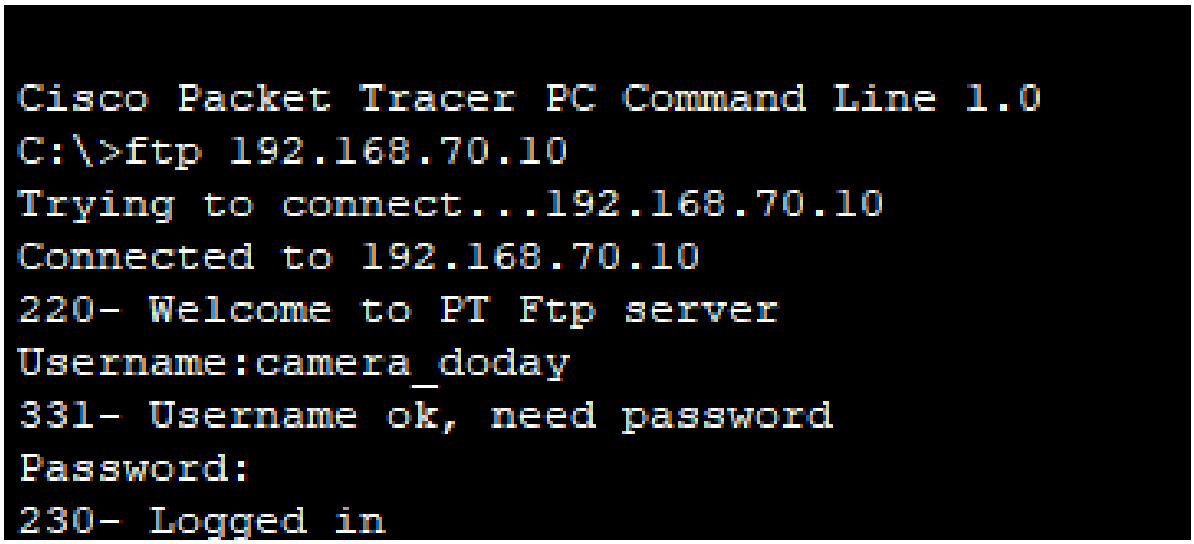

Рисунок 3.16 – Перевірка FTP-з’єднання

3.3 Організація VLAN та міжмережевої взаємодії

Організація VLAN та міжмережевої взаємодії є важливим кроком у створенні корпоративної мережі. Це дозволяє розділити мережевий трафік між різними відділами та IoT-пристроями, підвищуючи безпеку і покращуючи ефективність передачі даних. У ході налаштувань реалізується створення VLAN, їх інтеграція на маршрутизаторі через субінтерфейси, а також впровадження протоколу OSPF, який забезпечує динамічний обмін маршрутами між підмережами для стабільної та гнучкої роботи мережі.

Для розподілу трафіку між різними відділами і пристроями IoT у мережі створюємо VLAN. (рис 3.17). Це дозволяє ізолювати мережі для безпеки та зручності управління. Після створення VLAN призначаємо фізичні порти комутаторів у відповідні VLAN. (рис 3.18).

```
Switch1>enable
Switch1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch1(config)#vlan 10
Switch1(config-vlan)#name Marketing
Switch1(config-vlan)#exit
Switch1(config)#interface fastEthernet 0/1
Switch1(config-if)#switchport mode access
Switch1(config-if)#switchport access vlan 10
```

Рисунок 3.17 – Налаштування VLAN

```
Switch1(config)#interface range fa0/1 - 3
Switch1(config-if-range)#switchport mode access
Switch1(config-if-range)#switchport access vlan 10
Switch1(config-if-range)#exit
```

Рисунок 3.18 – Призначення портів до відповідних VLAN

Для організації міжмережевого маршрутизування між VLAN на маршрутизаторі створюємо субінтерфейси, кожен з яких налаштований з IP-адресою підмережі VLAN (рис. 3.19). Це дозволить комп'ютерам з різних VLAN обмінюватись трафіком.

```
R1_doday(config)#interface GigabitEthernet0/0/1.10
R1_doday(config-subif)# encapsulation dot1Q 10
R1_doday(config-subif)# ip address 192.168.10.1 255.255.255.0
R1_doday(config-subif)# no shutdown
R1_doday(config-subif)#exit
R1_doday(config)#interface GigabitEthernet0/0/1.20
R1_doday(config-subif)# encapsulation dot1Q 20
R1_doday(config-subif)# ip address 192.168.20.1 255.255.255.0
R1_doday(config-subif)# no shutdown
R1_doday(config-subif)#exit
R1_doday(config)#interface GigabitEthernet0/0/1.30
R1_doday(config-subif)# encapsulation dot1Q 30
R1_doday(config-subif)# ip address 192.168.30.1 255.255.255.0
R1_doday(config-subif)# no shutdown
```

Рисунок 3.19 – Налаштування субінтерфейсів маршрутизатора для міжмережевого маршрутизування між VLAN

Налаштовуємо протокол маршрутизації OSPF для автоматичного обміну маршрутами між маршрутизаторами в мережі (рис. 3.20). Це потрібно для забезпечення зв'язку між локальними VLAN і віддаленими офісами.

```
Rl_doday#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Rl_doday(config)#router ospf 1
Rl_doday(config-router)# network 192.168.10.0 0.0.0.255 area 0
Rl_doday(config-router)#network 192.168.20.0 0.0.0.255 area 0
Rl_doday(config-router)#network 192.168.30.0 0.0.0.255 area 0
Rl_doday(config-router)#network 192.168.40.0 0.0.0.255 area 0
Rl_doday(config-router)#network 192.168.50.0 0.0.0.255 area 0
Rl_doday(config-router)#network 192.168.60.0 0.0.0.255 area 0
Rl_doday(config-router)#network 10.255.255.0 0.0.0.3 area 0
Rl doday(config-router)#network 172.16.0.4 0.0.0.3 area 0
```

Рисунок 3.20 – Налаштування OSPF

Перевіряємо конфігурацію VLAN на комутаторах і наявність субінтерфейсів з IP-адресами на маршрутизаторі. Переконуємося, що OSPF працює і маршрути з усіх мереж відомі.

Перевірка створених VLAN виконується за допомогою команди show vlan brief на комутаторі. Вона дозволяє переконатися, що всі віртуальні мережі створені коректно, а порти призначені відповідним VLAN (рис. 3.21).

```
Switch1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                Fa0/22, Fa0/23, Gig0/1, Gig0/2
10   Marketing                        active    Fa0/1, Fa0/2, Fa0/3
20   Support                          active    Fa0/4, Fa0/5, Fa0/6, Fa0/7
30   IT                               active    Fa0/8, Fa0/9, Fa0/10
40   Student                          active    Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15
50   Reception                        active    Fa0/16, Fa0/17
```

Рисунок 3.21 – Перевірка VLAN на комутаторі

Перевірка IP-адрес на субінтерфейсах маршрутизатора здійснюється командою show ip interface brief. Вивід цієї команди дозволяє впевнитися, що кожен субінтерфейс має відповідну IP-адресу та перебуває в активному стані (рис. 3.22).

```
R1_doday#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        unassigned      YES NVRAM  up                    up
FastEthernet0/0.10     192.168.10.1    YES manual up                    up
FastEthernet0/0.20     192.168.20.1    YES manual up                    up
FastEthernet0/0.30     192.168.30.1    YES manual up                    up
FastEthernet0/0.40     192.168.40.1    YES manual up                    up
FastEthernet0/0.50     192.168.50.1    YES manual up                    up
FastEthernet0/1        unassigned      YES NVRAM  up                    up
FastEthernet0/1.60     192.168.60.1    YES manual up                    up
Ethernet0/0/0          192.168.0.1     YES manual up                    up
Ethernet0/1/0          192.168.1.1     YES manual up                    up
```

Рисунок 3.22 – IP-адреси субінтерфейсів на маршрутизаторі

Аналіз таблиці маршрутизації маршрутизатора за допомогою команди show ip route демонструє, які маршрути доступні для передачі даних між VLAN, а також до віддалених офісів (рис. 3.23).

```
10.0.0.0/30 is subnetted, 1 subnets
   10.255.255.0 [110/1010] via 192.168.1.2, 00:07:22, Ethernet0/1/0
192.168.0.0/30 is subnetted, 1 subnets
   192.168.0.0 is directly connected, Ethernet0/0/0
192.168.1.0/30 is subnetted, 1 subnets
   192.168.1.0 is directly connected, Ethernet0/1/0
192.168.3.0/30 is subnetted, 1 subnets
   192.168.3.0 [110/20] via 192.168.0.2, 00:07:22, Ethernet0/0/0
192.168.10.0/24 is directly connected, FastEthernet0/0.10
192.168.20.0/24 is directly connected, FastEthernet0/0.20
192.168.30.0/24 is directly connected, FastEthernet0/0.30
192.168.40.0/24 is directly connected, FastEthernet0/0.40
192.168.50.0/24 is directly connected, FastEthernet0/0.50
192.168.60.0/24 is directly connected, FastEthernet0/1.60
192.168.70.0/24 [110/11] via 192.168.0.2, 00:07:22, Ethernet0/0/0
192.168.80.0/24 [110/11] via 192.168.0.2, 00:07:22, Ethernet0/0/0
192.168.90.0/24 [110/11] via 192.168.0.2, 00:07:22, Ethernet0/0/0
192.168.110.0/24 [110/11] via 192.168.0.2, 00:07:22, Ethernet0/0/0
192.168.120.0/24 [110/11] via 192.168.0.2, 00:07:22, Ethernet0/0/0
```

Рисунок 3.23 – OSPF-маршрути в таблиці маршрутизатора

Перевірка доступності пристроїв у VLAN виконується за допомогою команди ping з одного комп’ютера до іншого в межах VLAN або між VLAN. Це підтверджує, що міжмережеве маршрутизування працює належним чином (рис. 3.24). Ping здійснено з VLAN50 в VLAN10.

```
C:\>ping 192.168.10.1

Pinging 192.168.10.1 with 32 bytes of data:

Reply from 192.168.10.1: bytes=32 time<1ms TTL=255
Reply from 192.168.10.1: bytes=32 time<1ms TTL=255
Reply from 192.168.10.1: bytes=32 time=1ms TTL=255
Reply from 192.168.10.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Рисунок 3.24 – Перевірка доступності ПК з VLAN 10

Для забезпечення передачі трафіку кількох VLAN між комутаторами або між комутатором і маршрутизатором налаштовуємо транк-порт. Транк дозволяє передавати кадри відразу з кількох VLAN по одному фізичному інтерфейсу, що зручно для масштабування мережі. Налаштування транк-порту на комутаторі виконується командою, зображеною на рисунку 3.25.

```
SW2_User(config-if)#switchport mode trunk

SW2_User(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1

SW2_User(config-if)#switchport trunk allowed vlan 70,80,90,110
SW2_User(config-if)#description Trunk to Router
```

Рисунок 3.25 – Налаштування транк-порту

Для перевірки стану транк-порту використовуємо команду show interfaces trunk (рис. 3.26).

```
Switch1#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/24      on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/24      10,20,30,40,50

Port        Vlans allowed and active in management domain
Fa0/24      10,20,30,40,50

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/24      10,20,30,40,50
```

Рисунок 3.26 – Перевірка стану транк-порту

3.4 Налаштування бездротового доступу

Налаштовуємо бездротову мережу для зони конференц-залу, де встановлено точку доступу з підтримкою Wi-Fi. Вона підключена до комутатора на другому поверсі в порт, який належить до VLAN 110 (Conference). SSID бездротової мережі – DoDay_WIFI, тип шифрування – WPA2-PSK, пароль – dodaydoday

Для маршрутизації трафіку цієї VLAN було створено підінтерфейс на Router2 – GigabitEthernet 0/0.110, якому призначено IP-адресу 192.168.110.1/24. Також на цьому ж маршрутизаторі налаштовано DHCP-сервер для автоматичної видачі IP-адрес клієнтам Wi-Fi (рис. 3.27).

```
R2_doday#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2_doday(config)#interface fastEthernet 0/0.110
R2_doday(config-subif)#encapsulation dot1Q 110
R2_doday(config-subif)#ip address 192.168.110.1 255.255.255.0
R2_doday(config-subif)#no shutdown
R2_doday(config-subif)#ex
R2_doday(config)#ip dhcp pool Conference
R2_doday(dhcp-config)#network 192.168.110.0 255.255.255.0
R2_doday(dhcp-config)#default-router 192.168.110.1
R2_doday(dhcp-config)#dns-server 8.8.8.8
R2_doday(dhcp-config)#exit
R2_doday(config)#
```

Рисунок 3.27 – Створення підінтерфейсу та налаштування DHCP

Після завершення налаштування точки доступу до безпровідної мережі додаємо один ноутбук та один смартфон (рис. 3.28). Ці пристрої під’єднуються до мережі Wi-Fi з ідентифікатором SSID DoDay_WIFI та паролем dodaydoday (рис. 3.29).

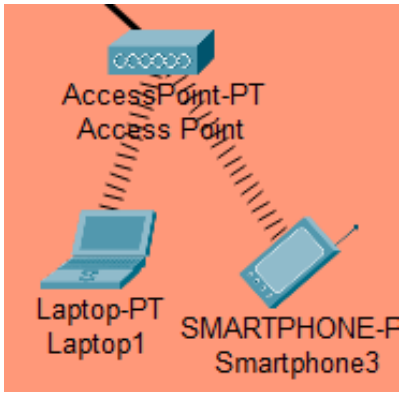

Рисунок 3.28 – Підключення ноутбука та смартфона до Wi-Fi

Приєднання здійснюється шляхом вибору відповідного бездротового інтерфейсу на пристрої, введення SSID, вибору методу аутентифікації (WPA2-PSK) та введення правильного ключа доступу. Після цього пристрої автоматично отримують IP-адреси від налаштованого DHCP-сервера, що підтверджує успішне підключення до мережі.

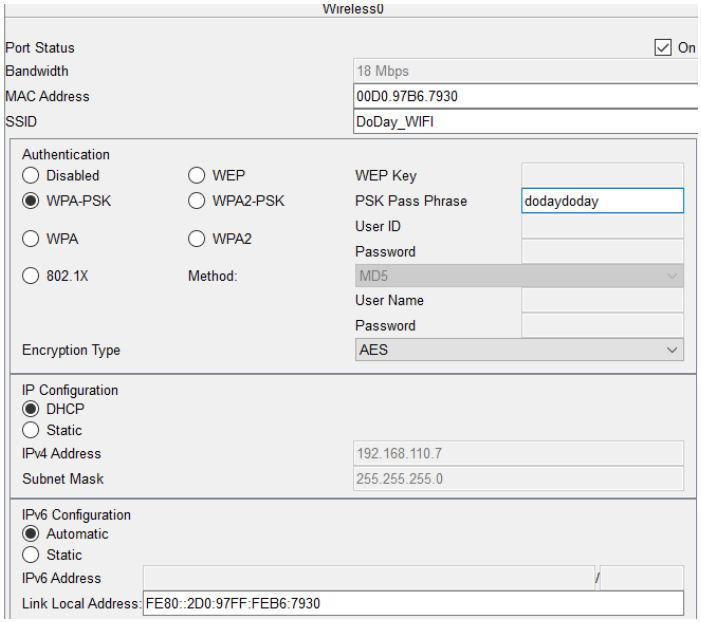

Рисунок 3.29 – Введення данних для підключення до Wi-Fi

Аналогічні налаштування виконано для бездротової точки доступу, встановленої на рецепції.

3.5 Організація доступу до віддалених офісів

Для організації зв’язку між центральним офісом і віддаленими офісами використовується GRE-тунель – віртуальний канал, який інкапсулює трафік і забезпечує його передачу через публічний Інтернет. Це дає змогу безпечно і стабільно об’єднати різні мережі в єдину корпоративну інфраструктуру.

Спершу призначаємо IP-адреси інтерфейсам WAN та LAN на маршрутизаторах. Наприклад, для Router_Lviv (рис. 3.30).

```
Router_Lviv(config)#interface FastEthernet0/0
Router_Lviv(config-if)# ip address 198.51.100.2 255.255.255.0
Router_Lviv(config-if)# no shutdown
Router_Lviv(config-if)#interface FastEthernet0/1
Router_Lviv(config-if)# ip address 192.168.102.1 255.255.255.0
Router_Lviv(config-if)# no shutdown
```

Рисунок 3.30 – Призначення IP-адреси інтерфейсам

Створюємо інтерфейс Tunnel, який буде логічним тунелем між офісами. На кожному маршрутизаторі задаємо IP-адресу тунелю, а також вказуємо локальний (джерело) і віддалений (призначення) IP для тунелю – це IP-адреси WAN -інтерфейсів. Приклад для маршрутизатора у Львові зображено на рисунку 3.31.

```
Router_Lviv(config)#interface Tunnel0
Router_Lviv(config-if)# ip address 172.16.0.6 255.255.255.252
Router_Lviv(config-if)# tunnel source FastEthernet0/0
Router_Lviv(config-if)# tunnel destination 203.0.113.1
Router Lviv(config-if)# no shutdown
```

Рисунок 3.31 – Створення інтерфейсу Tunnel

Наступним кроком налаштовуємо Tunnel на центральному маршрутизаторі.

Після конфігурації необхідно активувати інтерфейси та перевірити їхній стан. Команда show ip interface brief допоможе переконатися, що тунельний інтерфейс up і має правильну IP-адресу (рис. 3.32).

```
R3_doday#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        192.168.3.2     YES NVRAM  up                    up
FastEthernet0/1        192.168.1.2     YES NVRAM  up                    up
Ethernet0/0/0          unassigned      YES NVRAM  up                    up
Ethernet0/1/0          203.0.113.1     YES NVRAM  up                    up
Tunnel0                10.255.255.1    YES manual up                    up
Tunnel1                172.16.0.5      YES manual up                    up
```

Рисунок 3.32 – Перевірка статусу тунелю

Щоб маршрутизатори могли направляти трафік через тунель, IP-адреси тунелю додаються в маршрутизаторний протокол (у нашому випадку OSPF). Це дозволяє динамічно оновлювати маршрути і підтримувати актуальність інформації про доступні мережі. Приклад додавання тунельної мережі в OSPF зображено на рисунку 3.33.

```
Router_Lviv(config)#router ospf 1
Router_Lviv(config-router)# network 172.16.0.4 0.0.0.3 area 0
```

Рисунок 3.33 – Додавання тунельної мережі в OSPF

Переконуємось у працездатності тунелю, виконуючи команду пінгу на IP-адресу тунельного інтерфейсу віддаленого маршрутизатора (рис. 3.34).

```
Router_Lviv#ping 172.16.0.5

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/3/7 ms
```

Рисунок 3.34 – Тестування зв’язку

Для того, щоб пристрої з віддалених офісів мали доступ до зовнішніх ресурсів (наприклад, до Інтернету), необхідно на центральному маршрутизаторі налаштувати NAT Це дозволяє транслювати приватні IP-адреси віддалених офісів у публічну IP-адресу інтерфейсу WAN центрального офісу.

Приклад конфігурації NAT на центральному маршрутизаторі зображено на рисунку 3.35.

```
! Визначаємо інтерфейси
interface Ethernet0/1/0
 description WAN interface to Internet
 ip address 203.0.113.1 255.255.255.252
 ip nat outside

interface FastEthernet0/1
 description LAN interface (до основної мережі)
 ip address 192.168.1.2 255.255.255.0
 ip nat inside

interface Tunnel0
 description Tunnel до Харкова
 ip address 10.255.255.1 255.255.255.252
 ip nat inside

interface Tunnel1
 description Tunnel до Львова
 ip address 172.16.0.5 255.255.255.252
 ip nat inside

! Дозволяємо NAT для всіх підмереж (наприклад, 192.168.0.0/16)
access-list 1 permit 192.168.0.0 0.0.255.255

! Налаштовуємо NAT
ip nat inside source list 1 interface Ethernet0/1/0 overload
```

Рисунок 3.35 – Налаштування NAT на центральному маршутизаторі

3.6 Забезпечення безпеки корпоративної мережі

Для ефективного захисту корпоративної мережі компанії DoDay реалізовано базові механізми безпеки, що поєднують сегментацію, контроль доступу та моніторинг. Всі користувачі поділені на окремі VLAN, що зменшує ризик несанкціонованого доступу між відділами.

Додатково застосовано списки контролю доступу (ACL), які обмежують доступ до серверів та між VLAN, дозволяючи лише необхідний трафік. Для захищеного обміну даними з філіями використано VPN-тунелі GRE, налаштовані на рівні маршрутизаторів (розділ 3.5).

Для моніторингу стану мережі впроваджено SNMP, що дозволяє адміністраторам своєчасно реагувати на потенційні збої та загрози. У наступних підрозділах подано налаштування ACL та SNMP.

3.6.1 Налаштування списків контролю доступу (ACL)

Для забезпечення базового рівня мережевої безпеки впроваджено ACL (Access Control Lists) на маршрутизаторах. Це дозволяє контролювати, який трафік дозволений або заборонений між VLAN, а також до ключових ресурсів, зокрема до сервера зберігання відео з камер спостереження.

У мережі реалізовано такі правила:

– дозволено лише пристроям з VLAN IoT надсилати відео на FTP/HTTP-сервер;

– заборонено доступ до VLAN IoT з усіх інших сегментів мережі.

– дозволено керівництву, IT-відділу доступ до сервера;

– обмежено доступ до інтерфейсів маршрутизаторів лише з IT-відділу.

Приклад конфігурації ACL на маршрутизаторі зображено на рисунку 3.36.

```
R2_doday(config)#access-list 100 permit ip 192.168.60.0 0.0.0.255 host 192.168.70.10
R2_doday(config)#access-list 100 permit ip 192.168.30.0 0.0.0.255 host 192.168.70.10
R2_doday(config)#access-list 100 deny ip any 192.168.60.0 0.0.0.255
R2_doday(config)#access-list 100 permit ip any any
R2_doday(config)#interface FastEthernet0/1
R2_doday(config-if)# ip access-group 100 in
```

Рисунок 3.36 – Налаштування ACL на маршрутизаторі

Ці правила обмежують доступ до серверу (наприклад, 192.168.70.10), дозволяючи лише IoT та IT-відділу. Усі інші спроби доступу до підмережі IoT блокуються.

3.6.2 Механізми шифрування та VPN

З метою захисту передавання даних між головним офісом та віддаленими філіями було використано GRE-тунелі, налаштовано у розділі 3.4. Ці тунелі дозволяють інкапсулювати внутрішній трафік у зовнішні IP-пакети, що забезпечує логічне об’єднання віддалених мереж в одну приватну інфраструктуру.

Хоча GRE не забезпечує шифрування самостійно, у реальних мережах його часто поєднують з IPSec для забезпечення конфіденційності та цілісності трафіку. У рамках моделювання в Cisco Packet Tracer реалізовано тільки інкапсуляцію GRE для демонстрації структури захищеного тунельного з'єднання.

VPN-технології в цій мережі дозволяють безпечно з'єднувати віддалені офіси з головним, забезпечуючи надійний доступ до серверів, зокрема для зберігання відео з камер спостереження та обміну файлами.

3.6.3 Моніторинг мережі за допомогою SNMP

Для забезпечення контролю та моніторингу стану мережевої інфраструктури в мережі компанії впроваджено протокол SNMP (Simple Network Management Protocol). Цей протокол дозволяє централізовано збирати інформацію про стан обладнання, інтерфейсів, навантаження та виявляти потенційні збої.

У Cisco Packet Tracer налаштування SNMP здійснюється на маршрутизаторах і комутаторах за допомогою простого конфігураційного набору команд. Наприклад, на центральному маршрутизаторі було виконано наступні налаштування, що зображені на рисунку 3.37.

```
R3_doday#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3_doday(config)#snmp-server community public RO
%SNMP-5-WARMSTART: SNMP agent on host R3_doday is undergoing a warm start
R3_doday(config)#snmp-server community private RW
R3_doday(config)#exit
R3_doday#
```

Рисунок 3.37 – Налаштування SNMP

Команда snmp-server community public RO створює спільноту з правами лише для читання (read-only), що дозволяє системам моніторингу безпечно опитувати пристрої. Спільнота private з правами запису (read-write) використовується для адміністративного керування, хоча її використання має бути обмежене з міркувань безпеки.

Після налаштування SNMP-агенти на пристроях готові відповідати на запити від SNMP-менеджера, який може бути розгорнутий на окремому сервері або комп’ютері. Це дозволяє адміністратору відслідковувати стан портів, завантаження каналів та інші критично важливі параметри мережі в реальному часі.

Таким чином, SNMP відіграє ключову роль у забезпеченні стабільної роботи корпоративної мережі, дозволяючи вчасно реагувати на неполадки й оптимізувати функціонування інфраструктури.

3.7 Підключення камер спостереження

У попередніх розділах було налаштовано окремі VLAN для IoT-пристроїв (камер спостереження) на кожному поверсі, а також здійснено базову конфігурацію IP-камер. Також раніше створено та налаштовано FTP-сервер, який використовується як централізоване сховище для збереження відеозаписів із камер.

На цьому етапі зосередимось на покроковому підключенні камер до FTP-серверу, організації збереження даних та перевірці зв’язку.

Кожна камера отримала IP-адресу у межах VLAN 60 (IoT) згідно з DHCP або була налаштована статично. Перевірити доступність можна командою на сервері або з будь-якого іншого пристрою в тій же VLAN (рис. 3.38).

```
C:\>ping 192.168.60.1

Pinging 192.168.60.1 with 32 bytes of data:

Reply from 192.168.60.1: bytes=32 time<1ms TTL=255
Reply from 192.168.60.1: bytes=32 time<1ms TTL=255
Reply from 192.168.60.1: bytes=32 time<1ms TTL=255
Reply from 192.168.60.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.60.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Рисунок 3.38 – Перевірка доступності за допомогою команди ping

Для конфігурації FTP-параметрів на IP-камерах у веб-інтерфейсі або CLI IP-камери необхідно вказати налаштування, зображені на рисунку 3.39.

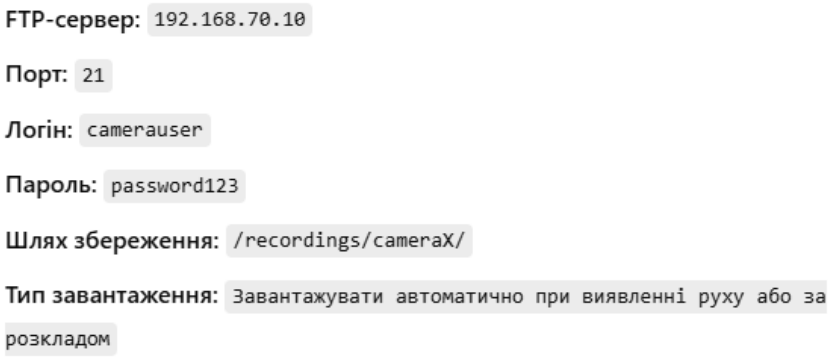

Рисунок 3.39 – Конфігурація FTP-параметрів

Після збереження параметрів на камері, зазвичай є кнопка «Test FTP», яка дозволяє пересвідчитися в коректності підключення. Також можна на сервері перевірити, чи з’являються тестові файли у вказаному каталозі.

Отже, відеозаписи з камер передаються по окремій мережі, а сервер приймає і зберігає їх у спеціальних папках на жорсткому диску. Зазвичай ці папки створюються у директорії FTP-сервера, наприклад, у теці типу /ftp/videos або /home/ftp/videos, де адміністратор може налаштувати доступ. Саме в цих папках зберігаються всі записи, і звідти їх можна переглядати, копіювати або робити резервні копії за потребою.

ВИСНОВКИ

В кваліфікаційній роботі здійснено детальний аналіз організаційної структури компанії DoDay, що дало змогу виявити потребу у впровадженні розгалуженої корпоративної мережі з підтримкою IoT, централізованим керуванням та захищеним з’єднанням між офісами в різних містах. Це стало основою для формування технічних вимог до мережевої інфраструктури.

Виконано вибір логічної топології мережі, що ґрунтується на ієрархічному підході з поділом на рівні доступу, розподілу й ядра. Обрана модель дозволяє забезпечити гнучкість і масштабованість, а також спрощує адміністрування і підтримку мережі.

Спроєктовано та реалізовано систему IP-адресації, що охоплює всі сегменти мережі, включаючи головний офіс та віддалені філії, створено окремі підмережі для кожного VLAN, що забезпечує логічну ізоляцію і дозволяє зручно керувати доступом до ресурсів.

Розроблено та впорядковано структуру віртуальних локальних мереж (VLAN), які відповідають функціональним відділам компанії: керівництво, бухгалтерія, відділ кадрів, юридичний відділ, технічний персонал тощо. Це дозволило організувати контроль доступу до інформації та зменшити обсяг широкомовного трафіку.

Налаштовано динамічну маршрутизацію між VLAN за допомогою протоколу OSPF та реалізовано концепцію підінтерфейсної маршрутизації (router-on-a-stick), завдяки цьому забезпечено стійкий зв’язок між усіма підмережами та автоматичне оновлення маршрутів.

Візуалізовано логічну та фізичну топологію корпоративної мережі за допомогою інструментів середовища Cisco Packet Tracer. Модель мережі відображає всі основні компоненти – маршрутизатори, комутатори, точки доступу, сервери, ПК, периферію та віддалені вузли, що дозволило ефективно протестувати її роботу ще до фізичної реалізації.

Спроєктовано та обґрунтовано вибір мережевого обладнання, обране рішення забезпечує баланс між вартістю, продуктивністю і масштабованістю.

Реалізовано повноцінну мережеву інфраструктуру в середовищі Cisco Packet Tracer, змодельовано маршрутизацію, роботу DHCP, VLAN, VPN, NAT, міжмережевих списків контролю доступу (ACL), а також перевірено коректну взаємодію між усіма сегментами мережі.

Налаштовано DHCP-сервер для автоматичної видачі IP-адрес, реалізовано VPN-з’єднання між офісами компанії (м. Львів, м. Харків та м. Київ). Застосовано GRE-тунелі, механізми IPsec, засоби авторизації та фільтрації трафіку, що забезпечує захищений обмін даними в межах мережі.

Розроблено комплекс заходів безпеки, зокрема фільтрацію на рівні маршрутизатора за допомогою ACL, сегментацію трафіку, реалізацію VLAN, шифрування та ізоляцію критичних вузлів. Мережева архітектура відповідає принципам безпеки «secure-by-design».

Отримано підтвердження працездатності побудованої моделі шляхом симуляції реального навантаження на мережу. Проведено тестування взаємодії між сегментами, перевірено стійкість VPN-з’єднань, доступність мережевих служб, стабільність передачі даних і масштабованість структури.

Як бачимо з отриманих результатів, розроблена корпоративна мережа є гнучкою, безпечною, стабільною та відповідає усім поставленим вимогам. Її можна впровадити у реальне корпоративне середовище компанії DoDay для підвищення ефективності взаємодії між її підрозділами.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Багнюк Н., Чичелюк О. Корпоративна мережа компанії DoDay. Програмне та апаратне забезпечення в інформаційних технологіях : зб. тез доп. міжнар. наук-практ. конф. Молодих науковців та студентів, м. Луцьк. 6 травня, 2025. С.17-19.

2. Захарова О. В. Основи інформаційно-аналітичної діяльності. Суми: СумДУ, 2024. 15 с. (дата звернення: 25.02.2025)

3. What Is Network Design?. *Cisco*. URL: https://surl.lu/zqpqbu (дата звернення: 10.02.2025).

4. How to Design a Network: 6 Best Practices for Success| NinjaOne. *NinjaOne*.URL: https://www.ninjaone.com/blog/how-to-design-a-network-best-practices/ (дата звернення: 28.02.2025).

5. An Introductory Guide to Enterprise Network Design|NetBox Labs. *NetBox Labs | The world's platform for network and infrastructure management*.URL: https://netboxlabs.com/blog/enterprise-network-design-guide/ (дата звернення: 05.03.2025).

6. Network Design and Best Practices. *Auvik*. URL: https://surl.li/yttikx (дата звернення: 11.03.2025).

7. Середовище обміну даними. Канали зв'язку. *Освітній проект «На Урок» для вчителів*. URL: https://naurok.com.ua/seredovische-obminu-danimi-kanali-zv-yazku-421899.html (дата звернення: 18.03.2025).

8. База даних для IoT: особливості роботи та оптимізація | Wezom. *IT-компанія повного циклу розробки програмних продуктів WEZOM* – Київ, Україна.URL: https://surl.li/hnlveb (дата звернення: 25.03.2025).

9. An Introductory Guide to Enterprise Network Design | NetBox Labs. *NetBox Labs | The world's platform for network and infrastructure management*. URL: https://surl.li/fosevp (дата звернення: 01.04.2025).

10. Що таке VLAN і як вона допомагає організувати мережу в бізнесі. *Макснет – Гігабітний інтернет-провайдер та оператор зв'язку для дому та бізнесу*. URLhttps://surl.li/bjsrmt (дата звернення: 08.04.2025).

11. IBM. What is Network Security? | IBM. *IBM - United States*. URL: https://www.ibm.com/think/topics/network-security (дата звернення: 13.04.2025).

12. Маршрутизатор Cisco ISR4331 (ISR4331/K9*). stack-systems.com.ua - Мережеве обладнання*. URL: https://surl.li/hihjis (дата звернення: 16.04.2025).

13. ТехноТрейд. Інтернет-магазин Wi-Fi обладнання ТехноТрейд. Мережеве Wi-Fi обладнання для інтернета. Інтернет-магазин по продажу обладнання для локальної мережі. Купити WiFi обладнання для бездротової мережі. URL: https://www.technotrade.com.ua/Products/MikroTik-CCR1009-7G-1C-1Splus.php (дата звернення: 18.04.2025).

14. EdgeRouter 4 (ER-4) Ubiquiti Networks купити в Україні – ціни, характеристики | Lanmarket.ua. *Магазин мережевого обладнання Lanmarket*. URL: https://lanmarket.ua/ua/ubiquiti/edgerouter-4-er-4/ (дата звернення: 22.04.2025).

15. Комутатори Cisco Catalyst 2960-X серії (Cisco 2960-X) | *Stack Systems UA*. stack-systems.com.URL: https://surl.li/wapiwe (дата звернення: 25.04.2025).

16. 28-портовий гігабітний розумний комутатор Omada з 24-портовим підтримкою PoE+. Omada. *Networks Empower Business* | TP-Link. URL: https://www.omadanetworks.com/uk-ua/business-networking/omada-switch-smart/sg2428p/ (дата звернення: 28.04.2025).

17. Точка доступа Cisco AIR 1832I (AIR-AP1832I-E-K9). stack-systems.com.ua. *Мережеве обладнання.* URL: https://surl.li/uaunts (дата звернення: 30.04.2025).

18. ТехноТрейд. Інтернет-магазин Wi-Fi обладнання ТехноТрейд. Мережеве Wi-Fi обладнання для інтернета. *Інтернет-магазин по продажу обладнання для локальної мережі*. Купити WiFi обладнання для бездротової

мережі. URL: https://www.technotrade.com.ua/Products/Ubiquiti-UniFi-Video-Camera-G3.php (дата звернення: 05.05.2025).

19. Сервер HP ProLiant ML350 Gen10 (8 SFF) . SERVAK. URLhttps://surl.li/dupzjf (дата звернення: 07.05.2025).

20. EdgeRouter X (ER-X) Ubiquiti Networks купити в Україні. *Магазин мережевого обладнання Lanmarket*. URL: https://lanmarket.ua/ubiquiti/ubiquiti-networks-edgerouter-x-er-x-2980/ (дата звернення: 10.05.2025).

21. TL-SG2210P Гігабітний керований 8-портовий PoE комутатор з двома комбінованими слотами SFP TP-Link Україна. TP-Link Deutschland Netzwerklösungen für Privat und Businessanwender. URL: https://www.tp-link.com/uk-ua/service-provider/smart-switch/tl-sg2210p/ (дата звернення: 12.05.2025).