

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 охоронних систем

(повне найменування кафедри)

КВАЛІФІКАЦІЙНА РОБОТА
ЗА СТУПЕНЕМ ВИЩОЇ ОСВІТИ «БАКАЛАВР»

КОРПОРАТИВНА МЕРЕЖА ІТ-КОМПАНІЇ «DIGITAL SOLUTIONS»

CORPORATE NETWORK OF THE IT-COMPANY «DIGITAL SOLUTIONS»

спеціальність 123 Комп'ютерна інженерія

(шифр і назва спеціальності)

освітня програма Комп'ютерна інженерія

(назва освітньої програми)

Виконав: здобувач вищої освіти
групи КІ-41
Мельничук Марія Олександрівна

(підпис)

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

(підпис)

Кваліфікаційну роботу
допущено до захисту
«_____» _____ 2026 р.
Гарант освітньої програми:
к.т.н., доцент
Лавренчук Світлана Василівна

(підпис)

Луцьк – 2026 року

ЛУЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Факультет комп'ютерних та інформаційних технологій

Кафедра комп'ютерної інженерії та охоронних систем

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

« 06 » 05 2026 р.

ЗАВДАННЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ ЗДОБУВАЧУ ВИЩОЇ ОСВІТИ

Мельничук Марія Олександрівна

(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи Корпоративна мережа IT-компанії «Digital Solutions»

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

затверджені наказом закладу вищої освіти від «06» травня 2026 року № 242/01-02

2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 28.05.2026 р.

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, різні інтернет-ресурси технічного спрямування

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

Вступ

Теоретичні основи побудови корпоративних комп'ютерних мереж

Аналіз та опис іт-компанії «Digital Solutions»

Проектування корпоративної мережі в Cisco Packet Tracer

Висновки

5. Перелік графічного (ілюстративного) матеріалу:

Теоретичні основи побудови корпоративних комп'ютерних мереж

Аналіз діяльності та мережевої інфраструктури компанії «Digital Solutions»

Проектування корпоративної мережі в Cisco Packet Tracer

Тестування мережі та результати реалізації проекту

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис	
		завдання видав	завдання прийняв
<i>Теоретичні основи побудови корпоративних комп'ютерних мереж</i>	<i>Багнюк Н. В., доцент</i>		
<i>Аналіз та опис іт-компанії «Digital Solutions»</i>	<i>Багнюк Н. В., доцент</i>		
<i>Проектування корпоративної мережі в Cisco Packet Tracer</i>	<i>Багнюк Н. В., доцент</i>		
<i>Нормоконтроль</i>	<i>Багнюк Н. В., доцент</i>		
<i>Гарант ОП</i>	<i>Лавренчук С. В., доцент</i>		
<i>Показник запозичень тексту</i>		%	
<i>Академічна доброчесність</i>	<i>Міскевич О. І., ст. викладач</i>		

7. Дата видачі завдання

06.05.2026 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	<i>Огляд літератури із досліджуваної проблеми, аналіз предметної області та наявних рішень</i>	до 10.05.2026 р.	
2.	<i>Теоретичні основи побудови корпоративних комп'ютерних мереж</i>	до 11.05.2026 р.	
3.	<i>Аналіз та опис іт-компанії «Digital Solutions»</i>	до 12.05.2026 р.	
4.	<i>Проектування корпоративної мережі в Cisco Packet Tracer</i>	до 15.05.2026 р.	
5.	<i>Представлення остаточного варіанту кваліфікаційної роботи керівникові</i>	до 20.05.2026 р.	
6.	<i>Нормоконтроль</i>	до 23.05.2026 р.	
7.	<i>Інструментальна перевірка на академічний плагіат</i>	до 27.05.2026 р.	
8.	<i>Здача кваліфікаційної роботи та всіх супровідних документів на кафедрі</i>	до 28.05.2026 р.	

Здобувач вищої освіти

(підпис)

Марія МЕЛЬНИЧУК

(прізвище, ініціали)

Керівник кваліфікаційної роботи

(підпис)

Наталія БАГНЮК

(прізвище, ініціали)

АНОТАЦІЯ

Мельничук М. О. Корпоративна мережа ІТ-компанії «Digital Solutions». Рукопис.

Кваліфікаційна робота бакалавра ОП «Комп'ютерна інженерія» спеціальності 123 Комп'ютерна інженерія. Луцький національний технічний університет. Луцьк, 2026.

У першому розділі досліджено теоретичні основи побудови корпоративних комп'ютерних мереж. Розглянуто поняття корпоративної мережі, її основні функції та призначення в сучасних організаціях. Проаналізовано базові архітектури комп'ютерних мереж, їх переваги та особливості використання в корпоративному середовищі. Особливу увагу приділено основним мережевим технологіям і протоколам, які застосовуються для забезпечення маршрутизації, передачі даних та організації мережесервісів. Також розглянуто принципи сегментації мережі та механізми забезпечення інформаційної безпеки, включаючи ізоляцію трафіку та контроль доступу.

У другому розділі наведено загальну характеристику компанії, основні напрями її діяльності та організаційну структуру. Детально розглянуто логічну структуру існуючої мережі компанії, визначено її основні компоненти та взаємозв'язки між підрозділами.

У третьому розділі виконано практичне проектування корпоративної мережі компанії. Реалізовано налаштування ключових мережесервісів, зокрема демілітаризованої зони (DMZ), DHCP, (ACL) для фільтрації та обмеження мережевого трафіку між сегментами. Додатково проведено тестування працездатності мережі, перевірено коректність маршрутизації, доступність сервісів і роботу політик безпеки.

Ключові слова: маршрутизація, VLAN, DHCP, DMZ, списки контролю доступу (ACL), контроль доступу, тестування мережі.

ANNOTATION

Melnychuk M. Corporate network of the IT company «Digital Solutions». Manuscript.

Qualifying work of a bachelor of EP «Computer Engineering» specialty 123 Computer Engineering. Lutsk National Technical University. Lutsk, 2026.

Qualification work consists of an introduction, three sections, conclusions, a references, and an appendix.

In the first chapter, the theoretical foundations of building corporate computer networks are investigated. The concept of a corporate network, its main functions, and its role in modern organizations are considered. Basic computer network architectures, their advantages, and features of their use in a corporate environment are analyzed. Particular attention is paid to the main networking technologies and protocols used to provide routing, data transmission, and network services. The principles of network segmentation and information security mechanisms, including traffic isolation and access control, are also examined.

In the second chapter, a general description of the enterprise, its main areas of activity, and organizational structure is presented. The logical structure of the existing company network is analyzed in detail, and its main components and interconnections between departments are identified.

In the third chapter, the practical design of the enterprise corporate network is carried out. The configuration of key network services is implemented, including a Demilitarized Zone (DMZ), DHCP, and Access Control Lists (ACLs) for filtering and restricting network traffic between segments. In addition, network functionality testing is performed to verify routing correctness, service availability, and the operation of security policies.

Keywords: routing, VLAN, DHCP, DMZ, Access Control Lists (ACLs), access control, network testing.

ЗМІСТ

ВСТУП.....	7
РОЗДІЛ 1 ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ КОРПОРАТИВНИХ КОМП'ЮТЕРНИХ МЕРЕЖ	9
1.1 Поняття та призначення корпоративних мереж	9
1.2 Архітектури комп'ютерних мереж.....	11
1.3 Основні мережеві технології та протоколи	12
1.4 Принципи сегментації та безпеки корпоративних мереж	16
1.5 Сучасні підходи до побудови мереж ІТ-компаній.....	17
РОЗДІЛ 2 АНАЛІЗ ТА ОПИС ІТ-КОМПАНІЇ «DIGITAL SOLUTIONS»	21
2.1 Загальна характеристика компанії та напрямки діяльності.....	21
2.2 Логічна структура мережі	25
2.3 Перспективи розширення мережі компанії.....	27
РОЗДІЛ 3 ПРОЄКТУВАННЯ КОРПОРАТИВНОЇ МЕРЕЖІ.....	29
3.1 Налаштування DMZ.....	29
3.2 Налаштування DHCP	39
3.3 Налаштування точок доступу	41
3.4 Налаштування списків контролю доступу	45
3.5 Тестування працездатності мережі та аналіз результатів.....	46
ВИСНОВКИ.....	48
ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	49

ВСТУП

Розвиток інформаційних технологій зумовлює зростання вимог до корпоративних комп'ютерних мереж, які є основою функціонування будь-якої ІТ-компанії. Ефективно спроектована мережна інфраструктура забезпечує надійну передачу даних, високу продуктивність роботи користувачів, безперервність бізнес-процесів та захищеність корпоративної інформації від зовнішніх і внутрішніх загроз.

Актуальність теми зумовлена необхідністю створення масштабованих, відмовостійких та безпечних мережеских рішень для ІТ-компаній, які працюють з великими обсягами даних та розподіленою структурою підрозділів. У таких умовах особливого значення набуває правильний вибір мережескої архітектури, протоколів маршрутизації, засобів сегментації трафіку та механізмів інформаційної безпеки.

Метою кваліфікаційної роботи є проектування корпоративної мережі ІТ-компанії, яка забезпечує ефективну взаємодію між підрозділами, безпечний доступ до внутрішніх ресурсів та можливість подальшого масштабування інфраструктури.

Для досягнення поставленої мети визначені такі завдання:

- дослідити теоретичні основи побудови корпоративних комп'ютерних мереж;
- проаналізувати сучасні мережескі архітектури та протоколи;
- розглянути принципи сегментації та забезпечення мережескої безпеки;
- здійснити аналіз діяльності та існуючої структури ІТ-компанії;
- розробити логічну структуру корпоративної мережі;
- виконати проектування основних мережеских сервісів (DMZ, DHCP, Wi-Fi, ACL);
- провести тестування працездатності запропонованого рішення.

Об'єктом дослідження є процес функціонування корпоративних комп'ютерних мереж ІТ-компаній.

Предметом дослідження є методи та засоби проектування, налаштування та захисту корпоративної мережі компанії «Digital Solutions».

Практичне значення роботи полягає у розробці моделі корпоративної мережі, яка може бути використана для впровадження в реальних умовах діяльності ІТ-компанії та забезпечує баланс між продуктивністю, масштабованістю та безпекою.

РОЗДІЛ 1

ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ КОРПОРАТИВНИХ КОМП'ЮТЕРНИХ МЕРЕЖ

1.1 Поняття та призначення корпоративних мереж

Корпоративна мережа є фундаментальною інфраструктурою будь-якої організації, що прагне до ефективного управління інформаційними ресурсами та комунікаційними потоками. Під корпоративною мережею розуміють сукупність апаратних засобів, програмного забезпечення та комунікаційних каналів, які об'єднують робочі станції, сервери, периферійне обладнання та інші мережеві пристрої в єдину інформаційну систему підприємства [1-2].

Корпоративна мережа виконує низку критично важливих функцій: забезпечення спільного доступу до файлів і ресурсів, організацію централізованого зберігання даних, підтримку корпоративних застосунків (ERP, CRM, системи документообігу), надання захищеного доступу до мережі Інтернет, а також забезпечення внутрішніх комунікацій через IP-телефонію та корпоративну електронну пошту [1-2].

Для IT-компаній, зокрема для «Digital Solutions», корпоративна мережа набуває особливого стратегічного значення, адже вона є середовищем, у якому безпосередньо здійснюється основна виробнича діяльність: розробка програмного забезпечення, тестування, деплоймент додатків, управління проєктами та взаємодія з клієнтами. Вимоги до надійності, пропускну здатності та безпеки таких мереж є значно вищими, ніж у підприємств інших галузей.

Мережі класифікують за географічним охопленням на [3-4]:

- локальні мережі (LAN – Local Area Network), що покривають одну будівлю або офіс;
- мережі міського масштабу (MAN – Metropolitan Area Network), які об'єднують кілька будівель у межах міста;
- глобальні мережі (WAN – Wide Area Network), що з'єднують географічно розподілені підрозділи організації через публічну або приватну інфраструктуру.

Крім того, активно використовуються програмно-визначені глобальні мережі (SD-WAN), що дозволяють централізовано управляти розподіленою інфраструктурою [5].

На рисунку 1.1 показано типову ієрархічну топологію корпоративної мережі, що включає три рівні: ядро, розподільний рівень та рівень доступу. Така архітектура забезпечує масштабованість та відмовостійкість мережевої інфраструктури.

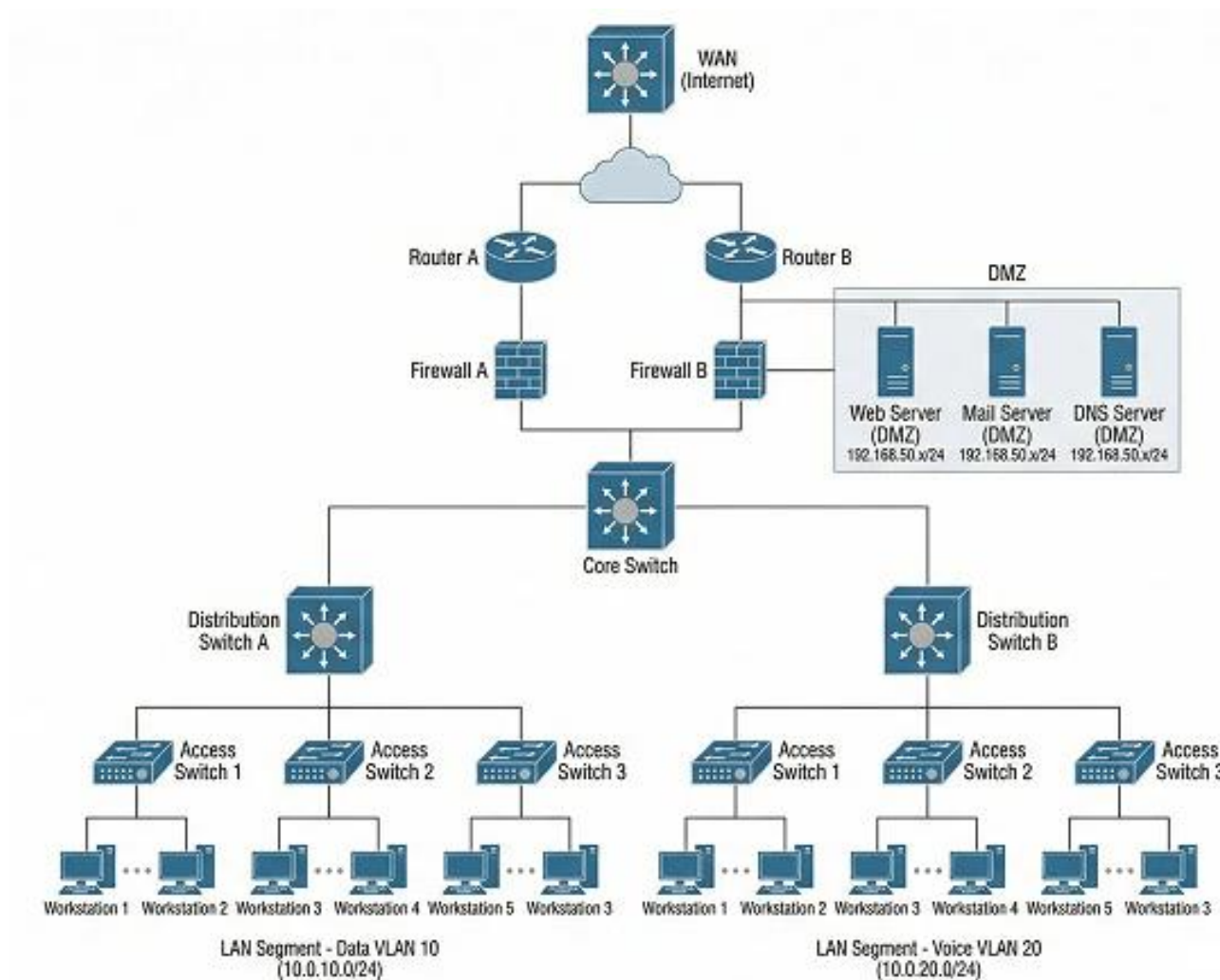


Рисунок 1.1 – Типова ієрархічна топологія корпоративної мережі

Важливою характеристикою корпоративної мережі є рівень її надійності. Для ІТ-компаній стандартом вважається досягнення показника доступності не менше 99,9 %, що допускає не більше 8,76 годин простою на рік. Для критичних систем цей показник підвищується до 99,99 % і вище.

1.2 Архітектури комп'ютерних мереж

Архітектура комп'ютерної мережі визначає логічну організацію взаємодії між її компонентами (рис. 1.2). В корпоративному середовищі домінують дві основні парадигми: клієнт-серверна архітектура та розподілена архітектура [6].

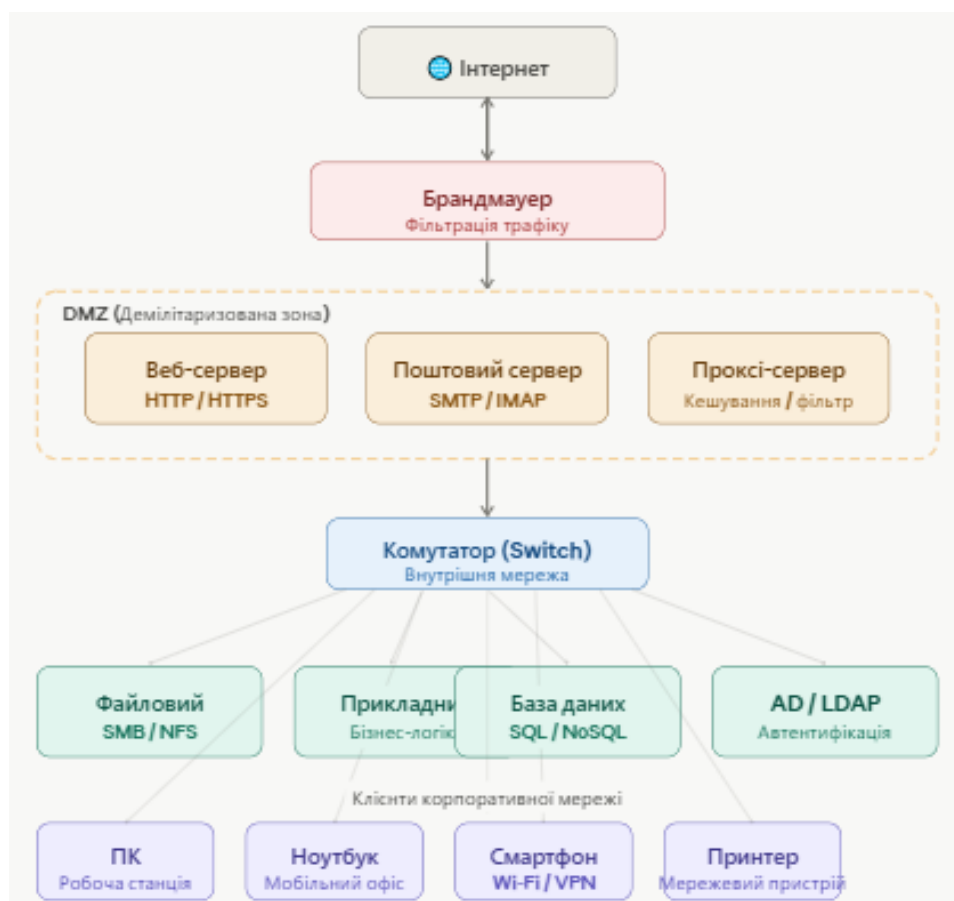


Рисунок 1.2 – Клієнт-серверна архітектура корпоративної мережі

Клієнт-серверна архітектура базується на чіткому розмежуванні ролей: сервери надають ресурси та сервіси, а клієнти їх споживають. Сервер є централізованим вузлом, що обробляє запити від множини клієнтів, забезпечуючи контрольований доступ до даних, бізнес-логіки та периферійних пристроїв. Перевагами такого підходу є централізоване адміністрування, висока безпека, зручність резервного копіювання та аудиту. Водночас сервер є єдиною точкою відмови, що вимагає реалізації відмовостійких кластерних рішень [6].

Існує кілька варіантів клієнт-серверної архітектури: дворівнева (клієнт безпосередньо взаємодіє з сервером бази даних), трирівнева (між клієнтом і СУБД існує рівень бізнес-логіки – сервер застосунків) та N-рівнева, що характерна для сучасних хмарних і мікросервісних систем. У мережевій інфраструктурі ІТ-компанії «Digital Solutions» доцільно застосовувати трирівневу модель для виробничих систем [6].

Розподілена архітектура передбачає рівноправну взаємодію вузлів, кожен з яких може одночасно виступати як клієнтом, так і сервером. У сучасній інтерпретації розподілена архітектура охоплює мікросервісний підхід, де застосунок декомпонується на незалежні, слабко зв'язані сервіси, що взаємодіють через API (здебільшого REST або gRPC). Перевагами розподіленої архітектури є горизонтальна масштабованість, відсутність єдиної точки відмови та незалежне розгортання окремих компонентів.

Для сучасних ІТ-компаній характерне використання гібридної архітектури: клієнт-серверної для корпоративних систем управління та мікросервісної або розподіленої для розробки власних продуктів. Контейнеризація (Docker) та оркестрація (Kubernetes) стали стандартними інструментами реалізації розподіленої архітектури у мережевому середовищі ІТ-компаній [4].

Окремою архітектурною концепцією є програмно-визначені мережі (Software-Defined Networking – SDN), що розділяють площину управління та площину даних. SDN дозволяє централізовано програмувати мережеву поведінку через контролери (наприклад, OpenDaylight, Cisco ACI), забезпечуючи динамічну адаптацію мережі до потреб застосунків [4].

1.3 Основні мережеві технології та протоколи

Стек протоколів TCP/IP (Transmission Control Protocol / Internet Protocol) є де-факто стандартом побудови сучасних корпоративних мереж (рис. 1.3). Він складається з чотирьох рівнів: канального, мережевого, транспортного та прикладного, кожен з яких виконує специфічні функції з передачі даних [7].



Рисунок 1.3 – Модель TCP/IP та відповідні протоколи кожного рівня [7]

На мережевому рівні ключовим є протокол IP, наявний у двох версіях. IPv4 оперує 32-бітними адресами (наприклад, 192.168.1.0/24), що теоретично дає 4,3 млрд. унікальних адрес. Через вичерпання адресного простору IPv4 впроваджується протокол IPv6 із 128-бітними адресами. IPv6 також пропонує вбудовану автоконфігурацію (SLAAC), покращену безпеку через обов'язкову підтримку IPsec та ефективнішу маршрутизацію завдяки спрощеному заголовку пакету [8-10].

На транспортному рівні протокол TCP (Transmission Control Protocol) забезпечує надійну доставку даних з підтвердженням отримання, керуванням потоком та контролем перевантажень. UDP (User Datagram Protocol) є альтернативою для застосунків, де пріоритетом є швидкість, а не надійність (DNS-запити, VoIP, потокове відео) – новий протокол транспортного рівня від Google, що поєднує переваги TCP і UDP та використовується у HTTP/3 [8-10].

Технологія VLAN (Virtual Local Area Network) дозволяє логічно сегментувати фізичну мережу на кілька ізольованих широкомовних доменів. Відповідно до стандарту IEEE 802.1Q, кожен кадр Ethernet може містити

12-бітний ідентифікатор QUIC VLAN (VLAN ID), що дозволяє створити до 4094 логічних мереж на спільній фізичній інфраструктурі. У корпоративних мережах VLAN використовуються для розмежування трафіку різних підрозділів, серверного сегменту, гостьового Wi-Fi та управлінського трафіку (рис. 1.4-1.6).

Які бувають типи VLAN [11]:

- «VLAN на основі портів або інтерфейсів;
- VLAN на основі MAC-адрес;
- VLAN на основі IP-мережі;
- VLAN на основі протоколу;
- VLAN комбінований».

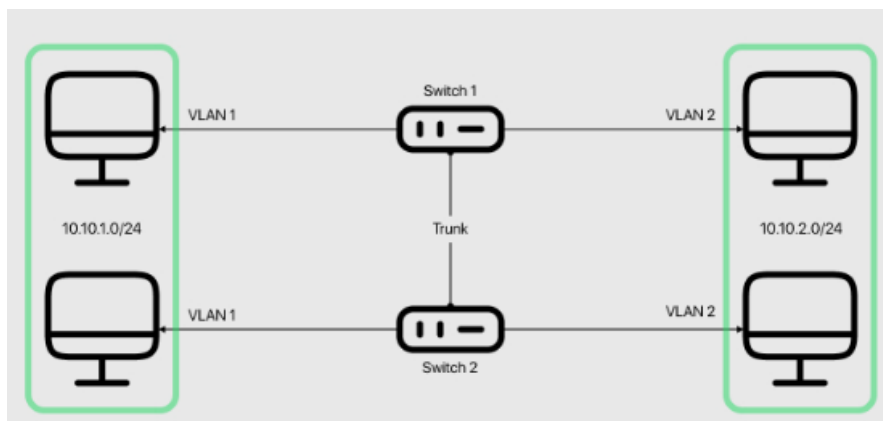


Рисунок 1.4 – Приклад сегментації мережі на основі технології VLAN: підключених до різних комутаторів [11]

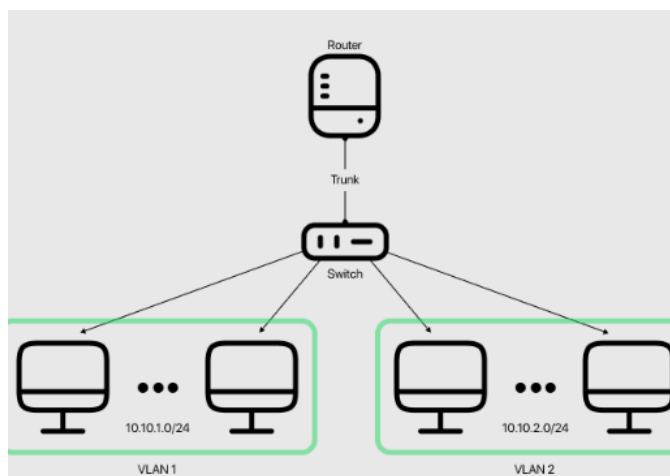


Рисунок 1.5 – Приклад сегментації мережі на основі технології VLAN: підключених до одного комутатору [11]

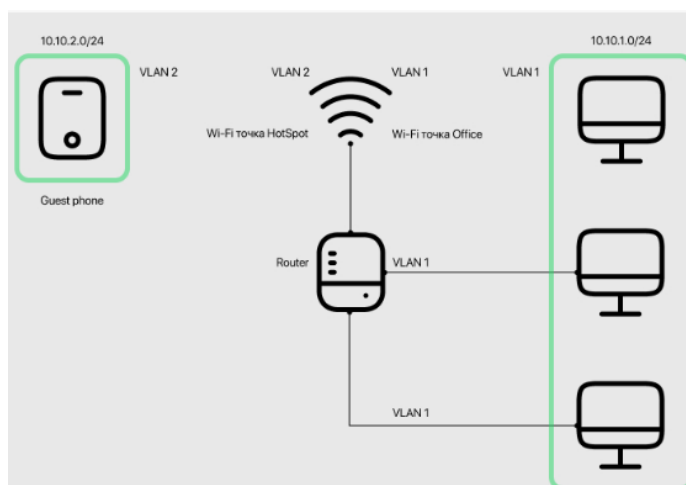


Рисунок 1.6 – Приклад сегментації мережі на основі технології VLAN: розділ гостьової Wi-Fi мережі та Wi-Fi мережі підприємства [11]

Протокол DHCP (Dynamic Host Configuration Protocol) автоматизує процес призначення мережевих параметрів (IP-адреса, маска підмережі, шлюз за замовчуванням, DNS-сервери) клієнтам мережі. DHCP-сервер може працювати у двох режимах: повністю динамічному (адреса видається з пулу на визначений термін – lease time) та зі статичним прив'язуванням (адреса призначається конкретному MAC-адресу пристрою). Для балансування навантаження і відмовостійкості в корпоративних мережах розгортають два DHCP-сервери з розподілом пулів адрес у співвідношенні 80/20 або використовують протокол DHCP Failover [12].

Система доменних імен DNS (Domain Name System) є розподіленою ієрархічною базою даних, що відповідає за трансляцію символічних доменних імен у мережеві адреси (прямий пошук) та навпаки (зворотний пошук). У корпоративному середовищі розгортається внутрішній DNS-сервер, який обслуговує внутрішній простір імен (наприклад, corp.digitalsolutions.ua) та виконує рекурсивні запити для зовнішніх доменів через DNS-форвардери. Протокол DNSSEC забезпечує криптографічний захист відповідей DNS від підміни (атаки типу DNS Spoofing) [13].

Серед інших важливих протоколів корпоративних мереж слід відзначити: OSPF і BGP (динамічна маршрутизація) [14], STP/RSTP (запобігання петлям у комотованих мережах) [15], NTP (синхронізація часу) [16], SNMP та NetFlow

(моніторинг мережевої інфраструктури) [17], а також протоколи захищеної передачі даних IPsec, TLS/SSL і SSH [18].

1.4 Принципи сегментації та безпеки корпоративних мереж

Безпека корпоративної мережі є комплексним поняттям, що охоплює технічні, організаційні та процедурні заходи захисту інформаційних ресурсів від несанкціонованого доступу, витоку, модифікації або знищення. В умовах зростаючого рівня кіберзагроз побудова захищеної мережевої інфраструктури є стратегічним пріоритетом для будь-якої ІТ-компанії.

Ключовим принципом безпеки є концепція ешелонованого захисту (Defense in Depth) [19], яка передбачає наявність кількох незалежних рубежів безпеки. Якщо зломисник долає один рубіж (наприклад, мережевий міжмережевий екран), він зіштовхується з наступним (системою виявлення вторгнень, контролем доступу на рівні застосунків тощо). Така багатошарова архітектура суттєво ускладнює реалізацію атак.

Мережева сегментація є фундаментальним механізмом обмеження радіуса ураження у разі компрометації одного сегменту. Практично вона реалізується через:

- фізичну сегментацію – розміщення обладнання різних підрозділів у різних фізичних мережах;
- логічну сегментацію на основі VLAN – найпоширеніший підхід у корпоративних мережах;
- демілітаризовану зону (DMZ) – ізольований сегмент для публічно доступних сервісів (веб-сервери, поштові шлюзи) [20];
- мікросегментацію – гранулярне розмежування трафіку між окремими робочими навантаженнями, що реалізується засобами SDN або хмарних платформ.

Архітектура нульової довіри (Zero Trust Architecture – ZTA) є сучасною парадигмою мережевої безпеки, що базується на принципі «не довіряй нікому, перевіряй усіх». На відміну від традиційного периметрального захисту, ZTA

передбачає, що загроза може виходити як зовні, так і зсередини мережі. Кожен запит до ресурсу проходить автентифікацію, авторизацію та шифрування незалежно від місцезнаходження ініціатора [21].

Міжмережевий екран нового покоління (Next-Generation Firewall – NGFW) є ключовим елементом мережевої безпеки. На відміну від традиційних міжмережевих екранів, NGFW здійснює глибоку інспекцію пакетів (Deep Packet Inspection – DPI), ідентифікацію застосунків (App-ID), контроль користувачів (User-ID), фільтрацію URL та інтегровану систему запобігання вторгненням (IPS). Провідними рішеннями на ринку є Palo Alto Networks, Cisco Firepower та Fortinet FortiGate [22].

Системи виявлення та запобігання вторгненням (IDS/IPS) аналізують мережевий трафік у режимі реального часу, зіставляючи його з базами сигнатур відомих атак та виявляючи аномалії поведінки. IPS діє у режимі inline і може автоматично блокувати підозрілий трафік, тоді як IDS лише фіксує події для подальшого аналізу [23].

Протокол IEEE 802.1X [24] забезпечує автентифікацію пристроїв і користувачів перед отриманням доступу до мережі. Разом із протоколом RADIUS (Remote Authentication Dial-In User Service) він формує систему контролю доступу до мережі (NAC – Network Access Control), що дозволяє розмежовувати права доступу залежно від ідентифікаційних даних, стану пристрою (відповідність вимогам безпеки – compliance) та інших атрибутів.

Важливим елементом захисту є шифрування мережевого трафіку. VPN (Virtual Private Network) на основі протоколів IPsec або SSL/TLS забезпечує захищений тунель для віддаленого доступу співробітників. Протокол TLS 1.3 є стандартом шифрування трафіку між клієнтами та сервісами. WPA3 використовується для захисту бездротових сегментів корпоративної мережі [25].

1.5 Сучасні підходи до побудови мереж ІТ-компаній

Мережева інфраструктура сучасних ІТ-компаній суттєво відрізняється від корпоративних мереж підприємств інших галузей. Специфіка полягає в

інтенсивному характері мережевого навантаження (розробка, тестування, CI/CD-конвеєри), необхідності підтримки гетерогенних середовищ (хмара, on-premises, гібрид), а також у вищих вимогах до доступності та гнучкості інфраструктури.

Концепція Intent-Based Networking (IBN) передбачає декларативне управління мережею: адміністратор задає бажаний стан (intent), а система самостійно визначає та застосовує необхідну конфігурацію. Платформи IBM, Cisco DNA Center та Juniper Apstra реалізують цей підхід, автоматизуючи рутинні операції та забезпечуючи безперервну перевірку відповідності стану мережі заявленому наміру [26].

Гіперконвергентна інфраструктура (HCI – Hyper-Converged Infrastructure) поєднує обчислювальні ресурси, зберігання даних та мережу в єдину програмно-керовану платформу. Рішення VMware vSAN, Nutanix та Microsoft Azure Stack HCI дозволяють значно спростити управління інфраструктурою та підвищити щільність розміщення навантажень. Для IT-компаній HCI є привабливим рішенням для розгортання середовищ розробки та тестування [27].

Хмарна та гібридна архітектура стали невід'ємною частиною мережевої стратегії IT-компаній. Підключення до хмарних провайдерів (AWS, Azure, Google Cloud) реалізується через виділені канали (AWS Direct Connect, Azure ExpressRoute) або захищені IPsec-тунелі. SD-WAN дозволяє оптимально розподіляти трафік між хмарними та локальними ресурсами, забезпечуючи якість обслуговування (QoS) для критичних застосунків.

Автоматизація мережевих операцій є ключовим трендом для IT-компаній. Підхід Infrastructure as code (IaC) передбачає опис мережевої конфігурації у вигляді коду (Ansible, Terraform, NAPALM), що забезпечує відтворюваність, версіонування та швидкість розгортання інфраструктури. Network DevOps (NetDevOps) інтегрує практики DevOps у процеси управління мережею, скорочуючи час від ідеї до реалізації мережевих змін.

Безпроводні технології нового покоління Wi-Fi 6 (802.11ax) та Wi-Fi 6E (з підтримкою діапазону 6 ГГц) забезпечують значно вищу пропускну здатність (до 9,6 Гбіт/с теоретично), меншу затримку та кращу роботу в умовах великої

щільності пристроїв. Ці характеристики є критично важливими для офісних середовищ ІТ-компаній із великою кількістю мобільних пристроїв та IoT-обладнання [5].

Для забезпечення безперервного моніторингу та видимості мережі (Network Visibility) застосовуються системи збору телеметрії: NetFlow/IPFIX для аналізу трафіку, платформи SIEM (Security Information and Event Management) для кореляції подій безпеки, а також рішення NPM (Network Performance Monitoring) на кшталт SolarWinds NPM, PRTG або Grafana із стеком Prometheus для збору метрик у реальному часі [6].

Таким чином, сучасна мережева інфраструктура ІТ-компанії являє собою складну багаторівневу екосистему, що поєднує класичні мережеві технології з програмно-визначеними рішеннями, хмарними сервісами та інтелектуальними засобами автоматизації й моніторингу. Проектування мережі для «Digital Solutions» має враховувати всі зазначені підходи з метою побудови масштабованої, захищеної та ефективної інфраструктури [3].

Висновки до розділу 1.

У першому розділі кваліфікаційної роботи проведено аналіз теоретичних основ побудови корпоративних комп'ютерних мереж. Встановлено, що корпоративна мережа є стратегічною інфраструктурою, яка визначає ефективність роботи організації. Розглянуто основні архітектурні підходи – клієнт-серверну та розподілену архітектуру – і визначено доцільність їх комбінованого застосування в ІТ-компанії.

Проаналізовано ключові мережеві технології та протоколи: TCP/IP як базовий стек, IPv4/IPv6 для адресації, VLAN для логічної сегментації, DHCP і DNS для підтримки мережевих сервісів. Досліджено принципи мережевої безпеки, зокрема ешелонований захист, архітектуру нульової довіри та механізми контролю доступу.

Виявлено сучасні тенденції розвитку мережевої інфраструктури ІТ-компаній: програмно-визначені мережі, автоматизація на основі IaC, гібридна хмарна архітектура та Wi-Fi 6/6E. Отримані теоретичні знання становлять

підґрунтя для проєктування корпоративної мережі ІТ-компанії «Digital Solutions» у наступних розділах роботи.

РОЗДІЛ 2

АНАЛІЗ ТА ОПИС IT-КОМПАНІЇ «DIGITAL SOLUTIONS»

2.1 Загальна характеристика компанії та напрямки діяльності

Digital Solutions – це компанія, яка пропонує IT-рішення та послуги клієнтам. Компанія складається з відділу кадрів та фінансового відділу, відділ бренду та маркетингу, адміністративного відділу, відділу IT-підтримки, відділу розробки програмного забезпечення та групи управління хмарними платформами (рис. 2.1).



Рисунок 2.1 – Структура компанії

З огляду на вимоги безпеки, відділи розташовані в окремі vlan, відповідно користувачі розміщені в окремих сегментах мережі в межах однієї локальної мережі. Відповідно розробка та впровадження захищеної, надійної, масштабованої та стійкої мережевої системи є ключовим чинником у гарантуванні конфіденційності, цілісності та доступності даних і комунікацій.

Для побудови корпоративної мережі компанії застосовано ієрархічну багаторівневу архітектуру, яка забезпечує високу продуктивність, масштабованість та надійність функціонування мережевої інфраструктури. Такий підхід передбачає розподіл мережі на окремі логічні рівні, кожен з яких виконує власні функції та взаємодіє з іншими рівнями через стандартизовані механізми маршрутизації та комутації.

Ієрархічна структура [28] дозволяє спростити адміністрування мережі, підвищити ефективність управління трафіком та забезпечити можливість подальшого розширення інфраструктури без суттєвих змін у вже реалізованій архітектурі. Завдяки розподілу функцій між рівнями зменшується навантаження на окремі мережеві пристрої та підвищується загальна стабільність роботи корпоративних сервісів.

Особлива увага приділяється забезпеченню відмовостійкості мережі. Для цього передбачається резервування критично важливих каналів зв'язку та мережевого обладнання, використання альтернативних маршрутів передачі даних, а також впровадження механізмів автоматичного перемикання у разі виникнення аварійних ситуацій. Такий підхід мінімізує ризик простою інформаційних систем та забезпечує безперервний доступ користувачів до корпоративних ресурсів і сервісів.

Застосування багаторівневої моделі разом із засобами резервування створює надійну основу для функціонування сучасної корпоративної мережі, здатної підтримувати зростання компанії, інтеграцію нових сервісів та ефективно виконання бізнес-процесів.

Для забезпечення доступу до зовнішніх ресурсів та корпоративних сервісів мережа компанії підключена до провайдера для забезпечення виходу до мережі Інтернет, доступ до хмарних сервісів та можливості організації захищених каналів зв'язку з віддаленими філіями та користувачами.

Бездротовий доступ у мережі реалізовується за допомогою точок доступу (WAP), встановлених у кожному відділі компанії. Централізоване керування бездротовою інфраструктурою здійснюється контролером WLC, що спрощує адміністрування мережі, забезпечує єдину політику безпеки та дозволяє розмежувати доступ для працівників і гостей.

Для підвищення пропускної здатності та надійності мережевої інфраструктури між ключовими мережевими пристроями доцільно застосувати технологію EtherChannel [29]. Вона дозволяє об'єднати декілька фізичних каналів зв'язку в один логічний інтерфейс, що забезпечує ефективніше використання доступної пропускної здатності та балансування мережевого навантаження.

Застосування EtherChannel підвищує відмовостійкість мережі. У разі виходу з ладу одного з фізичних каналів передача даних автоматично продовжується через інші активні з'єднання без переривання роботи користувачів і мережевих сервісів. Це забезпечує стабільність функціонування корпоративної мережі та безперервність бізнес-процесів.

Створення підмереж передбачає розподіл IP-адрес відповідно до визначених діапазонів для кожного відділу компанії, що забезпечує коректне функціонування мережі та уникнення конфліктів адрес. Для цього розраховується маска підмережі, яка дозволяє створити необхідну кількість сегментів, кожен із власним шлюзом і діапазоном адрес. Базові налаштування пристроїв включають призначення імен хостів, встановлення паролів для доступу через консоль і привілейований режим, додавання банера з попередженням про авторизований доступ, шифрування паролів та вимкнення функції IP domain lookup, щоб запобігти затримкам при помилковому введенні команд. Маршрутизація між VLAN забезпечує взаємодію між усіма відділами через багаторівневий комутатор, на якому створюються SVI-інтерфейси для кожного VLAN із відповідними IP-адресами та активується функція маршрутизації. Це дозволяє пристроям різних сегментів обмінюватися даними, підтримуючи логічну ізоляцію мережі та ефективну комунікацію між усіма підрозділами Digital Solutions.

DHCP-сервер у корпоративній мережі Digital Solutions налаштований таким чином, щоб усі пристрої отримують свої адреси динамічно від серверів, розташованих у серверному сегменті. Це означає, що саме сервери виконують роль DHCP-служби, формуючи пул адрес для кожного VLAN і забезпечуючи автоматичний розподіл конфігураційних параметрів – IP-адреси, маски, шлюзи та DNS. Такий підхід централізує управління адресацією, спрощує адміністрування та гарантує узгодженість усіх налаштувань у межах корпоративної інфраструктури.

У серверному сегменті всі пристрої отримують IP-адреси статично, тобто адміністратор призначає кожному серверу унікальну адресу вручну. Такий підхід забезпечує стабільність роботи критично важливих сервісів, зокрема Active Directory, DNS, DHCP та файлових серверів, оскільки їхні IP-адреси залишаються незмінними й можуть бути використані як постійні точки доступу для клієнтів та

інших мережевих пристроїв. Статична адресація у серверній кімнаті також спрощує адміністрування, дозволяє уникнути конфліктів при динамічному розподілі адрес і гарантує безперервність роботи корпоративної інфраструктури Digital Solutions.

У корпоративній мережі Digital Solutions основним протоколом маршрутизації є OSPF, який використовується як на маршрутизаторах, так і на багаторівневих комутаторах для розповсюдження маршрутів між усіма сегментами мережі. Це забезпечує динамічне оновлення таблиць маршрутизації, швидку конвергенцію та масштабованість у випадку розширення інфраструктури. Для кожного VLAN створюються відповідні оголошення мереж, що дозволяє пристроям у різних підмережах взаємодіяти без необхідності ручного додавання статичних маршрутів.

Додатково для захисту віддаленого адміністрування через SSH налаштовується стандартний ACL на лінії VTY. Таким чином, доступ до пристроїв через SSH буде суворо регламентований, що мінімізує ризики несанкціонованого втручання та відповідає вимогам корпоративної політики безпеки.

Для корпоративної мережі Digital Solutions міжмережевий екран Cisco ASA виконує роль центрального елемента безпеки, який контролює доступ до ресурсів у різних сегментах. Налаштування передбачає визначення зон безпеки – наприклад, inside для внутрішньої мережі, outside для зовнішнього доступу та DMZ для серверів, що мають бути доступними з Інтернету. Кожній зоні призначається рівень довіри: внутрішня мережа отримує найвищий рівень, зовнішня – найнижчий, а DMZ займає проміжне положення.

Далі формуються політики доступу у вигляді списків контролю доступу (ACL), які визначають, який трафік дозволено чи заборонено між зонами. Наприклад, внутрішнім користувачам дозволяється вихід у зовнішню мережу через NAT, тоді як вхідні з'єднання з Інтернету обмежуються лише до певних сервісів у DMZ (наприклад, веб-серверів). Для управління використовується SSH або ASDM, доступ до яких також регламентується правилами безпеки.

Таким чином, Cisco ASA забезпечує сегментацію мережі, контроль трафіку та централізоване впровадження політик безпеки, що гарантує захист

корпоративних ресурсів Digital Solutions від несанкціонованого доступу та зовнішніх загроз.

2.2 Логічна структура мережі

Логічна структура мережі являє собою модель організації взаємозв'язків між вузлами та сегментами, яка визначає принципи маршрутизації, адресації та взаємодії протоколів незалежно від фізичного розташування кабелів чи обладнання. Вона описує, як дані рухаються всередині системи, які правила їхнього обміну застосовуються та яким чином забезпечується доступ до ресурсів. Основними складовими такої структури є вузли у вигляді комп'ютерів, серверів, маршрутизаторів і комутаторів, сегменти у вигляді VLAN чи підмереж, логічні канали передачі даних, протоколи TCP/IP, OSPF або RIP, а також система адресації, що включає IP-адреси, маски підмереж та ідентифікатори VLAN.

У практиці застосовуються різні логічні топології, серед яких шина, де всі вузли підключені до одного каналу, зірка з центральним вузлом, кільце з циркуляцією даних по колу, повнозв'язна структура з прямими зв'язками між усіма вузлами та ієрархічна модель, що поєднує риси зірки та шини. У корпоративних мережах логічна структура зазвичай включає центральний маршрутизатор, який об'єднує кілька VLAN для різних відділів, використання OSPF для маршрутизації між сегментами, DHCP-сервер для автоматичного призначення IP-адрес та DNS-сервер для іменування ресурсів. Таким чином, логічна структура демонструє організацію руху даних між відділами та серверами, тоді як фізична структура відображає реальне прокладання кабелів і розташування обладнання.

Текст до таблиці з адресацією мережі по відділах зазвичай пояснює принципи розподілу IP-адрес та логіку їхнього призначення. У корпоративній мережі кожен відділ отримує власну підмережу, що забезпечує ізоляцію трафіку, спрощує адміністрування та підвищує рівень безпеки. Адресація виконується відповідно до обраної схеми підмережування, де для кожного сегмента визначається діапазон IP-адрес, маска та шлюз за замовчуванням. Це дозволяє чітко розмежувати ресурси бухгалтерії, адміністративного відділу, відділу розробки чи гостьової Wi-Fi мережі.

У таблиці 2.1 відображаються назви відділів, їхні VLAN або підмережі, діапазони IP-адрес та відповідні шлюзи. Такий підхід дає змогу швидко ідентифікувати, які адреси належать конкретному сегменту, а також забезпечує правильну маршрутизацію між ними. Важливо, що адресація узгоджується з DHCP-серверами, які автоматично призначають адреси клієнтам, і з DNS-серверами, що відповідають за іменування ресурсів. Таким чином, таблиця адресації є ключовим елементом логічної структури мережі, оскільки вона демонструє організацію доступу до ресурсів та взаємодію між відділами.

Таблиця 2.1 – Діапазони адрес сегментів

Назва сегменту	Адреса мережі	Маска мережі	Шлюз за замовчуванням
DMZ	172.20.1.0	/28 255.255.255.240	172.20.1.1
vlan 2	172.16.1.0	/24 255.255.255.0	172.16.1.1
vlan 3	172.16.2.0	/24 255.255.255.0	172.16.2.1
vlan 4	172.16.3.0	/24 255.255.255.0	172.16.3.1

Опишемо мережеву архітектуру взаємодії та розташування ключових пристроїв (табл. 2.2): брандмауера (захист і контроль доступу), маршрутизатора (маршрутизація трафіку) та Layer-3 комутатора (комутатор із функціями маршрутизації).

Таблиця 2.2 – Мережева архітектура взаємодії та розташування ключових пристроїв

Назва обладнання	Номер порту	IP-адреса, маска
Бранмауер BRAND_MELNYCHUK6	G1/1	172.20.1.1/30
	G1/2	12.7.4.1/30
	G1/3	172.21.1.1/30
Маршрутизатор провайдера ISP_MELNYCHUK2	G 0/0	11.5.3.2/30
	G0/1	12.7.4.2/30

Продовження таблиці 2.2

Назва обладнання	Номер порту	IP-адреса, маска
Маршрутизатор CLOUD	G 0/0	9.12.2.2/30
	G 0/1	11.5.3.1/30
Маршрутизатор AZURE	G 0/0	35.27.1.1/8
	G 0/1	9.12.2.1/30
Хмарне сховище – сервер	Fa0/5	35.27.1.2/8

2.3 Перспективи розширення мережі компанії

Перспективи розширення мережі компанії можна розглядати у кількох взаємопов'язаних площинах. Передусім йдеться про технологічний розвиток, який включає перехід на сучасні протоколи, наприклад IPv6, впровадження програмно-визначених мереж (SDN) та розширення системи кіберзахисту. Це дозволяє забезпечити масштабованість та підвищити рівень безпеки даних. Важливим напрямом є організаційне розширення, що передбачає створення нових сегментів мережі для окремих відділів, інтеграцію віддалених філій та оптимізацію управління ресурсами через централізовані служби.

З економічної точки зору перспективи полягають у залученні інвестицій для модернізації інфраструктури, впровадженні хмарних сервісів та розширенні клієнтської бази. Розвиток мережі також може бути спрямований на інтеграцію розгортання бездротових технологій нового покоління та створення резервованих каналів зв'язку для забезпечення безперервності бізнес-процесів. У стратегічному вимірі розширення мережі компанії означає не лише збільшення кількості користувачів чи вузлів, а й формування гнучкої, масштабованої та захищеної інфраструктури, здатної підтримувати зростання компанії та її вихід на нові ринки.

Наявність сформованої логічної структури з чіткою адресацією по відділах, використання сучасних протоколів і централізованих служб, що забезпечує масштабованість та гнучке адміністрування є надзвичайно важливим елементом для успішної роботи компанії. Сегментація у вигляді VLAN підвищує рівень безпеки та дозволяє ізолювати трафік між відділами. Слабкі сторони полягають у

можливих обмеженнях пропускної здатності та резервування каналів, а також у використанні застарілого обладнання, що ускладнює інтеграцію нових технологій. Відсутність повної автоматизації управління мережею може призводити до додаткових витрат часу та ресурсів.

Можливості розширення полягають у переході на IPv6, що відкриває перспективи масштабування адресного простору та інтеграції нових сервісів. Використання хмарних технологій і програмно-визначених мереж дозволяє централізовано керувати інфраструктурою та швидко адаптувати її до потреб бізнесу. Розгортання VoIP, Wi-Fi нового покоління та резервованих каналів забезпечить безперервність бізнес-процесів і розширить спектр послуг для клієнтів. Загрози пов'язані зі зростанням кіберризиків і складністю захисту розширеної інфраструктури, високою вартістю модернізації обладнання та ліцензійного програмного забезпечення, а також ризиком несумісності нових технологій із наявними системами, що потребує додаткових інвестицій у інтеграцію та навчання персоналу.

РОЗДІЛ 3

ПРОЄКТУВАННЯ КОРПОРАТИВНОЇ МЕРЕЖІ

3.1 Налаштування DMZ

В даному проєкті використовується демілітаризована зона для серверів (рекламний сервер, ERP-сервер, поштовий сервер, файловий сервер). «DMZ (Demilitarized Zone, демілітаризована зона) – як технічний ресепшн для мережі. Окрема підмережа між інтернетом і внутрішньою локальною мережею (LAN). Там є публічні сервіси: веб, пошта, DNS, VPN, проксі та інші служби, до яких звертаються ззовні. Їх ізолюють від LAN, щоб зменшити ризики при зламі» [30].

Так як більшість користувачів мають ноутбуки, тому ноутбук має мати карту, яка призначена для бездротового зв'язку WPC 300 (рис. 3.1).

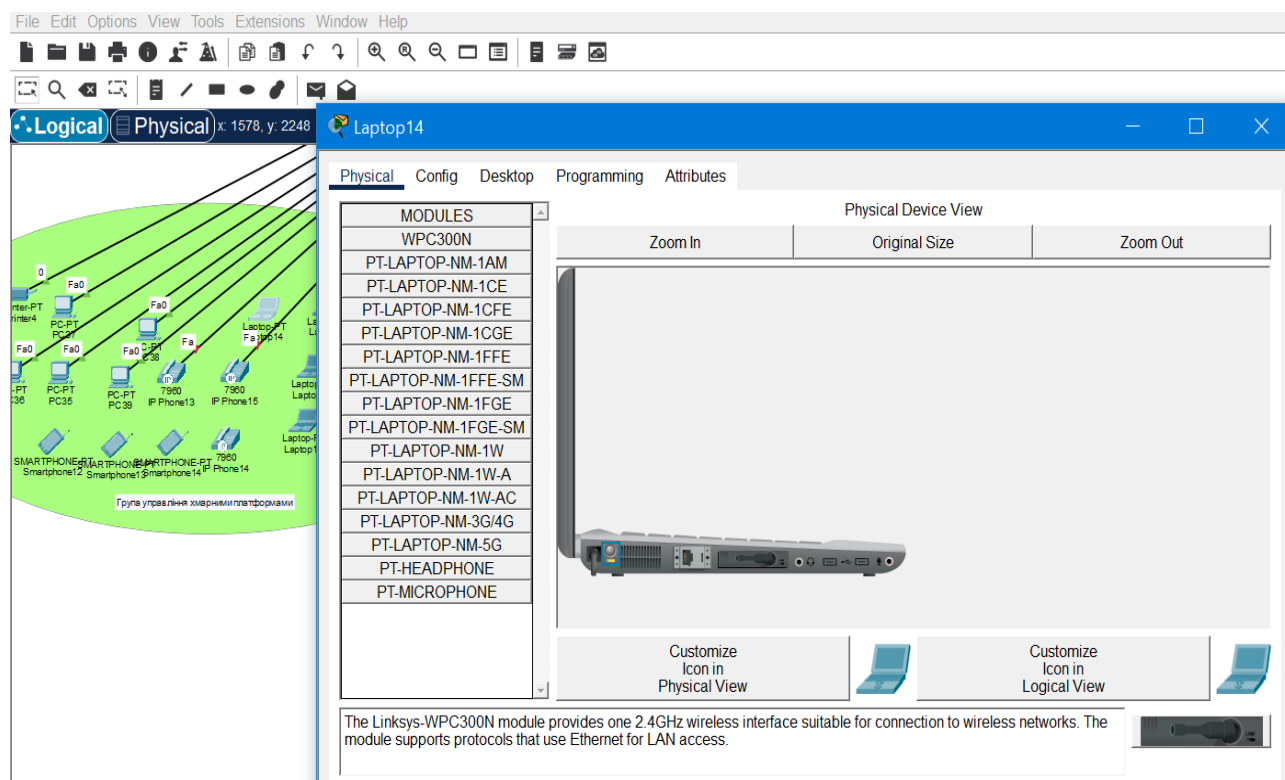


Рисунок 3.1 – Ноутбук з картою для бездротового зв'язку WPC 300

Так як в даній мережі є голосовий шлюз, то налаштуємо IP-телефон, вибравши відповідний модуль (рис. 3.2).

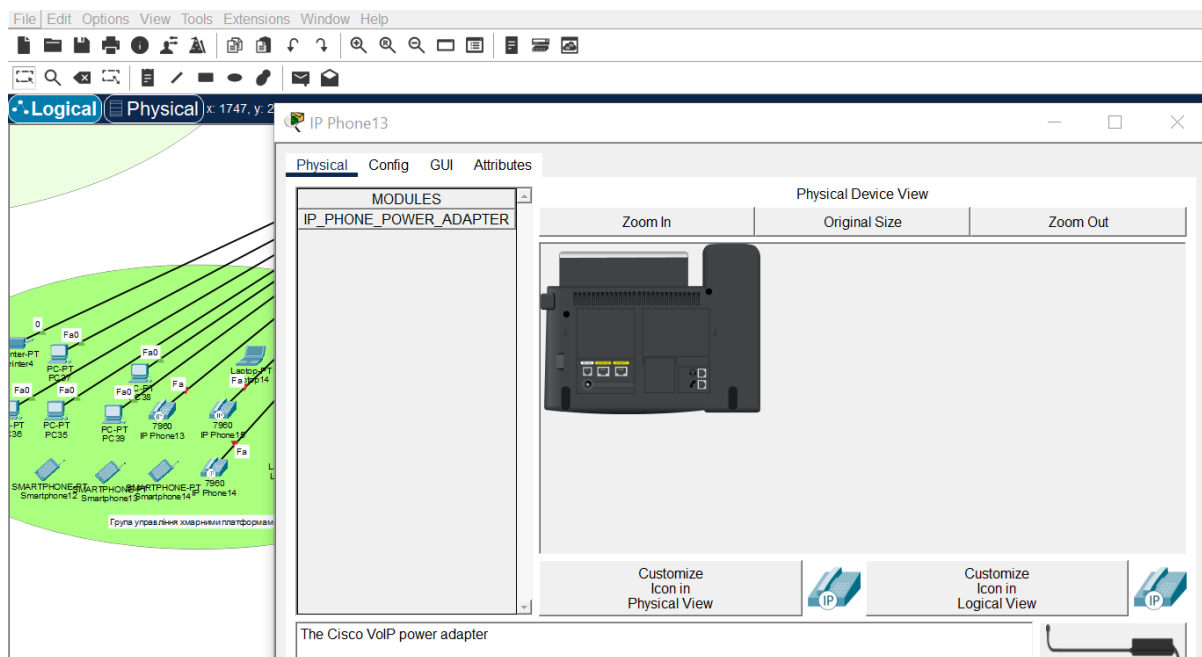


Рисунок 3.2 – Налаштування телефону

Виконаємо базові налаштування мережевого екрана. Мережевий екран має бути захищений паролем та створимо користувача (рис. 3.3). Пароль використаємо mariia.

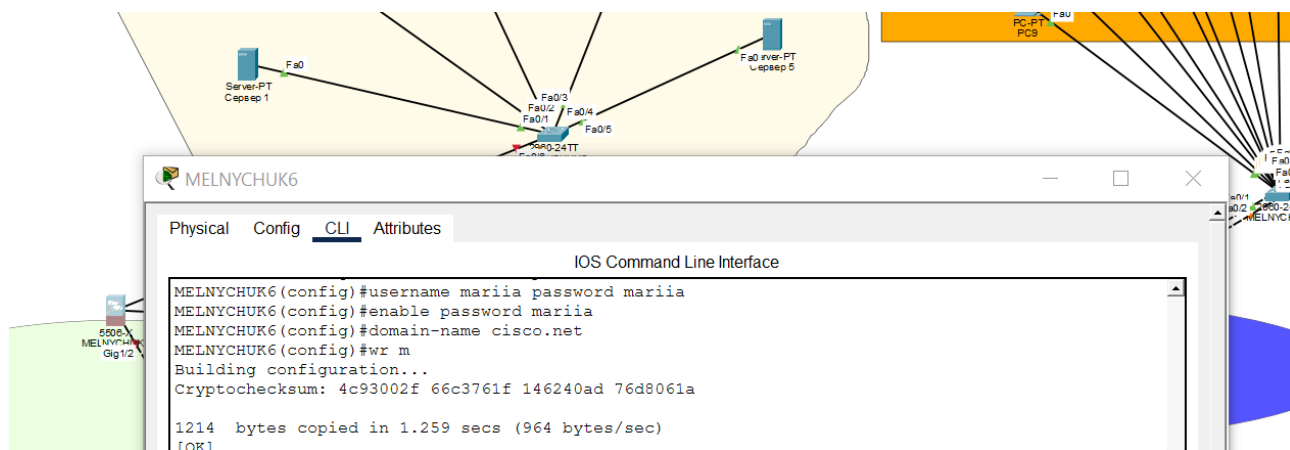


Рисунок 3.3 – Базові налаштування мережевого екрана

Налаштування проміжного мережевого обладнання (маршрутизаторів, комутаторів) в операційній системі Cisco IOS дуже схоже.

Проведемо налаштування обладнання (налаштуємо ім'я, пароль (mariia) та його шифрування, банерне повідомлення та вимкнення пошуку IP-домену) в демілітаризованій зоні, зокрема на комутаторі 2960 (рис. 3.4).

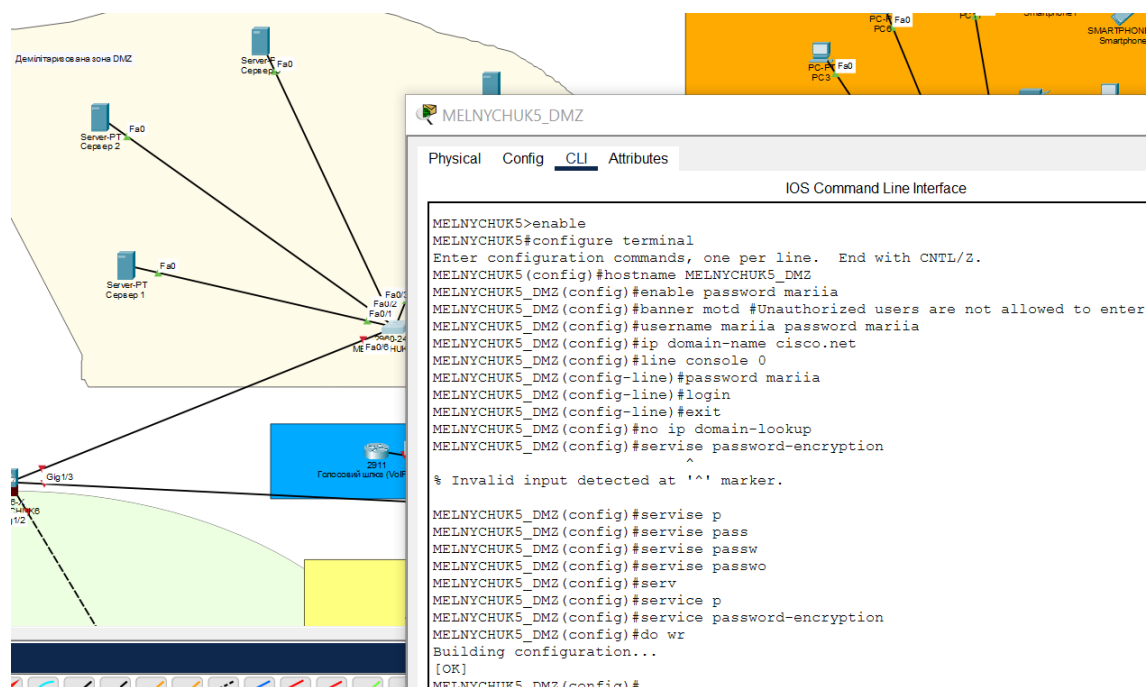


Рисунок 3.4 – Налаштування імені та паролю

В даному випадку налаштовуємо обладнання, що належить компанії. Компанія не контролює маршрутизатори інтернет-провайдера (рис. 3.5), тобто, в даному випадку не контролює хмарні платформи.

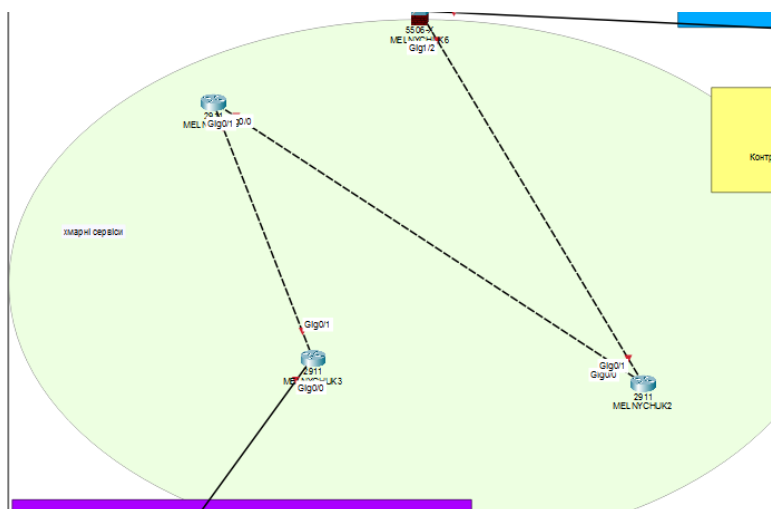


Рисунок 3.5 – Маршрутизатори інтернет-провайдера

Для обміну даними між елементами мережі, налаштовано базові налаштування комутаторів рівня доступу, такі як паролі та їх шифрування, доменні налаштування (рис. 3.6, додаток А).

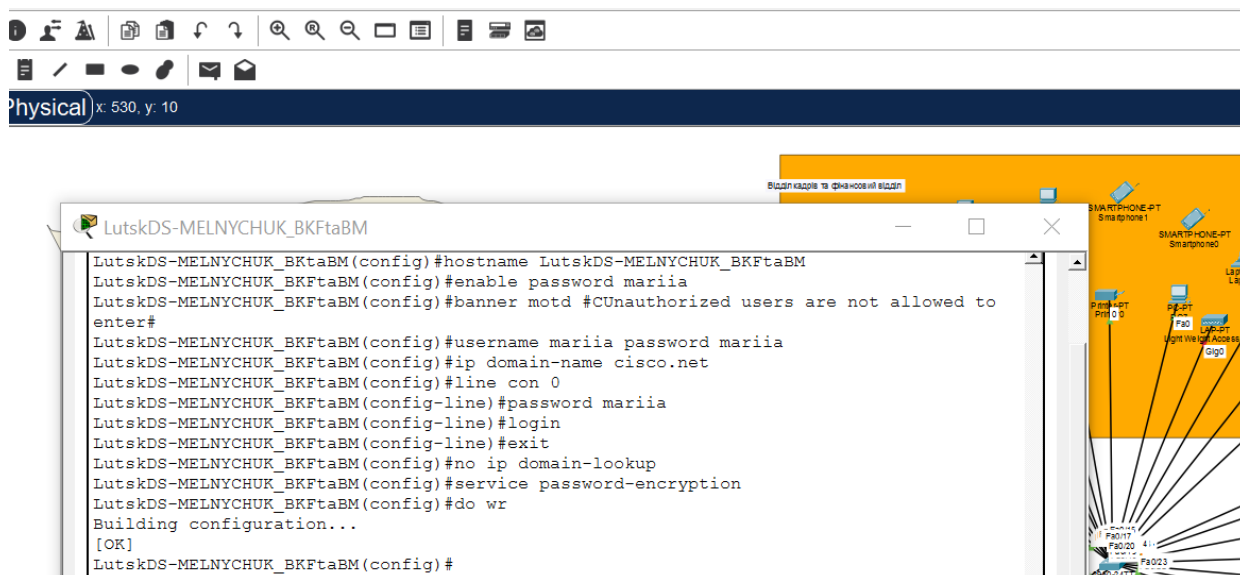


Рисунок 3.6 – Базові налаштування комутатора
LutskDS-MELNYCHUK_BKFtaBM

Далі проведено налаштування основного комутатора та голосового шлюзу (рис. 3.7).

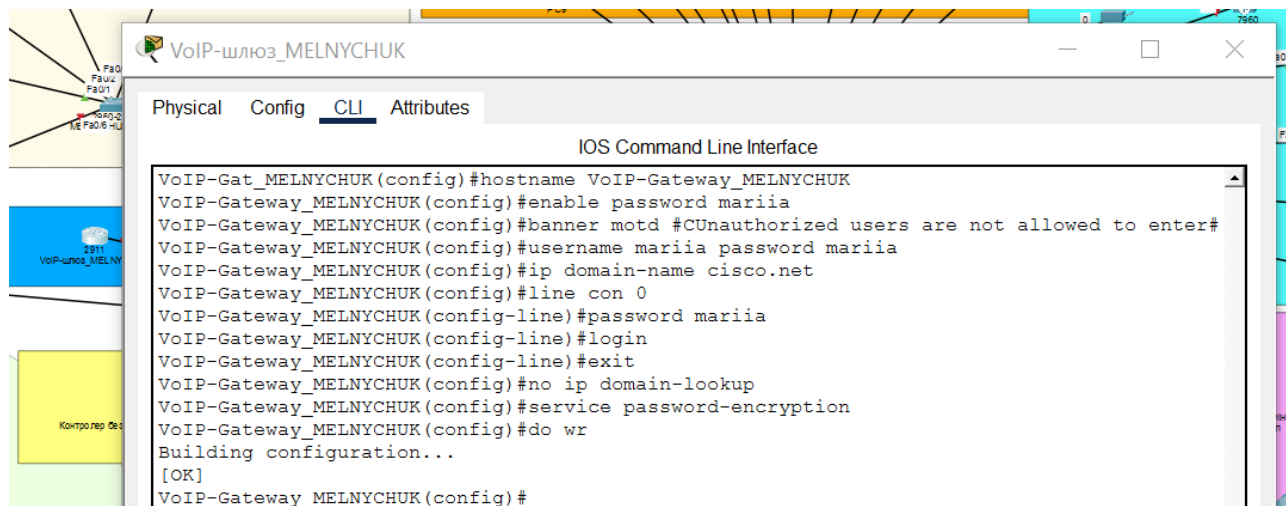


Рисунок 3.7 – Базові налаштування налаштування голосового шлюзу
VoIP-Gateway_MELNYCHUK

Налаштуємо дротові, бездротові та голосові vlan (рис. 3.8, додаток Б). Створюємо vlan 2, 3 та 4. Vlan 2 (назва VLAN2_DP) – дротові пристрої, vlan 3 (назва VLAN3_WLAN) – бездротові пристрої, vlan 4 (назва VLAN4_VOIP) – голосова vlan.

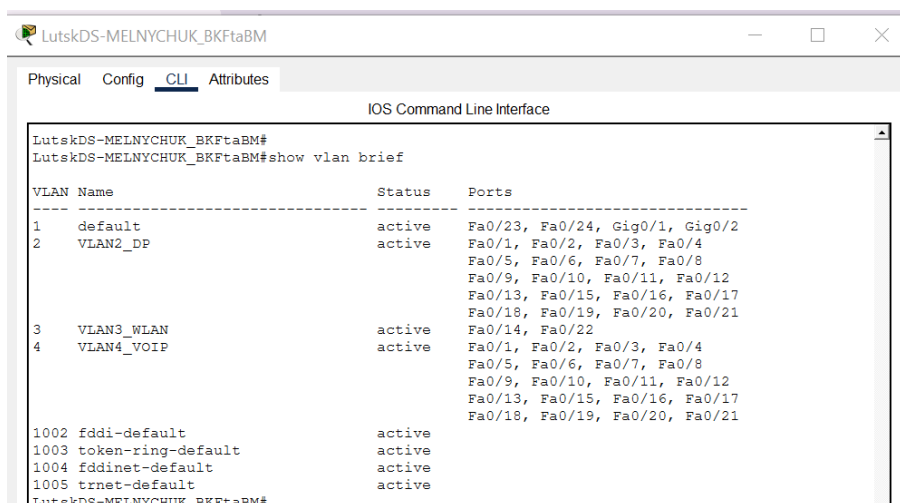


Рисунок 3.8 – Налаштування портів в відповідний vlan на комутаторі LutskDS-MELNYCHUK_BKftaBM

Після налаштувань комутаторів доступу, налаштовано комутатор рівня L3, тобто, основний комутатор, який з'єднує комутатори доступу в одну магістраль. На ньому, аналогічно до комутаторів доступу, налаштовуємо відповідні vlan (vlan 2 (назва VLAN2_DP) – дротові пристрої, vlan 3 (назва VLAN3_WLAN) – бездротові пристрої, vlan 4 (назва VLAN4_VOIP) – голосова vlan).

Контролер бездротової локальної мережі має бути в тій самій vlan, що і точки доступу, тобто vlan 3 (рис. 3.9).



Рисунок 3.9 – Налаштування порту контролера бездротової локальної мережі до vlan 3

Для передачі трафіку різних vlan потрібно налаштувати транкові порти. «Транковий порт – це канал точка-точка, через який передається трафік усіх

VLANів. Траковий порт не належить до жодного VLANу, цей порт передає тегований трафік. Транк може бути налаштований між свічками або свічкою та маршрутизатором».

Використаємо в подальшому налаштуванні технологію EtherChannel – це технологія об'єднання кількох фізичних каналів зв'язку між комутаторами або іншими мережевими пристроями в один логічний канал. Такий підхід забезпечує підвищення пропускної здатності, балансування навантаження та підвищення відмовостійкості мережевої інфраструктури. Замість використання одного каналу з високою швидкістю, EtherChannel дозволяє агрегувати кілька інтерфейсів, що працюють паралельно, створюючи єдиний логічний зв'язок.

Ключовим стандартом для реалізації цієї технології є Link Aggregation Control Protocol (LACP), визначений у специфікації IEEE 802.3ad. LACP автоматизує процес формування агрегованих каналів, забезпечуючи:

- динамічне узгодження параметрів між пристроями, що дозволяє уникнути конфліктів при налаштуванні;
- виявлення та виключення несправних лінків, що підвищує надійність роботи каналу;
- гнучке масштабування, оскільки кількість фізичних портів у групі може змінюватися залежно від потреб мережі.

У корпоративних мережах застосування EtherChannel з LACP має такі переваги:

- підвищення продуктивності (сумарна пропускна здатність логічного каналу дорівнює сумі швидкостей усіх фізичних інтерфейсів);
- балансування навантаження (трафік розподіляється між каналами відповідно до алгоритмів хешування (MAC-адреси, IP-адреси, порти TCP/UDP);
- відмовостійкість (вихід з ладу одного фізичного каналу не призводить до розриву логічного з'єднання);
- стандартизованість (використання LACP забезпечує сумісність між обладнанням різних виробників).

Таким чином, EtherChannel із застосуванням LACP є важливим інструментом побудови масштабованих і надійних корпоративних мереж, що відповідають сучасним вимогам до продуктивності та безпеки (рис. 3.10, додаток В).

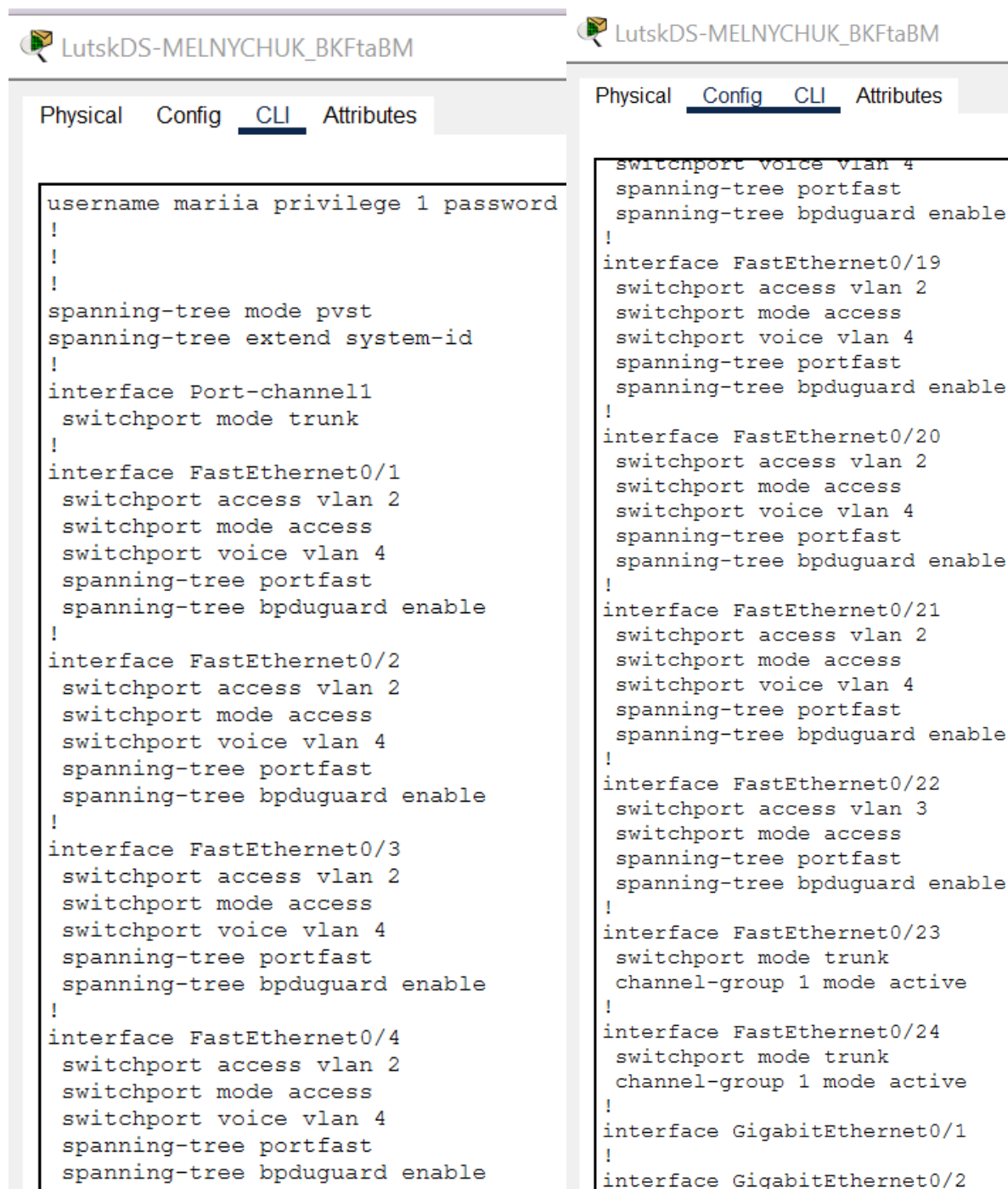
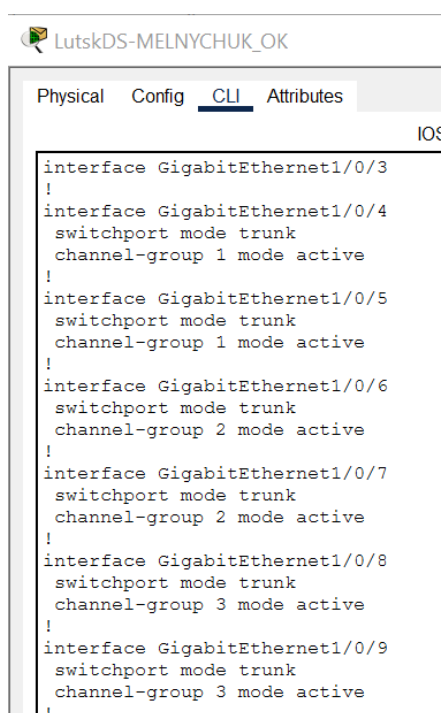


Рисунок 3.10 – Агрегація каналів на комутаторі
LutskDS-MELNYCHUK_BKFtaBM

Використаємо стандарт LACP для агрегації каналів. Агрегація каналів (link aggregation) у комп'ютерних мережах є технологією об'єднання декількох

фізичних каналів передачі даних у єдиний логічний канал з метою підвищення пропускної здатності, надійності та ефективності використання мережевих ресурсів. Такий підхід забезпечує паралельну передачу трафіку через кілька з'єднань, що дозволяє досягти сумарної пропускної здатності, більшої за можливості окремого каналу, а також реалізувати механізми резервування у випадку відмови окремих ліній зв'язку. Технологія широко застосовується в Ethernet-мережах у вигляді груп агрегованих каналів (LAG) та підтримується стандартами, зокрема IEEE 802.1AX, що регламентують принципи їх формування і балансування навантаження між каналами. У сучасних мережевих інфраструктурах агрегування каналів розглядається як ефективний інструмент підвищення продуктивності та відмовостійкості без необхідності переходу на більш дорогі високошвидкісні інтерфейси.

Для завершення налаштування агрегації потрібно провести налаштування між багаторівневим L3 комутатором LutskDS-MELNYCHUK_OK та комутаторами рівня доступу (рис. 3.11).



```

LutskDS-MELNYCHUK_OK
Physical Config CLI Attributes
IOS
interface GigabitEthernet1/0/3
!
interface GigabitEthernet1/0/4
switchport mode trunk
channel-group 1 mode active
!
interface GigabitEthernet1/0/5
switchport mode trunk
channel-group 1 mode active
!
interface GigabitEthernet1/0/6
switchport mode trunk
channel-group 2 mode active
!
interface GigabitEthernet1/0/7
switchport mode trunk
channel-group 2 mode active
!
interface GigabitEthernet1/0/8
switchport mode trunk
channel-group 3 mode active
!
interface GigabitEthernet1/0/9
switchport mode trunk
channel-group 3 mode active
!

```

Рисунок 3.11 – Приналежність портів L3 комутатора до створених каналів

Також налаштуємо як транковий порт interface GigabitEthernet1/0/3, який приєднує до VoIP-шлюзу (рис. 3.12).

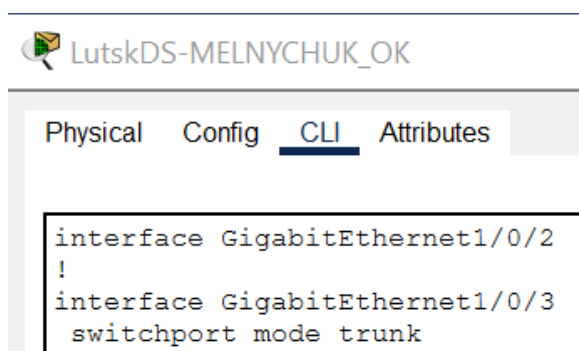


Рисунок 3.12 – Транковий порт interface GigabitEthernet1/0/3

Проведемо налаштування брандмауера. В налаштуваннях використаємо команду `no switchport` у Cisco IOS для переведення інтерфейсу комутатора з режиму Layer 2 (комутаторного) у режим Layer 3 (маршрутизованого), так як за замовчуванням порти комутатора працюють як switchport – тобто вони належать до певної VLAN і виконують функції комутації кадрів Ethernet (рис. 3.13). Виконання команди `no switchport` відключає ці функції, і порт стає маршрутизованим інтерфейсом, на який можна призначати IP-адресу та використовувати для маршрутизації пакетів між різними мережами. Практичне застосування: використовується на Layer 3 комутаторах, коли потрібно організувати маршрутизацію безпосередньо на комутаторі. Наприклад, для підключення комутатора до маршрутизатора або для створення інтерфейсу, що виконує роль шлюзу для VLAN.

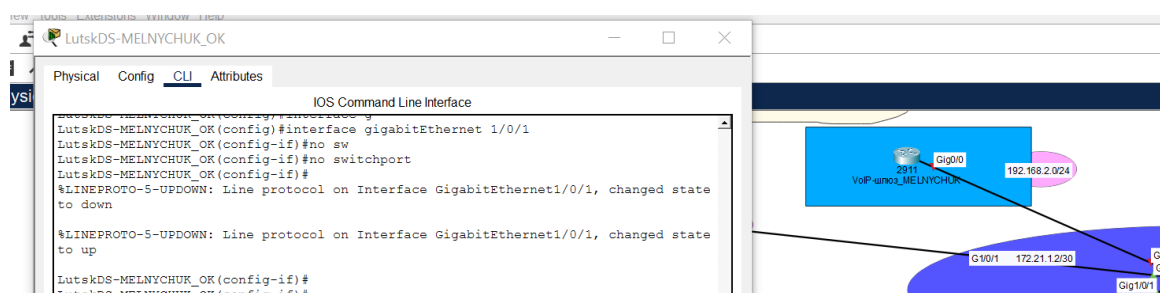


Рисунок 3.13 – Переведення інтерфейсу комутатора з режиму Layer 2 у режим Layer 3

В демілітаризованій зоні налаштовано сервери (рис. 3.14).

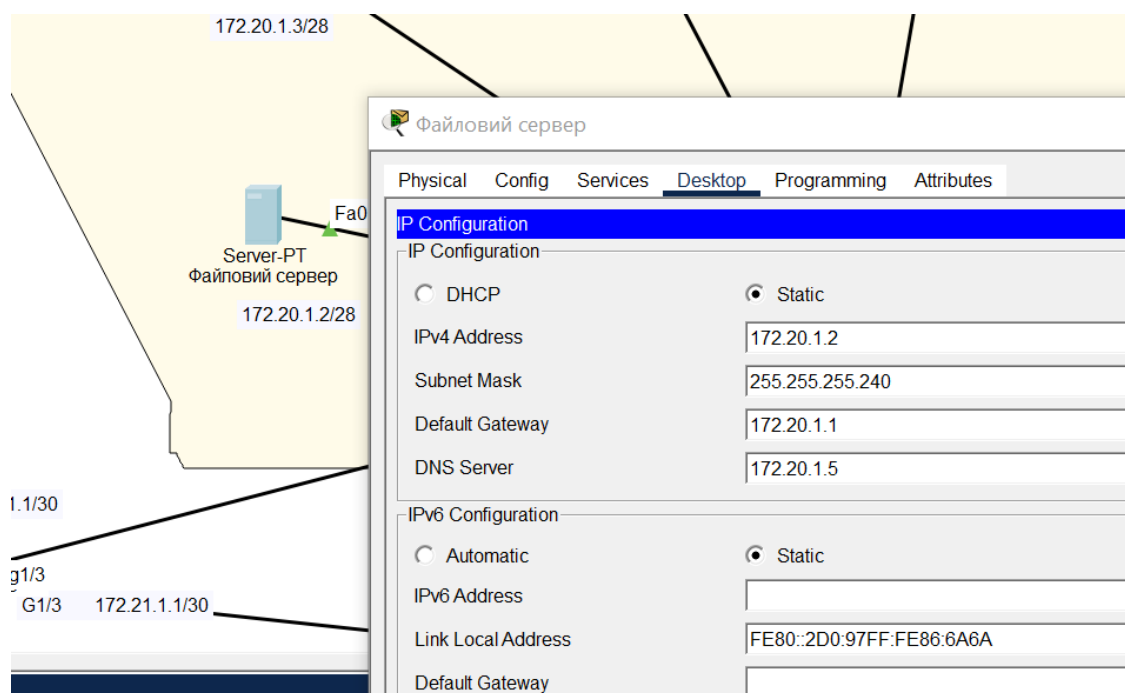


Рисунок 3.14 – Налаштування серверів в DMZ

Налаштуємо пристрої для мережі провайдера (рис. 3.15). На даному етапі виконано налаштування мережевого обладнання провайдера, яке забезпечує взаємодію між центральним офісом та віддаленими філіями компанії. На маршрутизаторі провайдера налаштовано IP-адресацію інтерфейсів, що з'єднують корпоративні майданчики, а також реалізовано протокол динамічної маршрутизації OSPF для автоматичного обміну маршрутною інформацією між мережевими сегментами. Це дозволяє забезпечити коректну передачу даних між усіма підключеними вузлами та спрощує подальше масштабування мережі.

Для підвищення надійності роботи мережевої інфраструктури виконано перевірку зв'язності між усіма вузлами провайдера, а також тестування процесу маршрутизації пакетів. Реалізована конфігурація забезпечує стабільне функціонування транспортної мережі та створює основу для подальшого впровадження сервісів VPN, міжмережевого екранування та інших засобів захисту інформації.

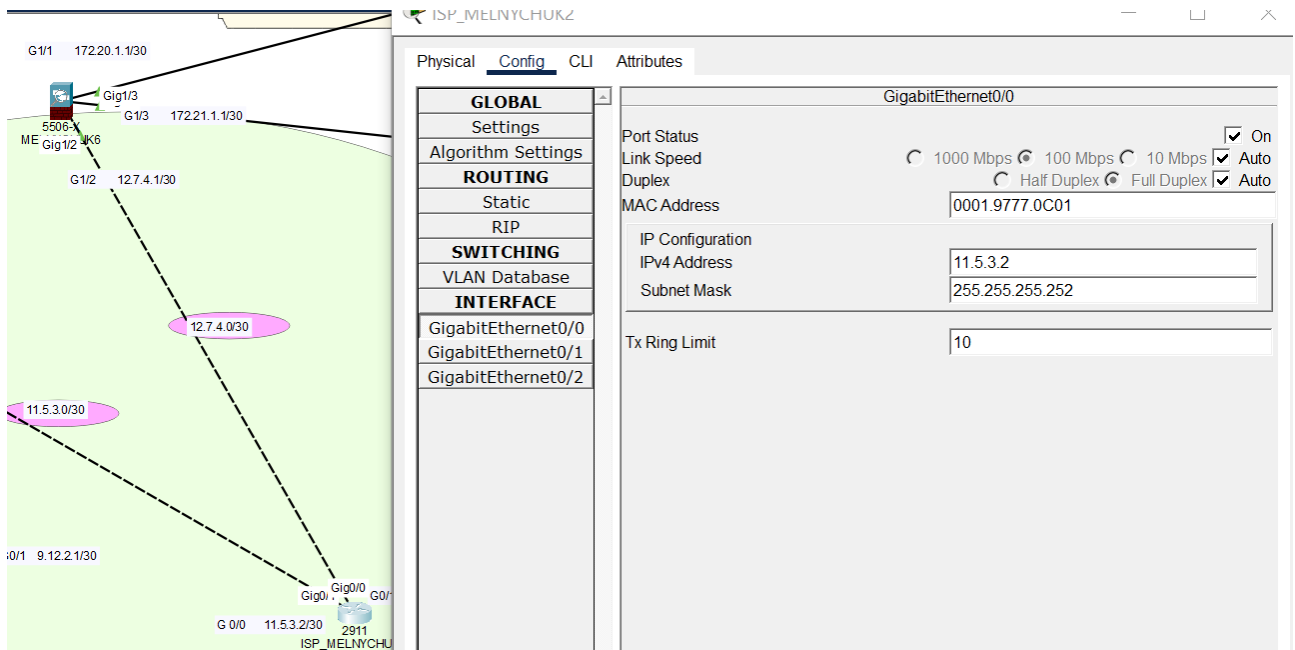


Рисунок 3.15 – Налаштування мережі провайдера

3.2 Налаштування DHCP

Проведемо налаштування DHCP та маршрутизації (рис. 3.16, додаток Г). Створюємо SVI інтерфейси. Для автоматизації процесу видачі IP-адрес клієнтським пристроям у мережі налаштовано службу DHCP (Dynamic Host Configuration Protocol). Використання DHCP дозволяє централізовано керувати параметрами мережевого підключення та усуває необхідність ручного налаштування адресації на кожному робочому місці.

У процесі конфігурування створено окремі DHCP-пули для кожного VLAN та структурного підрозділу компанії. Для кожного пулу визначено діапазон IP-адрес, маску підмережі, адресу шлюзу за замовчуванням та DNS-сервери. Також із діапазонів розподілу виключено адреси, зарезервовані для мережевого обладнання, серверів та інших пристроїв, що використовують статичну адресацію.

Після завершення налаштування проведено тестування роботи служби DHCP, під час якого клієнтські пристрої успішно отримали мережеві параметри в автоматичному режимі. Це підтвердило коректність роботи служби та забезпечило спрощене адміністрування корпоративної мережі.

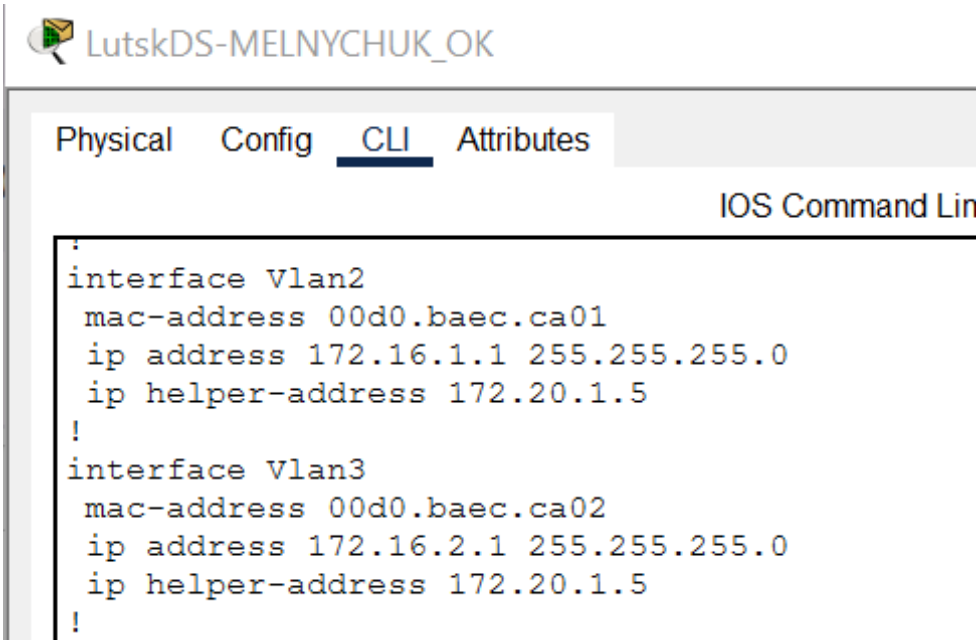


Рисунок 3.16 – Створюємо SVI інтерфейси

Налаштуємо DHCP-сервер (рис. 3.17).

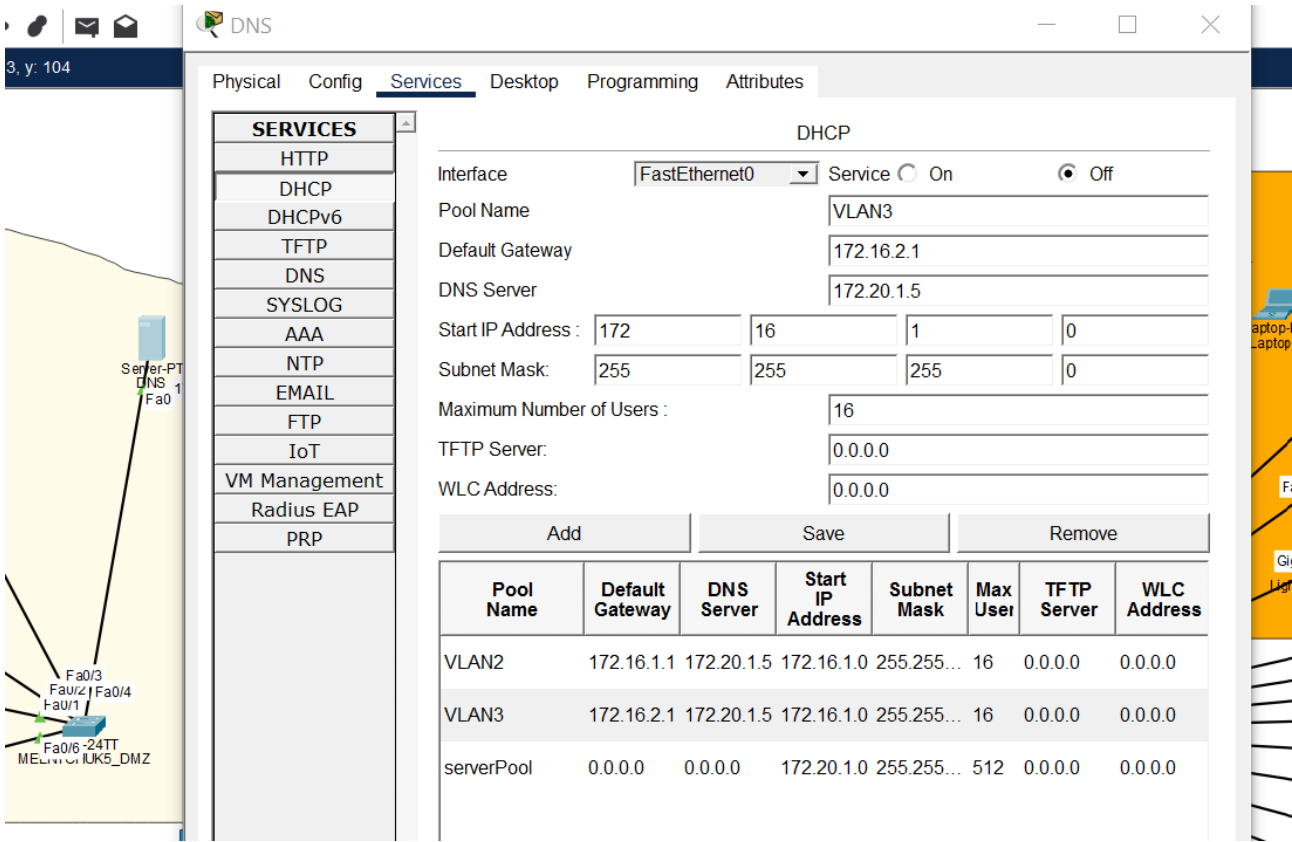


Рисунок 3.17 – Налаштування DHCP-сервера

3.3 Налаштування точок доступу

Налаштування точок доступу. Точки доступу контролюються контролером бездротової мережі (рис. 3.18). Для забезпечення бездротового доступу до корпоративної мережі виконано налаштування точок доступу Wi-Fi в усіх підрозділах компанії. Керування бездротовою інфраструктурою здійснюється централізовано за допомогою контролера бездротової мережі (WLC), що дозволяє спростити адміністрування, моніторинг та оновлення конфігурації мережі.

У процесі налаштування створено окремі бездротові мережі (SSID) для працівників компанії та гостей користувачів. Для кожної мережі визначено відповідні параметри безпеки, включаючи механізми автентифікації та шифрування трафіку. Бездротові мережі прив'язано до відповідних VLAN, що забезпечує логічне розділення трафіку та підвищує рівень захисту інформації.

Після завершення конфігурування проведено перевірку підключення клієнтських пристроїв, отримання мережевих параметрів через DHCP та доступу до необхідних ресурсів мережі. Результати тестування підтвердили коректну роботу бездротової інфраструктури та стабільне функціонування сервісів для співробітників і гостей компанії.

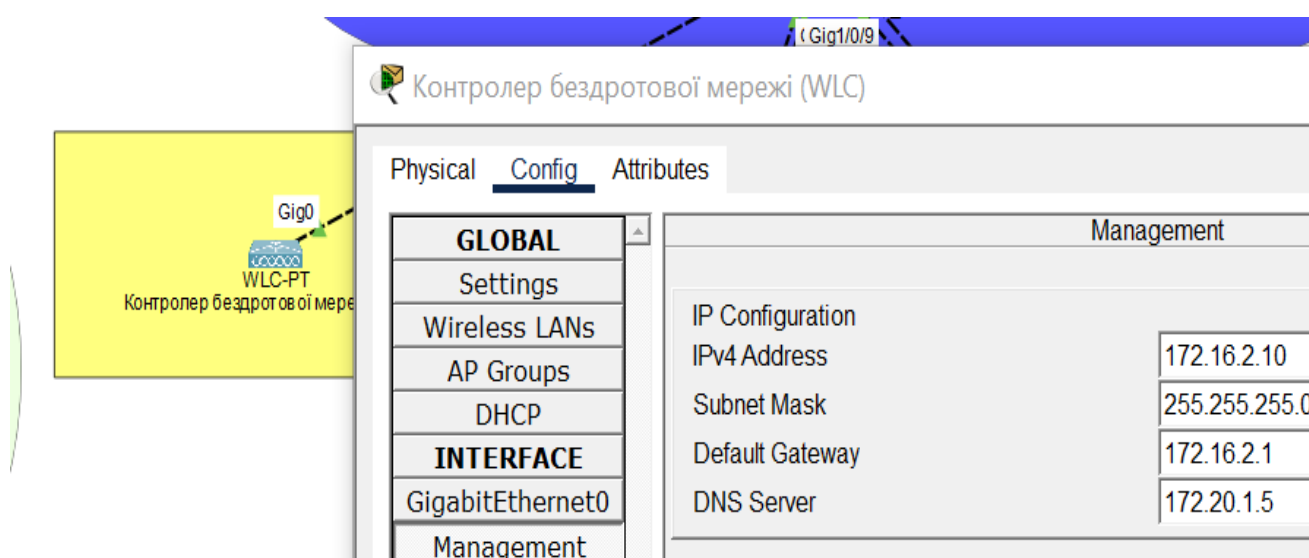


Рисунок 3.18 – Налаштування адресації контролера бездротової мережі

Налаштування WLC Address (рис. 3.19).

The screenshot shows the 'Services' tab in a network configuration interface. On the left, a list of services includes HTTP, DHCP, DHCPv6, TFTP, DNS, SYSLOG, AAA, NTP, EMAIL, FTP, IoT, VM Management, Radius EAP, and PRP. The 'DHCP' service is selected. The configuration fields for DHCP are as follows:

- Interface: FastEthernet0
- Service: ☒ On, ☐ Off
- Pool Name: VLAN3
- Default Gateway: 172.16.2.1
- DNS Server: 172.20.1.5
- Start IP Address: 172.16.1.0
- Subnet Mask: 255.255.255.0
- Maximum Number of Users: 16
- TFTP Server: 0.0.0.0
- WLC Address: 172.16.2.10 (highlighted with a blue circle)

Below the configuration fields are three buttons: 'Add', 'Save', and 'Remove'. At the bottom, a table lists the configured DHCP pools:

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
VLAN2	172.16.1.1	172.20.1.5	172.16.1.0	255.255.255.0	16	0.0.0.0	0.0.0.0
VLAN3	172.16.2.1	172.20.1.5	172.16.1.0	255.255.255.0	16	0.0.0.0	0.0.0.0
serverPool	0.0.0.0	0.0.0.0	172.20.1.0	255.255.255.0	512	0.0.0.0	0.0.0.0

Рисунок 3.19 – Налаштування WLC Address

Ввімкнемо процес маршрутизації IP-пакетів за допомогою команди `ip routing`. Так як за замовчуванням деякі пристрої (наприклад, Layer-3 Switch) можуть мати вимкнену маршрутизацію, команда `ip routing` активує функцію маршрутизації, дозволяючи пристрою пересилати пакети між різними VLAN або мережами. Після цього комутатор зможе працювати як маршрутизатор – виконувати інтер-VLAN routing, використовувати статичні маршрути чи протоколи динамічної маршрутизації (OSPF, EIGRP тощо). Якщо команда не задана, пристрій працює лише як комутатор другого рівня (L2) і не пересилає пакети між мережами (рис. 3.20-3.21).

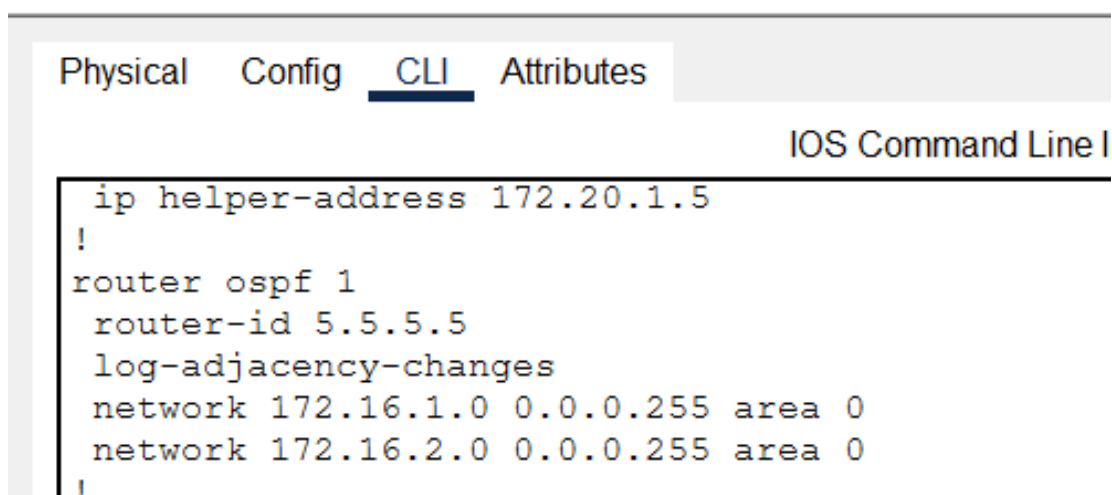


Рисунок 3.20 – Налаштування маршрутизації на комутаторі L3

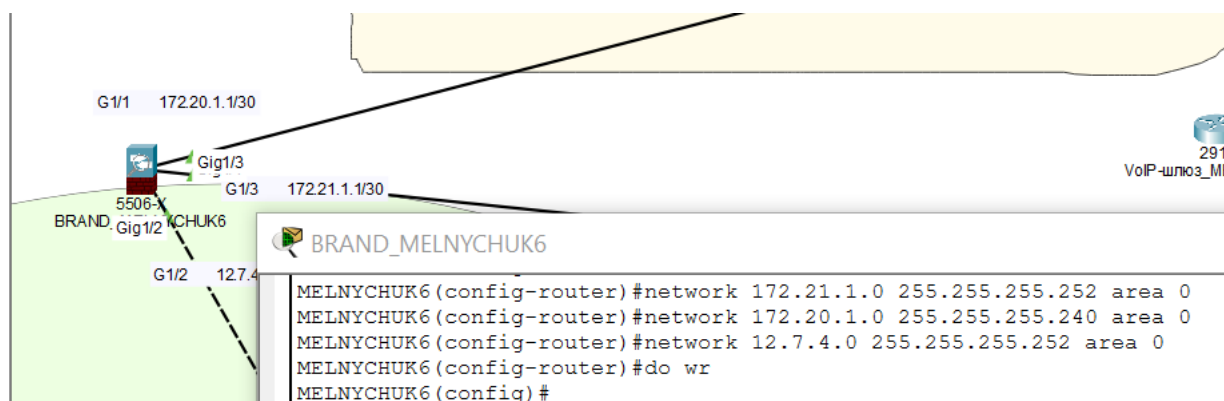


Рисунок 3.21 – Налаштування маршрутизації на брандмауері

Для того, щоб пристрої з локальної мережі могли досягати хостів в віддалених мережах, потрібно на брандмауері налаштувати NAT (рис. 3.22). Таким чином кілька пристроїв у локальній мережі могли виходити в Інтернет, використовуючи одну публічну IP-адресу. Це економить адресний простір і підвищує безпеку.

Спочатку налаштовано динамічний NAT між користувачами та демілітаризованою зоною. Dynamic NAT (динамічний NAT) означає, що внутрішні приватні IP-адреси зіставляються із пулом зовнішніх публічних адрес не статично, а динамічно. Тобто кожен раз, коли пристрій із локальної мережі виходить у зовнішню мережу, йому виділяється одна з доступних зовнішніх IP-адрес із пулу.

Особливості Dynamic NAT: внутрішні адреси не мають постійного відповідника у зовнішніх (відображення змінюється), потрібен пул зовнішніх IP-адрес (наприклад, кілька публічних адрес від провайдера), якщо зовнішніх адрес у пулі менше, ніж внутрішніх пристроїв, то частина пристроїв може тимчасово не отримати доступ до Інтернету.

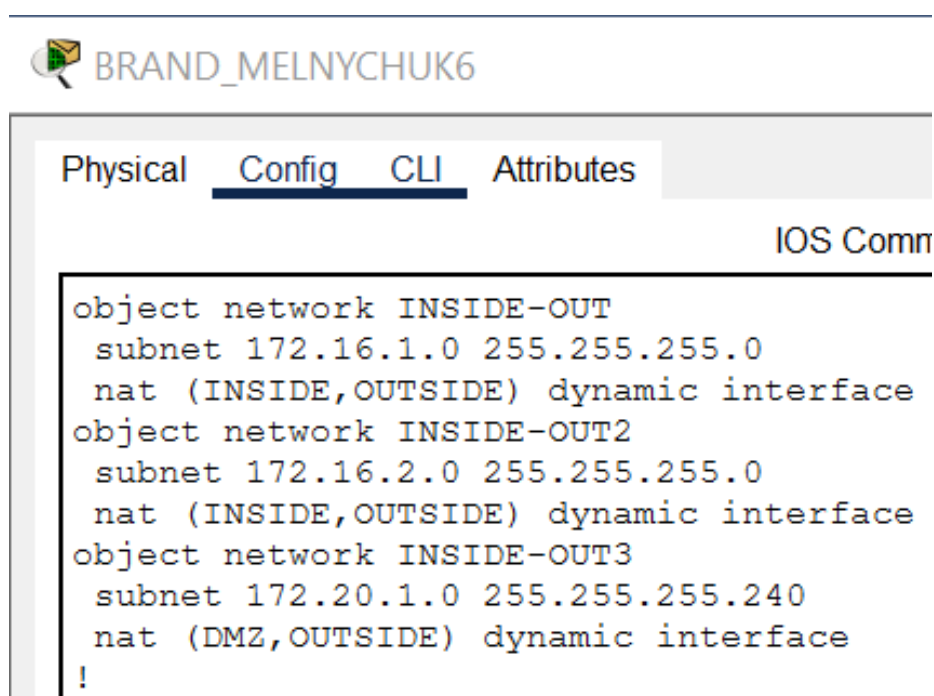


Рисунок 3.22 – Налаштування Dynamic NAT

Так як пункт призначення, який запитуватиме внутрішній хост, невідомий, потрібно налаштувати статичний NAT (рис. 3.23).

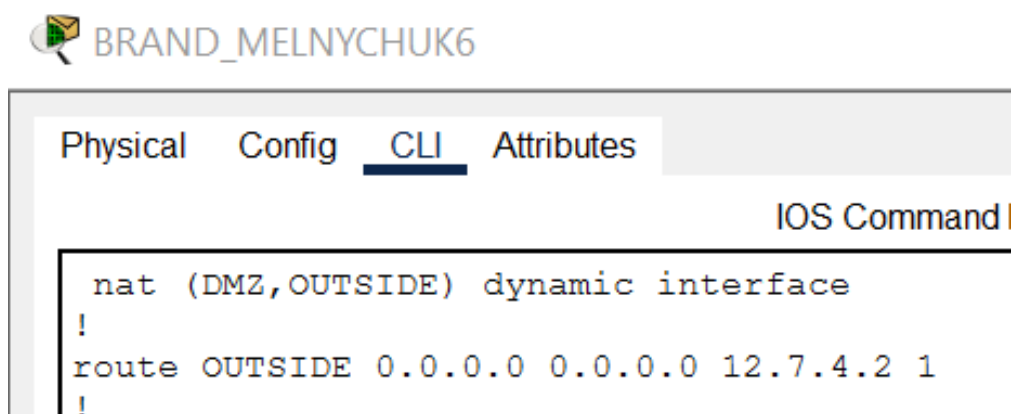


Рисунок 3.23 – Налаштування статичного NAT

3.4 Налаштування списків контролю доступу

Для забезпечення безпеки трафіку, створимо списки контролю доступу (рис. 3.24). Для підвищення рівня безпеки корпоративної мережі налаштовано списки контролю доступу (Access Control Lists, ACL), які забезпечують фільтрацію мережевого трафіку відповідно до встановленої політики безпеки. Використання ACL дозволяє контролювати взаємодію між окремими сегментами мережі та обмежувати доступ до критично важливих ресурсів.

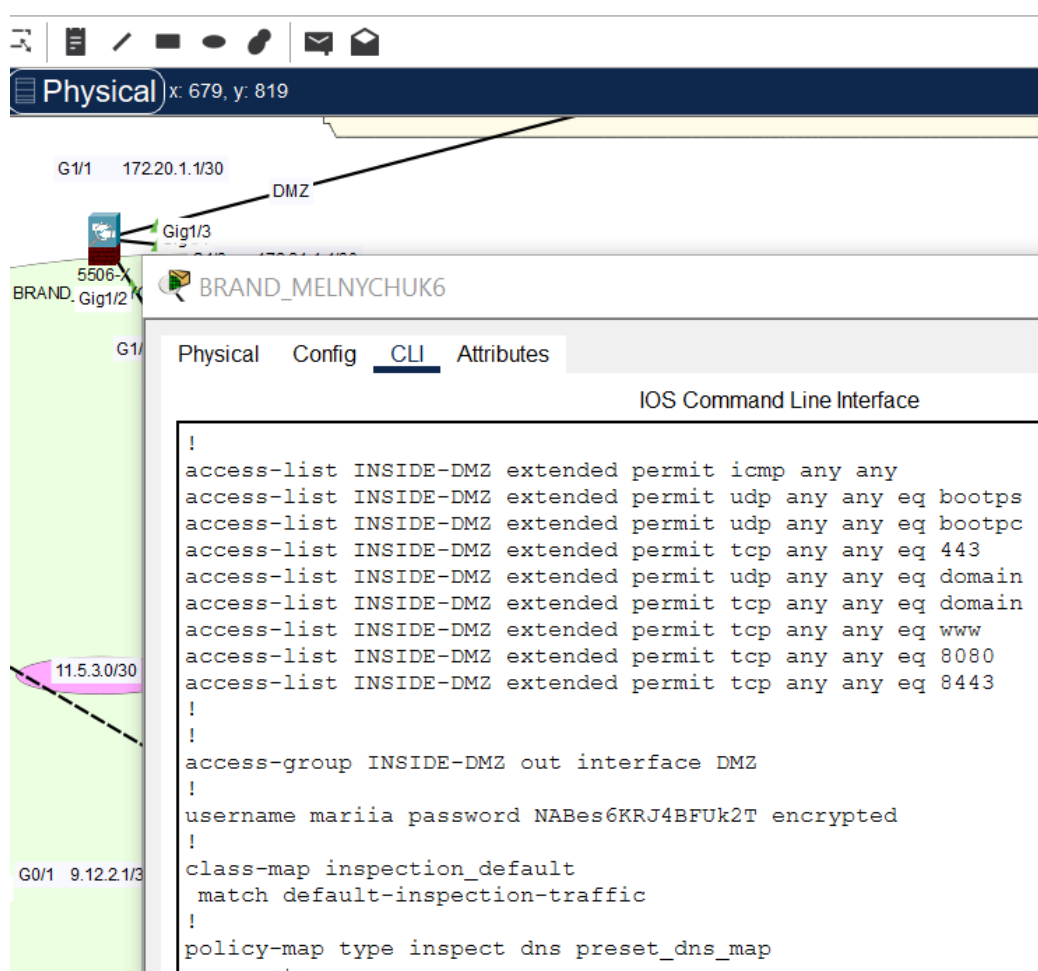


Рисунок 3.24 – Налаштування списків контролю доступу

У ході налаштування створено розширені списки контролю доступу, які застосовуються до інтерфейсів маршрутизаторів і комутаторів третього рівня. За допомогою правил ACL реалізовано обмеження доступу між різними VLAN, захист серверного сегмента від несанкціонованих підключень, а також контроль

доступу гостьової бездротової мережі до внутрішніх ресурсів компанії. При цьому дозволено лише необхідні мережеві сервіси та протоколи, потрібні для коректної роботи користувачів і мережевого обладнання.

Після впровадження списків контролю доступу проведено тестування політик фільтрації шляхом перевірки дозволених і заборонених мережевих з'єднань. Отримані результати підтвердили ефективність реалізованих механізмів захисту та відповідність мережі встановленим вимогам інформаційної безпеки.

3.5 Тестування працездатності мережі та аналіз результатів

Після завершення налаштування всіх компонентів корпоративної мережі проведено комплексне тестування її працездатності (рис. 3.25). Метою тестування стала перевірка коректності функціонування мережевих сервісів, маршрутизації, механізмів безпеки та взаємодії між центральним офісом і віддаленими філіями компанії.

У процесі тестування перевірено доступність мережевих пристроїв за допомогою команд ping та traceroute, що дозволило підтвердити наявність зв'язку між усіма сегментами мережі. Також виконано перевірку роботи протоколу маршрутизації OSPF, коректності обміну маршрутною інформацією та автоматичного оновлення таблиць маршрутизації. Результати показали стабільну роботу маршрутизації та відсутність втрати пакетів під час передачі даних між мережами.

Окрему увагу приділено перевірці функціонування служби DHCP, яка успішно надавала клієнтським пристроям необхідні параметри мережевого підключення. Тестування бездротової мережі підтвердило можливість підключення користувачів до відповідних SSID та отримання доступу до дозволених ресурсів відповідно до налаштованих політик безпеки.

Для оцінки ефективності механізмів захисту проведено перевірку роботи списків контролю доступу (ACL) та міжмережевих екранів. Результати тестування підтвердили коректне блокування несанкціонованого трафіку та дотримання

встановлених правил доступу між VLAN, серверними сегментами та гостьовими мережами.

За результатами проведених випробувань встановлено, що спроектована корпоративна мережа забезпечує стабільний обмін даними між усіма підрозділами компанії, підтримує необхідний рівень продуктивності та відповідає вимогам щодо надійності, масштабованості й інформаційної безпеки.

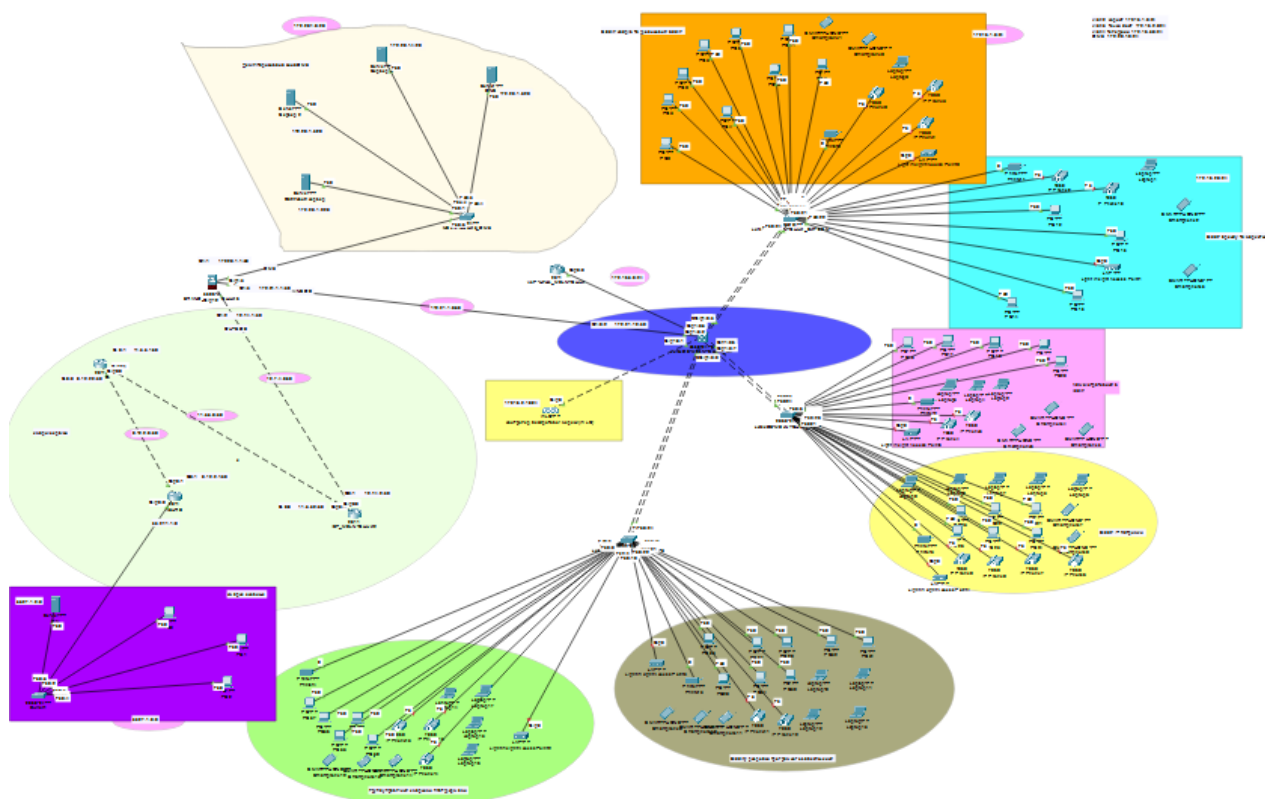


Рисунок 3.25 – Проєкт мережі

Отримані результати підтверджують правильність обраних технічних рішень та можливість подальшого розвитку мережевої інфраструктури без суттєвих змін її архітектури.

ВИСНОВКИ

У процесі виконання кваліфікаційної роботи досліджено теоретичні та практичні аспекти побудови корпоративних комп'ютерних мереж, а також виконано проєктування мережевої інфраструктури для ІТ-компанії «Digital Solutions».

У ході роботи проаналізовано основні принципи функціонування корпоративних мереж, сучасні мережеві архітектури та протоколи, а також підходи до сегментації мережі та забезпечення її безпеки. Це дозволило сформувати базу для подальшого практичного проєктування та вибору оптимальних технічних рішень.

На основі аналізу діяльності компанії розроблено логічну структуру корпоративної мережі, яка враховує потреби різних підрозділів, забезпечує ефективний обмін даними та можливість масштабування інфраструктури в майбутньому.

У практичній частині роботи виконано налаштування ключових мережевих сервісів, зокрема DMZ-зони, DHCP-сервера, бездротової інфраструктури Wi-Fi та списків контролю доступу (ACL). Це забезпечило коректну організацію мережевого трафіку, автоматизацію адресації, розмежування доступу користувачів та підвищення рівня інформаційної безпеки.

Проведене тестування працездатності мережі підтвердило правильність обраних рішень і коректність налаштування всіх компонентів. Результати перевірки показали стабільну роботу мережі, відсутність критичних помилок та відповідність розробленої інфраструктури вимогам щодо продуктивності, надійності та безпеки.

Отже, поставлена мета роботи досягнута, а розроблена модель корпоративної мережі ІТ-компанії «Digital Solutions» може бути використана як основа для впровадження з подальшим розширенням і модернізацією.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Комп'ютерні мережі. Книга 1: навчальний посібник / А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник. Львів: «Магнолія 2006», 2023. 256 с.
2. Комп'ютерні мережі. Книга 2: навчальний посібник / А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник. Львів: «Магнолія 2006», 2023. 312 с.
3. Мережні топології. StudFiles. URL: <https://studfile.net/preview/7446861/page:9/> (дата звернення: 22.02.2026).
4. Класифікація комп'ютерних мереж URL: <https://mozok.click/736-klasifikacya-kompyuternih-merezh.html> (дата звернення: 15.02.2026).
5. SD-WAN: що це і як працює програмно-визначена мережа Netwave. URL: <https://netwave.ua/blog/sd-wan-sho-ce-i-yak-pracyuye/> (дата звернення: 27.02.2026).
6. Що таке клієнт-серверна архітектура? Для новачків! 2025. YouTube. URL: <https://www.youtube.com/watch?v=4zcs36NLmQ8> (дата звернення: 03.03.2026).
7. TCP/IP. Безпека та відеоспостереження. URL: <https://oxorona.com/tcp-ip/> (дата звернення: 05.03.2026).
8. Костюченко А.О., Цибко Г.Ю. Адресація в комп'ютерних мережах: навчально-методичний посібник. URL: <http://erpub.chnpu.edu.ua:8080/jspui/bitstream/> (дата звернення: 07.03.2026)
9. Буров Є.В., Митник М.М. Комп'ютерні мережі. Підручник. Том 1. Львів: «Магнолія 2006», 2021. 340 с.
10. Комп'ютерні мережі. Підручник. Том другий /Є.В. Буров, М.М. Митник/ Львів: Видавництво ПП «Магнолія 2006», 2024. 204 с.
11. Технологія VLAN. Об'єднання офісів у локальну мережу. Westelecom. URL: <https://westelecom.ua/blog/tehnologia-vlan-obedinenie-ofisov-v-lokalnuu-virtualnuu-set> (дата звернення: 10.03.2026).
12. Що таке DHCP? Простий посібник із розуміння призначення IP-адрес. Fiberroad Technology. URL: <https://fiberroad.com/uk/resources/glossary/what-is-dhcp/> (дата звернення: 14.03.2026).

13. Що таке DNS, як працює DNS-сервер та як прописати NS-сервери. URL: <https://cityhost.ua/uk/blog/scho-take-dns-ta-yak-pracyu-sistema-domennih-imen.html> (дата звернення: 18.03.2026).

14. KnowledgeCatch. Routing and Routing Protocols Simplified: BGP, OSPF, RIP, 2024. YouTube. URL: <https://www.youtube.com/watch?v=rLNmrFh-sd8> (date of access: 22.03.2026).

15. Протокол зв'язуючого дерева STP та його модифікації. URL: <https://surl.lu/vbjtgo> (date of access: 26.03.2026).

16. Що таке Протокол часової синхронізації мережі (NTP). Терміни та визначення кібербезпеки. KeepSolid VPN Unlimited. URL: <https://surl.li/gdhvyg> (дата звернення: 27.03.2026).

17. ManageEngine FSO. Associating SNMP credentials in NetFlow Analyzer, 2024. YouTube. URL: <https://www.youtube.com/watch?v=MJvxs0ncdks> (date of access: 02.04.2026).

18. Watch and Learn. 006 Security Protocols: SSL/TLS, IPSec, VPNs, SSH Protecting Data in Transit, 2023. YouTube. URL: <https://www.youtube.com/watch?v=SI5Ae98mApQ> (date of access: 05.04.2026).

19. Contributors to Wikimedia projects. Defense in depth (computing) - Wikipedia. Wikipedia, the free encyclopedia. URL: [https://en.wikipedia.org/wiki/Defense_in_depth_\(computing\)](https://en.wikipedia.org/wiki/Defense_in_depth_(computing)) (date of access: 14.04.2026).

20. NIST Technical Series Publications. URL: <https://surl.li/nhzqsh> (date of access: 18.04.2026).

21. What Is Zero Trust Architecture? | Microsoft Security. Your request has been blocked. This could be due to several reasons. URL: <https://www.microsoft.com/en-us/security/business/security-101/what-is-zero-trust-architecture> (date of access: 23.04.2026).

22. Міжмережевий екран нового покоління NGFW. Westelecom. URL: <https://westelecom.ua/blog/mezsetevoj-ekran-novogo-pokolenia-ngfw-cto-eto-i-zacem-on-nuzen> (дата звернення: 25.04.2026).

23. Що таке IPS/IDS і де застосовується. HostZealot. URL: <https://www.hostzealot.com.ua/blog/about-solutions/shho-take-ipsids-i-de-zastosovujetsya> (дата звернення: 28.04.2026).

24. Contributors to Wikimedia projects. IEEE 802.1X Wikipedia. Wikipedia, the free encyclopedia. URL: https://en.wikipedia.org/wiki/IEEE_802.1X (date of access: 01.05.2026).

25. WPA, WPA2, WPA3: у чому різниця між стандартами безпеки Wi-Fi? URL: <https://www.strong-eu.com/ua/blog/wpa-wpa2-wpa3-what-are-the-differences-between-wi-fi-security-standards> (дата звернення: 08.05.2026).

26. Curic M., Chris van Maastricht, Tattis T. What is Intent Based Networking? IBM. URL: <https://www.ibm.com/think/topics/intent-based-networking> (date of access: 10.05.2026).

27. Schneider J., Susnjara S., Smalley I. What is Hyperconverged Infrastructure? IBM. URL: <https://www.ibm.com/think/topics/hyperconverged-infrastructure> (date of access: 11.05.2026).

28. 10 Типів організаційних структур компаній. Worksection. URL: <https://worksection.com/ua/blog/10-types-of-organizational-structures-for-companies.html> (дата звернення: 12.05.2026).

29. Учасники проєктів Вікімедіа. EtherChannel – Вікіпедія. Вікіпедія. URL: <https://uk.wikipedia.org/wiki/EtherChannel> (дата звернення: 13.05.2026).

30. Що таке мережа DMZ? | IT Education Center Blog - блог навчального центру DevOps ITEDU by NETFORCE Group. IT Education Center Blog. URL: https://itedu.center/ua/blog/articles/dmz_network/?srsltid=AfmBOoqBu_uZAGy4k8tSlO4naUOpBT3qvRas6O7e_ZwlqEWPJXFgT3A1 (дата звернення: 13.05.2026).