НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ

І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

Факультет ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ПОГОДЖЕНО	**ДОПУСКАЄТЬСЯ ДО ЗАХИСТУ**
Декан факультету Інформаційних технологій	**Завідувач кафедри** Комп'ютерних систем, мереж та кібербезпеки
_____Ігор БОЛБОТ (підпис)	_____Дмитро КАСАТКІН (підпис)
«___»_____2026 р.	«___»_____2026 р.

БАКАЛАВРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

На тему: «Розробка корпоративної мережі ІТ компанії»

Спеціальність F7 «Комп’ютерна інженерія»

Освітньо-професійна програма «Комп’ютерна інженерія»

Гарант освітньої програми канд. фіз.-мат. наук, доцент	_____ (підпис)	**Євгеній НІКІТЕНКО**
Керівник бакалаврської кваліфікаційної роботи ст. викладач	_____ (підпис)	**Володимир МАТІЄВСЬКИЙ**
Виконав	_____ (підпис)	**Денис БОБИР**

КИЇВ-2026

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ
Факультет ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ЗАТВЕРДЖУЮ
Завідувач кафедри
комп'ютерних систем, мереж та кібербезпеки
канд. пед. наук, доцент_____Дмитро КАСАТКІН
«_____»_____20____ р.

З А В Д А Н Н Я

ДО ВИКОНАННЯ БАКАЛАВРСЬКОЇ КВАЛІФІКАЦІЙНОЇ РОБОТИ
ЗДОБУВАЧУ

Бобирю Денису Григоровичу
(прізвище, ім'я, по батькові)
Спеціальність «Комп'ютерна інженерія »

Освітньо-професійна програма «Комп'ютерна інженерія »

Тема кваліфікаційної бакалаврської роботи
«Розробка корпоративної мережі ІТ компанії
»
затверджена наказом ректора НУБіП України від «10»___12_____2025 р. №___3072 «С»___
Термін подання завершеної роботи на кафедру «15»___05_____2026 р.
Вихідні дані до бакалаврської кваліфікаційної роботи
вимоги до корпоративної мережі ІТ компанії
Специфікації пристроїв
Перелік питань, що підлягають дослідженню:
Теоретичні основи побудови мереж; Дослідження заходів безпеки для корпоративних мереж
Проєктування мережі ІТ компанії; Створення моделі та її тестування
Перелік графічного матеріалу (за необхідності).

Дата видачі завдання "__10__"_____12_____2025 р.

Керівник бакалаврської кваліфікаційної роботи _____ **Володимир МАТІЄВСЬКИЙ**
ст. викладач (підпис)

Завдання взяв до виконання _____ **Денис БОБИР**
(підпис)

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1	Аналіз вимог до комп’ютерної мережі	10.03.2026 р.	Виконано
2	Проєктування комп’ютерної мережі	15.03.2026	Виконано
3	Моделювання комп’ютерної мережі	20.04.2026	Виконано
4	Тестування розробленої моделі комп’ютерної мережі	07.05.2026	Виконано
5	Оформлення пояснювальної записки	24.05.2026	Виконано

Студент_____ / Денис БОБИР /
(підпис) (ініціали та прізвище)

Керівник проекту (роботи)_____ / Володимир МАТІЄВСЬКИЙ/
(підпис) (ініціали та прізвище)

РЕФЕРАТ

Пояснювальна записка: 64 сторінки, 36 рисунків, 4 таблиці, 6 додатків, 10 джерел.

У цій роботі проведено комплексне дослідження, що охоплює життєвий цикл створення сучасної мережевої інфраструктури для IT-компанії — від теоретичного фундаменту та ідеї мережі, до фінальної реалізації та перевірки готового рішення. Основний акцент зроблено на балансі між високою продуктивністю, масштабованістю механізмів безпеки.

У першому розділі закладено методологічний фундамент проєктування корпоративних мереж. Проаналізовано архітектурні особливості IT-інфраструктури та стек протоколів TCP/IP. Окрему увагу приділено технології VLAN, а також сервісам DHCP і DNS, які забезпечують автоматизацію адміністрування та прозору взаємодію користувачів із мережевими ресурсами.

Другий розділ присвячено питанням кібербезпеки та захисту конфіденційної інформації. Розглянуто методи захисту на канальному та мережевому рівнях моделі OSI. Зокрема, обґрунтовано принципи роботи міжмережевих екранів та застосування списків контролю доступу (ACL) для фільтрації трафіку й запобігання несанкціонованому втручанню.

У третьому розділі розроблено практичний проєкт мережі для IT-підприємства. Сформульовано технічні вимоги до обладнання, спроєктовано логічну структуру та розраховано IP-адресацію для 14 клієнтських пристроїв (10 ПК та 4 ноутбуки). Завдяки сегментації через VLAN оптимізовано керування мережею та підвищено її відмовостійкість.

У четвертому розділі описано практичну реалізацію та тестування розробленої моделі в середовищі Cisco Packet Tracer. У процесі симуляції налаштовано мережеве обладнання, розгорнуто серверні служби та впроваджено динамічну маршрутизацію на базі протоколу OSPF. Фінальне тестування підтвердило працездатність, масштабованість та готовність створеної моделі до експлуатації.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ ТА УМОВНИХ ПОЗНАЧЕНЬ

ACL (Access Control List) − список контролю доступу

CLI (Command Line Interface) − інтерфейс командного рядка

DHCP (Dynamic Host Configuration Protocol) − протокол динамічного налаштування вузла

DNS (Domain Name System) − система доменних імен

FW (Firewall) − міжмережевий екран

HTTP (HyperText Transfer Protocol) − протокол передачі гіпертексту

IP (Internet Protocol) − міжмережевий протокол

L2/L3 (Layer 2 / Layer 3) − рівні моделі OSI 2 та 3

LAN (Local Area Network) − локальна комп'ютерна мережа

OSI (Open Systems Interconnection) − еталонна модель взаємодії відкритих систем

OSPF (Open Shortest Path First) − протокол динамічної маршрутизації

SVI (Switched Virtual Interface) −логічний інтерфейс на комутаторі

VLAN (Virtual Local Area Network) − віртуальна локальна мережа

ВСТУП

В умовах стрімкої глобальної цифровізації та безперервного технологічного прогресу роль комп’ютерних мереж вийшла далеко за межі звичайного технічного супроводу. Сьогодні надійна мережева інфраструктура – це фундаментальний стратегічний актив фактично «нервова система» будь-якої сучасної IT-компанії. Успіх технологічного бізнесу безпосередньо залежить від якості побудови мережевого простору, адже саме він забезпечує безперебійний доступ до даних, ефективну командну взаємодію всіх підрозділів в умовах гібридної роботи та безпечне зберігання інтелектуальної власності.

Будь-який, навіть короткочасний збій у роботі мережі або найменша вразливість у системі захисту можуть спровокувати ланцюгову реакцію, від паралізації розробки програмних продуктів до серйозних фінансових втрат і втрати довіри клієнтів. Особливої ваги сьогодні набувають питання створення адаптивної інфраструктури, здатної не просто функціонувати «тут і зараз», а й динамічно масштабуватися. Сучасні інженерні рішення повинні забезпечувати баланс між високою пропускною здатністю та складними механізмами кібербезпеки. Впровадження технологій логічної сегментації на базі VLAN, використання протоколів динамічної маршрутизації (зокрема OSPF) та інтеграція потужних міжмережевих екранів (таких як Cisco ASA) дозволяє створювати керовані екосистеми, що відповідають суворим стандартам IT-індустрії. Саме тому в нашому проєкті була приділена особлива увага сегментації та налаштуванню безпеки.

Метою даної роботи є проєктування та комплексна практична реалізація життєздатної моделі комп’ютерної мережі, яка адаптована під потреби IT-компанії (на 50-70 робочих місць) з можливістю стрімкого та комфортного розширення в майбутньому. Дослідження базується на використанні актуальних технологічних стеків Cisco, що дозволяють мінімізувати потенційні ризики та оптимізувати розподіл мережевих потоків між різними департаментами.

Для досягнення цієї мети нами було окреслено та послідовно розв’язано такі завдання:

– здійснити аналіз теоретичних основ побудови корпоративних мереж за ієрархічною моделлю (Core, Distribution, Access), що дозволило виокремити ключові принципи стабільності сучасних інфраструктурних рішень;

– дослідити специфічні потреби IT-сектору, де вимоги до відмовостійкості та захищеності каналів зв’язку вимагають особливо уважного підходу до вибору архітектури та активного обладнання;

– розробити детальну логічну структуру мережі, де за допомогою технології VLAN було відокремлено 6 різних сегментів мережі ієрархічної системи IP-адресації, та реалізовано ефективну модель ізоляції підрозділів (Developers, HR, Management тощо);

– спроєктувати та впровадити систему захисту, що включає налаштування списків контролю доступу (ACL) який був налаштований на SW1-CORE та конфігурування засобів міжмережевого екранування для запобігання зовнішнім і внутрішнім загрозам;

– провести практичну перевірку розробленої моделі через налаштування реальних конфігурацій (маршрутизації, серверних служб DHCP, DNS) та фінальне тестування працездатності систем безпеки, таких як ACL.

Об’єктом дослідження виступає комп’ютерна мережа IT-компанії як цілісна, багатокомпонентна та динамічна система.

Предметом дослідження є сукупність методологічних підходів, протоколів маршрутизації та апаратно-програмних засобів, спрямованих на проєктування та забезпечення безпеки корпоративного середовища.

Практична цінність отриманих результатів полягає у створенні деталізованої архітектурної моделі та набору конфігураційних сценаріїв, які можуть бути використані як готовий шаблон для побудови мереж у реальному секторі, забезпечуючи високу автоматизацію адміністрування та безпеку даних.

РОЗДІЛ 1: АНАЛІЗ ВИМОГ ТА ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ МЕРЕЖІ ІТ-КОМПАНІЇ

1.1. Поняття та структура комп'ютерних мереж підприємств

На сучасному етапі розвитку інформаційних технологій комп'ютерна мережа підприємства вже давно вийшла за межі простої технічної надбудови. Сьогодні – це складна, динамічна та багатофункціональна система, що інтегрує в єдиний організм робочі станції персоналу, серверні потужності та різноманітні інтелектуальні пристрої. Якщо говорити просто, то це «фундамент», на якому тримається весь операційний процес будь-якої сучасної ІТ-компанії. Саме завдяки професійно побудованій мережі співробітники отримують можливість не просто обмінюватися повідомленнями, а працювати в єдиному інформаційному полі, спільно використовуючи бази даних, спеціалізований софт та дороге мережеве обладнання. Важливо розуміти, що мережа дозволяє реалізувати концепцію централізованого зберігання інформації: будь-який документ чи проєкт доступний авторизованому користувачу з будь-якого робочого місця, що в рази підвищує мобільність та продуктивність колективу.

Окрім того, сучасна мережа повинна забезпечувати безперебійну роботу хмарних сервісів та внутрішніх систем автоматизації, що робить її роль критичною для виживання бізнесу.

Порівнюючи корпоративну мережу зі звичайною домашньою мережею, ми бачимо колосальну різницю не лише в кількості кабелів, а й у самій філософії побудови. Домашній роутер обслуговує кілька гаджетів, тоді як мережа підприємства має справу з сотнями, а іноді й тисячами підключень одночасно. Це висуває надзвичайно жорсткі вимоги до таких параметрів, як пропускна здатність та відмовостійкість. У бізнес-середовищі кожна хвилина простою мережі конвертується у прямі фінансові збитки, тому надійність тут – це не побажання, а критична необхідність. Крім того, на перший план виходить інформаційна безпека. Корпоративні дані – це інтелектуальна власність, ціна

якої на ринку може бути дуже високою, тому захист від зовнішніх атак та внутрішніх витоків закладається ще на етапі проектування архітектури.

Географічно такі мережі можуть бути локалізовані в одному офісі або ж розтягуватися на цілі країни, поєднуючи віддалені філії через зашифровані канали VPN. За своєю суттю вони є локальними (LAN), але за потреби легко інтегруються в регіональні (MAN) та глобальні (WAN) структури, використовуючи при цьому стандартизований стек протоколів TCP/IP та технології Ethernet.

Типова структура мережі великого підприємства ніколи не будується хаотично. Зазвичай використовується перевірена ієрархічна модель, що складається з трьох функціональних рівнів:

1. Рівень доступу (Access Layer). Це те, що ми бачимо безпосередньо в офісі: розетки, до яких підключаються комп'ютери, принтери, IP-телефони чи точки доступу Wi-Fi. Його головна задача − прийняти користувача в мережу, забезпечити йому первинний зв'язок та провести базову ідентифікацію пристрою.

2. Рівень розподілу (Distribution Layer). Тут зосереджена вся «інтелектуальна» робота. Комутатори цього рівня займаються маршрутизацією трафіку між віртуальними локальними мережами, розділяють мережу на окремі логічні зони та стежать за виконанням правил безпеки за допомогою списків контролю доступу (ACL).

3. Ядро мережі (Core Layer). Це найпотужніша частина системи. Вона призначена для того, щоб максимально швидко, без жодних затримок, перекидати величезні масиви даних між основними сегментами мережі та серверами. Будь-які «вузькі місця» на цьому рівні можуть сповільнити роботу всього підприємства.

Центральним елементом будь-якої корпоративної мережі є сервери. Важко уявити сучасну IT-компанію без поштового сервера, серверів баз даних, файлових сховищ або систем резервного копіювання. Всі ці ресурси працюють у межах структури домену, що дозволяє адміністраторам централізовано керувати

правами кожного окремого співробітника. Це значно спрощує адміністрування: замість того, щоб налаштовувати кожен комп’ютер окремо, правила безпеки задаються один раз для всієї мережі. Більше того, використання доменних структур дозволяє впроваджувати єдині політики безпеки, що автоматично застосовуються до всіх робочих станцій, гарантуючи відповідність корпоративним стандартам.

Важливим аспектом, про який не можна забувати при описі мережі, є її топологія. Топологія − це «карта» [1] або схема того, як саме з’єднані між собою вузли мережі. Вона може бути фізичною (як прокладені кабелі) або логічною (як по них ідуть сигнали). Вибір топології − це фундамент проєктування, адже він визначає, наскільки швидко мережа працюватиме, скільки грошей піде на кабелі та наскільки легко буде додати нові робочі місця в майбутньому.

Хоча з розвитком технологій Ethernet багато старих підходів відійшли в минуле, їхні базові принципи залишаються актуальними й сьогодні, виступаючи базою для розуміння сучасних стандартів.

Шинна топологія − це «ветеран» мережевих технологій. Її концепція полягала в тому, що всі пристрої «висіли» на одному спільному кабелі, який називали магістраллю. Будь-який сигнал, що йшов по кабелю, бачили всі пристрої, але приймав його тільки адресат. Класичним прикладом такої мережі були старі системи 10BASE2. Незважаючи на невелику вартість та простоту в налаштуванні, «шина» мала величезний недолік: якщо кабель десь перебивали (або просто відходив контакт), «падала» абсолютно вся мережа компанії. Крім того, через те, що канал був один на всіх, при великій кількості комп’ютерів вони постійно «перебивали» один одного, створюючи колізії. Це вимагало використання спеціальних алгоритмів виявлення колізій (CSMA/CD), проте навіть вони не рятували від значного падіння швидкості.

Сьогодні шинна топологія майже не використовується в реальному житті, проте її принципи все ще активно вивчаються в середовищах на кшталт Cisco Packet Tracer для розуміння логіки роботи сегментів мережі.

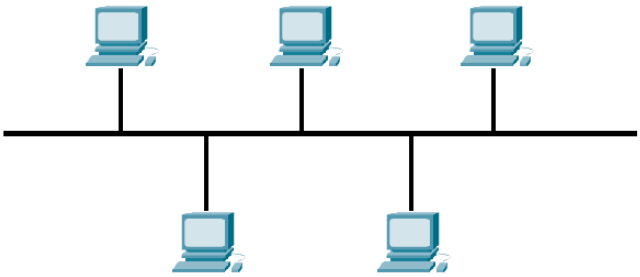

Рис. 1.1 – Топологія «Шина»

На зміну шині прийшла топологія зірка, яка на сьогодні є золотим стандартом. Тут все працює інакше: кожен пристрій підключений своїм власним, окремим кабелем до центрального пристрою − комутатора. Це кардинально змінило рівень надійності. Тепер, якщо хтось випадково пошкодить свій кабель або у когось зламається комп'ютер, це не вплине на роботу всього офісу. Комутатор працює як розумний диспетчер, направляючи дані саме тому, кому вони призначені, що усуває проблему колізій і дозволяє мережі працювати на великих швидкостях − від 100 Мбіт/с до 10 Гбіт/с. А також , таку мережу дуже легко розширювати: просто вставляєш кабель у вільний порт комутатора, і новий користувач уже в мережі. Це робить «зірку» ідеальним вибором для сучасних офісів, що постійно ростуть.

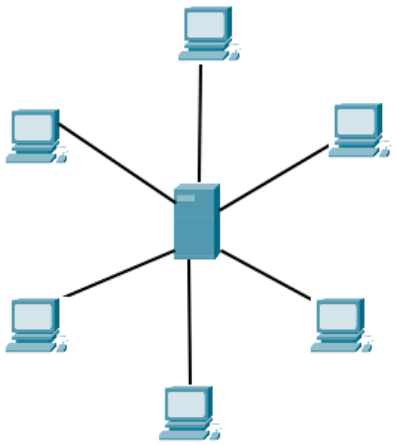

Рис. 1.2 – Топологія «Зірка»

Також варто згадати про кільцеву топологію, яка була досить популярною в минулому, особливо в мережах Token Ring. Тут пристрої з'єднувалися

послідовно один за одним, утворюючи замкнене кільце. Дані ходили по колу, передаючись від сусіда до сусіда, поки не досягали цілі. Щоб не було хаосу, використовувався спеціальний «токен» (маркер) – право на передачу даних мав лише той, хто тримає маркер в цей конкретний момент. Це дозволяло уникнути конфліктів у мережі, що було перевагою перед шиною. Головна слабкість кільця – повна залежність від кожного вузла. Вихід з ладу одного ПК або розрив будь-якої ділянки кабелю міг повністю паралізувати роботу всього сегмента. Хоча сьогодні ця топологія майже зникли з офісів, вона досі застосовується в промислових мережах та деяких операторських рішеннях, де критично важливо забезпечити стабільну передачу даних без затримок.

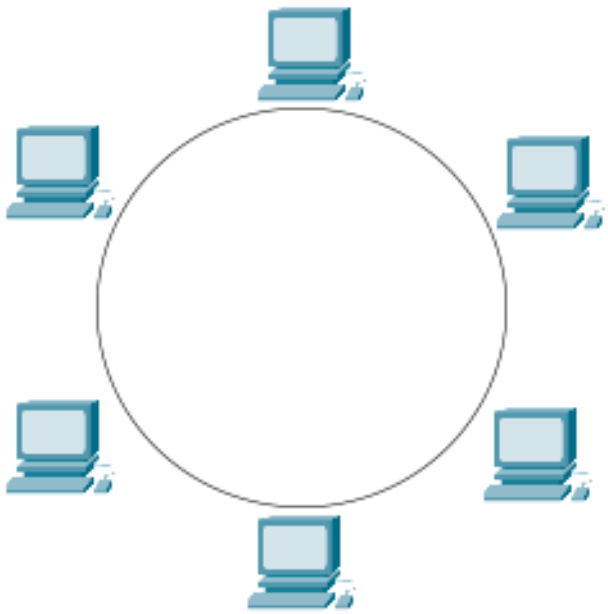

Рис. 1.3 – Топологія «Кільце»

Коли мова йде про максимальну надійність, наприклад, у дата-центрах або у великих провайдерів, використовується топологія сітка. У такій мережі кожен пристрій має декілька зв’язків з іншими вузлами. Це створює неймовірну кількість резервних шляхів. Навіть якщо кілька кабелів буде пошкоджено, протоколи маршрутизації автоматично знайдуть обхідний шлях і дані дійдуть до отримувача. Сітка може бути повною (всі з’єднані з усіма) або частковою, де

резервуються тільки найбільш завантажені напрямки. Звичайно, це дорого через велику кількість кабелів та портів, але для критичної інфраструктури, де кожна секунда простою коштує тисячі доларів, це єдине вірне рішення, що гарантує абсолютну відмовостійкість.

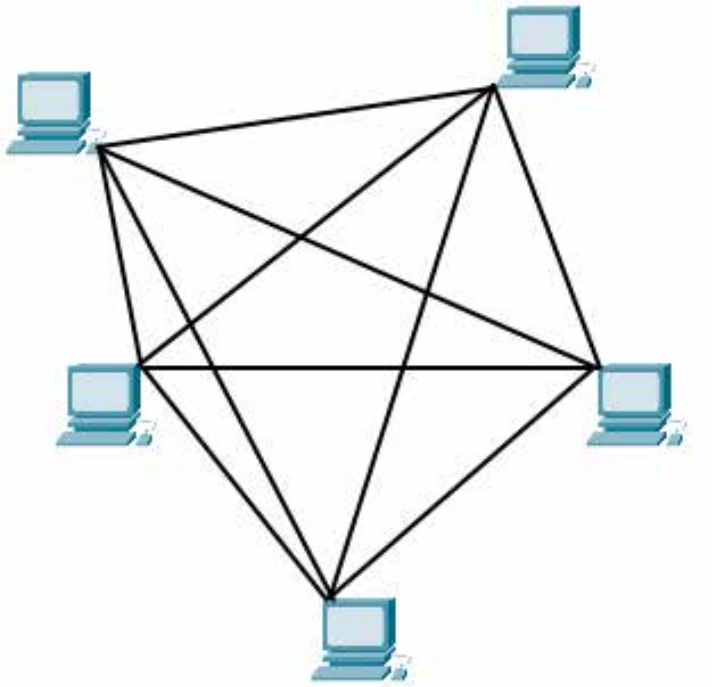

Рис. 1.4 – Топологія «Сітка»

Проте найбільш поширеною в корпоративному секторі є топологія дерево, яку часто називають ієрархічною зіркою. Фактично, це поєднання декількох топологій типу «зірка», які каскадно з'єднуються між собою. Вгорі стоїть головний комутатор (корінь дерева), від нього йдуть комутатори підрозділів, а вже до них − кінцеві пристрої. Це дозволяє ідеально структурувати мережу під потреби підприємства: наприклад, кожна гілка дерева − це окремий відділ або поверх. Така структура дуже гнучка і дозволяє легко додавати нові сегменти без втручання в уже працюючі частини. Окрім масштабованості, дерево дозволяє легко впроваджувати групові політики та контролювати трафік на кожному рівні ієрархії. Проте тут важливо приділяти увагу центральному вузлу, бо якщо «корінь» дерева вийде з ладу, значна частина компанії залишиться ізольованою.

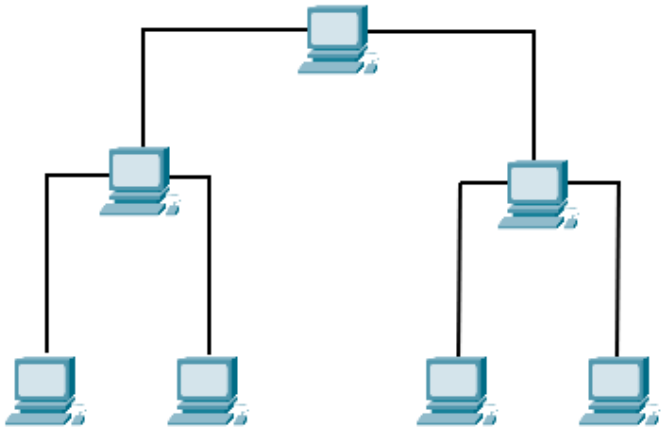

Рис. 1.5 – Топологія «Дерево»

На основі детального розгляду фізичних та логічних схем побудови мереж, у таблиці 1.1 наведено порівняльну характеристику всіх вищезгаданих топологій. Це дозволяє обґрунтувати вибір ієрархічної моделі як найбільш оптимальної для проєктованої інфраструктури.

Таблиця 1.1 – Порівняльна характеристика базових топологій мереж

Топологія	Переваги	Недоліки	Сфера застосування
Шина	Низька вартість кабелю	Обрив магістралі зупиняє всю мережу	Тимчасові або застарілі системи
Зірка	Відсутність колізій	Вихід з ладу вузла розриває мережу	Спеціалізовані промислові мережі
Кільце	Стійкість до поломок окремих вузлів	Залежність від центрального вузла	Рівень доступу в офісах
Сітка	Максимальна відмовостійкість	Дуже висока вартість та складність	Ядро мережі, дата-центри
Дерево	Ефективне керування, масштабованість	Потребує ретельного планування	Мережі IT-компаній (обрано в проєкті)

Сучасне проєктування мереж не обмежується лише фізикою кабелів та вибором топології. Сьогодні невід’ємною частиною архітектури є логічне розділення за допомогою технології VLAN. Вона дозволяє розбити одну велику фізичну мережу на декілька маленьких віртуальних зон. Це означає, що бухгалтери, розробники та маркетологи можуть працювати у власних ізольованих мережевих просторах, навіть якщо вони підключені до одного й того ж комутатора. Такий підхід суттєво підвищує рівень безпеки, адже користувач з одного VLAN не може просто так потрапити в інший без дозволу маршрутизатора. Крім того, це допомагає оптимізувати мережевий трафік, обмежуючи поширення широкомовних запитів, які часто стають причиною «забивання» каналів зв'язку.

Оскільки через корпоративну мережу проходить величезна кількість службової та конфіденційної інформації, захист даних стає пріоритетом номер один. Для цього використовуються потужні міжмережеві екрани, які фільтрують весь трафік на вході та виході, а також системи виявлення та запобігання атак (IDS/IPS). Додатково на рівні комутаторів впроваджується контроль доступу до портів, що не дозволяє сторонньому пристрою просто підключитися до мережі в офісі. Не менш важливим є питання стабільності та безперервності роботи. Щоб робота підприємства не зупинялася через дрібні поломки чи технічні збої, інженери використовують складні системи резервування. Це включає створення запасних шляхів передачі даних за допомогою протоколів STP (Spanning Tree Protocol) та дублювання найбільш критичного обладнання. У разі аварії система автоматично, за лічені секунди, переключається на резервний маршрут, що робить інфраструктуру практично невразливою до локальних несправностей.

Отже, сучасна комп'ютерна мережа [6] підприємства − це не просто набір заліза, а складна інженерна споруда, що поєднує в собі апаратну базу, інтелектуальні програмні алгоритми та чітко вивірені правила безпеки. Її головна мета − бути максимально ефективним, непомітним, але надійним інструментом, що забезпечує стабільну та безпечну життєдіяльність усього технологічного бізнесу в умовах постійно зростаючих цифрових загроз.

1.2. Особливості мереж IT-компаній

Дослідивши базову архітектуру корпоративних мереж у попередньому підрозділі, необхідно визнати, що IT-галузь диктує свої правила гри, які часто йдуть врозріз із загальноприйнятими стандартами для звичайних офісів. Проєктування інфраструктури для IT-компанії – це завжди пошук компромісу між максимальною відкритістю для інновацій та залізною дисципліною в питаннях безпеки. Мережа тут виступає не просто як середовище для передачі пакетів, а як складна екосистема, де кожен розробник, тестувальник чи системний адміністратор має свої специфічні запити до трафіку та доступності ресурсів. Головною відмінністю в даному контексті є екстремальна динамічність ресурсів. В IT-середовищі мережа майже ніколи не перебуває у стані спокою. Постійне розгортання нових мікросервісів, робота з контейнеризацією (Docker, Kubernetes) та необхідність миттєво створювати ізольовані сегменти для тестів перетворюють адміністрування на динамічний процес. Тут неможливо один раз налаштувати порти і забути про них на тривалий час; інженерам доводиться впроваджувати технології програмно-визначуваних мереж (SDN) або будувати дуже гнучку логіку VLAN, щоб мережева інфраструктура не ставала перешкодою для відділу розробки.

Особливе місце в роботі IT-підприємства займає продуктивність, яка сприймається не як бонус, а як життєва необхідність. Багато хто помилково вважає, що для роботи програміста достатньо будь-якого стабільного підключення, проте реальність інша: IT-компанія генерує специфічний, «важкий» трафік. Це зумовлено постійною синхронізацією з Git-репозиторіями, викачуванням об’ємних образів віртуальних машин та безперервною роботою CI/CD пайплайнів, які збирають та тестують код у реальному часі. Коли одночасно кілька команд ініціюють збірку великих проєктів, навантаження на магістральні канали зростає в геометричній прогресії. Саме тому в таких проєктах використання 10-гігабітних магістралей у ядрі мережі є фактично

галузевим стандартом, що дозволяє уникнути деградації швидкості, яка для фахівця є синонімом вимушеного простою в роботі.

Ще однією рисою, яку неможливо оминути, є відмова від суто локальної моделі на користь гібридної природи та глибокої хмарної залежності. Сучасна IT-компанія − це майже завжди поєднання власних серверів (On-premise) та левової частки сервісів, що «живуть» у хмарах типу AWS або Azure. У такому сценарії інтернет-канал стає критично важливою артерією, без якої компанія просто не зможе функціонувати. Це накладає особливі вимоги на прикордонне обладнання, зокрема на R1-EDGE, який ми будемо розглядати далі. Резервування каналів зв'язку від різних провайдерів та налаштування автоматичного перемикання (Failover) стають не просто додатковою опцією, а обов'язковою умовою виживання бізнесу.

Питання безпеки в таких умовах вимагає філігранного балансу між максимальною захищеністю та зручністю використання мережі. Оскільки головним капіталом компанії є її код та інтелектуальна власність, питання захисту стоїть надзвичайно гостро. Проте розробникам потрібна певна свобода для налаштування сервісів, що часто конфліктує з жорсткими вимогами відділів безпеки. Виходом стає впровадження глибокої мікросегментації. Ми ділимо мережу не просто на «офіс» і «сервери», а створюємо окремі рівні доступу для різних груп користувачів, що детально відображено в розділі 2 при описі безпеки 2-го рівня та конфігурації Firewall. Кожен сегмент має бути ізольований настільки, щоб навіть у разі зламу окремого робочого місця, потенційний зловмисник уперся в логічний бар'єр і не зміг розвинути атаку на критичні вузли системи.

В епоху панування розподілених команд використання VPN стає стандартом де-факто. Оскільки команди можуть бути розкидані по різних країнах, а віддалена робота стала нормою, мережа більше не обмежена фізичними стінами офісу − її периметр розмивається. Співробітник у кав'ярні або вдома має бути таким же захищеним учасником мережі, як і той, хто знаходиться безпосередньо в центрі розробки. Це змушує інженерів приділяти

величезну увагу побудові VPN-шлюзів на базі Cisco ASA або подібних рішень, які здатні витримувати сотні одночасних зашифрованих сесій без відчутної втрати пропускної здатності.

Паралельно з цим в IT-компаніях формується особлива культура моніторингу та автоматизації. В розгалужених мережах ручне керування неминуче призводить до помилок, які стають головною причиною збоїв. Тому критично важливим є тотальний моніторинг кожного порта та кожної служби в реальному часі. Використання систем збору логів та візуалізації стану мережі дозволяє інженерам діяти превентивно. Автоматизація розгортання конфігурацій, яку ми частково реалізуємо через скрипти в додатках, допомагає підтримувати ідеальний порядок у мережі, навіть коли кількість вузлів перевалить за кілька сотень.

Нарешті, не варто забувати про пріоритезацію трафіку через механізми Quality of Service (QoS). IT-компанії − це простір постійних мітингів, дейлі нарад та презентацій проєктів замовникам. Якщо в момент важливого відеодзвінка сервер почне викачувати терабайтне оновлення бази даних і «заб'є» канал, це може мати негативні наслідки для репутації компанії. Тому налаштування черг трафіку є пріоритетним завданням: голос і відео завжди повинні мати «зелений коридор», незалежно від ступеня завантаженості каналів іншими процесами. Підбиваючи підсумок, особливості мережі IT-компанії − це поєднання високої швидкості, адаптивності та безкомпромісного захисту. Саме ці фактори стали фундаментом для розробки логічної структури в розділі 3 та подальшої реалізації проєкту в середовищі Cisco Packet Tracer, де мережа має залишатися непомітною для користувача, але бути нездоланною фортецею для зовнішніх загроз.

1.3. Основні мережеві протоколи та стандарти

Функціонування будь-якої мережевої інфраструктури, особливо в межах високотехнологічної IT-компанії, неможливе без чітко регламентованих правил взаємодії пристроїв. Стандартизовані мережеві протоколи та технології − це

саме ті «закони», що регулюють методи передачі даних між різними вузлами, незалежно від їхнього апаратного забезпечення чи операційних систем. Завдяки цій стандартизації ми отримуємо універсальну основу: сервери та клієнтські станції здатні взаємодіяти узгоджено, навіть якщо вони вироблені різними вендорами або використовують кардинально різне програмне забезпечення. Для IT-сектору точне налаштування цих протоколів є критичним завданням, оскільки надійність внутрішніх сервісів, безперебійний доступ до зовнішніх ресурсів та швидкість співпраці між розробниками напряму залежать від коректності мережевих алгоритмів.

Варто наголосити, що реалізація мережевих протоколів ніколи не відбувається ізольовано. Вона базується на складних ієрархічних моделях взаємодії, серед яких галузевим стандартом де-факто стала модель TCP/IP. Саме вона лежить в основі сучасного Інтернету та локальних корпоративних систем. Модель TCP/IP розділяє весь процес передачі інформації на кілька функціональних рівнів, що дозволяє спростити проєктування та подальше обслуговування мережі. Такий модульний підхід дає системним адміністраторам можливість локалізувати несправності на конкретному етапі передачі даних, не перевіряючи всю систему в цілому.

Прикладний рівень цієї моделі забезпечує безпосередню взаємодію користувацького софту з мережевими ресурсами. Саме тут розташовані протоколи, без яких щоденна робота IT-фахівців була б неможливою. Якщо раніше достатньо було використання стандартних HTTP чи FTP для передачі файлів та веб-сторінок, то сьогодні на перший план виходять їхні захищені версії. Наприклад, протокол HTTPS, що використовує шифрування TLS, став обов’язковим стандартом для захисту конфіденційної інформації та вихідного коду, що передається через мережу. Протокол SMTP, своєю чергою, продовжує залишатися фундаментом для електронної пошти, проте в сучасних умовах він також вимагає додаткових налаштувань безпеки для запобігання витоку корпоративних даних.

Транспортний рівень відповідає за безпосередню доставку даних між кінцевими вузлами, і тут ми маємо справу з двома ключовими «гравцями» – TCP та UDP. Протокол TCP є незамінним для задач, де цілісність даних стоїть на першому місці. Завдяки складним механізмам встановлення з'єднання (так зване «тристороннє рукостискання»), контролю цілісності та повторній передачі пакетів у разі їх втрати, TCP забезпечує надійну роботу систем контролю версій, баз даних та веб-сервісів. З іншого боку, протокол UDP, хоч і не гарантує доставку кожного біта, має мінімальні накладні витрати. Це робить його ідеальним вибором для сервісів реального часу, таких як відеоконференції або IP-телефонія, де невелика втрата пакетів є менш критичною, ніж затримка звуку чи картинки.

Мережевий рівень реалізується через протокол IP, який виконує функції глобальної адресації та маршрутизації. Кожен пристрій у структурі отримує свою унікальну адресу, що дозволяє ідентифікувати його серед мільйонів інших вузлів. Сьогодні ми спостерігаємо поступовий, але неминучий перехід від IPv4 до IPv6. Для IT-компаній, що оперують сотнями віртуальних машин, серверів та контейнерів, розширений адресний простір IPv6 стає порятунком від дефіциту адрес та складнощів із NAT. Це дозволяє будувати більш прозорі та масштабовані мережеві архітектури.

На канальному рівні надзвичайно важливою технологією є VLAN (Virtual Local Area Network), яка дозволяє здійснювати логічну сегментацію. У звичайній мережі всі пристрої знаходяться в одному широкомовному домені, що призводить до «засмічення» каналів службовим трафіком та створює ризики безпеки. Використання VLAN дозволяє нам розрізати фізичну мережу на ізольовані сегменти. Для IT-підприємства це можливість відокремити, наприклад, сегмент розробки від бухгалтерської мережі чи гостьового Wi-Fi. Окрім безпеки, це значно оптимізує трафік: широкомовні пакети не виходять за межі свого сегмента, що зменшує навантаження на комутаційне обладнання. Гнучкість VLAN також дозволяє змінювати структуру відділів без необхідності фізичного перемикання кабелів у патч-панелях.

Для кращого розуміння взаємодії апаратних засобів та програмних протоколів у межах обраної архітектури, у таблиці 1.2 систематизовано функціональні ролі обладнання з прив’язкою до рівнів мережевої моделі.

Таблиця 1.2 – Розподіл функцій та протоколів за рівнями мережевої моделі

Рівень моделі OSI/TCP-IP	Обладнання	Протоколи та технології	Роль у даному проєкті
Прикладний	Сервери (DNS, DHCP, Web)	HTTP, DNS, DHCP, SSH	Надання мережевих сервісів користувачам
Транспортний	Кінцеві станції, Firewall	TCP, UDP	Забезпечення надійності передачі даних
Мережевий	Маршрутизатор (R1), L3-Switch	IP, OSPF, ICMP, ACL	Міжвланова маршрутизація та безпека периметра
Канальний	Комутатори (L2-Switch)	Ethernet, VLAN (802.1Q), STP	Комутація всередині відділів, ізоляція трафіку
Фізичний	Кабельна система, Wi-Fi AP	IEEE 802.3, 802.11	Фізичне середовище передачі сигналів

Автоматизація налаштувань робочих станцій забезпечується протоколом DHCP. В динамічному IT-середовищі, де співробітники постійно підключають нові ноутбуки, тестові гаджети або розгортають тимчасові віртуальні сервери, ручне призначення IP-адрес перетворилося б на адміністративне пекло. DHCP автоматично конфігурує всі необхідні параметри: від самої адреси до маски підмережі та адреси шлюзу. Це не лише економить час, а й нівелює ризик

виникнення конфліктів IP-адрес, які часто стають причиною важкодіагностованих збоїв у мережі.

Для зручності користування ресурсами використовується протокол DNS. Він перетворює цифрові IP-адреси на зрозумілі людині доменні імена. У внутрішній мережі IT-компанії DNS відіграє роль навігатора: замість того, щоб запам’ятовувати адресу сервера з базою даних, розробник просто звертається до нього за логічним іменем. Окрім зручності, DNS дозволяє реалізувати механізми балансування навантаження: одне ім’я може вказувати на кілька серверів, що підвищує відмовостійкість всієї системи.

Коли мережа виходить за межі одного сегмента, в гру вступають протоколи маршрутизації. Для невеликих мереж може бути достатньо статичних маршрутів, проте складні структури IT-компаній вимагають динамічного підходу. Протоколи на кшталт OSPF автоматично аналізують топологію мережі, знаходять найкоротші шляхи для передачі пакетів і миттєво реагують на вихід з ладу будь-якого вузла, переспрямовуючи трафік в обхід. Це гарантує безперервність бізнес-процесів навіть у разі локальних аварій на лініях зв’язку.

Завершальним, але не менш важливим елементом є технології безпеки та шифрування. Передача даних у відкритому вигляді сьогодні — це неприпустимий ризик. Технології TLS, IPsec та побудова VPN-тунелів забезпечують захист інформації на всьому її шляху. У поєднанні з сучасними методами автентифікації та системами автоматизованого управління конфігураціями, ці протоколи формують цілісну, безпечну та масштабовану інфраструктуру. Саме такий комплексний підхід до використання TCP/IP, VLAN, DHCP та DNS дозволяє створити мережу, яка не просто працює, а є надійним фундаментом для розвитку сучасного IT-бізнесу.

Висновки до розділу 1

У першому розділі ми провели всебічний аналіз сучасного стану та тенденцій розвитку мережевих технологій у контексті забезпечення потреб IT-

підприємств. Нами було встановлено, що ключовими факторами при проєктуванні інфраструктури є не лише висока швидкість передачі даних, а й відмовостійкість та адаптивність до динамічних змін бізнес-процесів. Дослідили специфіку функціонування корпоративних систем, що працюють з великими обсягами конфіденційної інформації, та визначено пріоритетні напрями захисту даних. На основі проведеного аналізу обґрунтовано вибір ієрархічної моделі побудови мережі, яка дозволяє розділити функції комутації, агрегації та ядра, що є критично важливим для забезпечення масштабованості системи без втрати продуктивності. Сформований нами перелік технічних вимог став базисом для подальшого проєктування логічної та фізичної структур мережі.

РОЗДІЛ 2. БЕЗПЕКА КОРПОРАТИВНИХ МЕРЕЖ

2.1. Безпека 2-го рівня та безпека Wlan

Стійкість другого рівня моделі OSI та комплексний захист бездротових мереж WLAN є критичними точками опору в сучасній ієрархічній мережі. Саме на канальному рівні відбувається первинна комутація кадрів та регулювання доступу до фізичного носія, що робить цей ступінь «фундаментом» безпеки. Якщо зловмисник зможе скомпрометувати рівень L2, усі подальші заходи захисту на вищих рівнях (маршрутизація, файрволи) можуть виявитися марними. Канальний рівень відповідає за фізичну адресацію через MAC-адреси та виявлення помилок, проте він за своєю природою є вразливим до специфічних маніпуляцій, таких як підміна ідентифікаторів, ARP-спуфінг та спроби несанкціонованого виходу за межі віртуальних сегментів VLAN. Ситуація додатково ускладнюється у бездротових сегментах, де «фізичним кабелем» виступає радіоефір, відкритий для будь-якого пристрою в зоні покриття.

На канальному рівні управління доступом до середовища базується на протоколах CSMA/CD для дротового Ethernet та CSMA/CA для Wi-Fi. Ці алгоритми запобігають хаосу в ефірі, визначаючи черговість передачі даних. Проте, незважаючи на впорядкованість, базові механізми фільтрації MAC-адрес сьогодні вже не можуть вважатися надійним бар’єром. Оскільки MAC-адресу легко підробити програмними методами, зловмисник може без зусиль видати себе за легітимний пристрій. Для протидії таким загрозам в професійному середовищі недостатньо простого «білого списку»; необхідно впроваджувати динамічну автентифікацію за стандартом 802.1X, використовувати RADIUS-сервери та здійснювати постійний моніторинг таблиць комутації для виявлення підозрілих змін.

Особливо небезпечними є атаки на протокол розрізнення адрес – ARP. Оскільки ARP за замовчуванням довіряє всім відповідям у мережі, зловмисник може надіслати хибне повідомлення, змусивши пристрої вважати його комп’ютер шлюзом за замовчуванням. Це дозволяє реалізувати атаку типу Man-

in-the-Middle (MITM) − перехоплення всього трафіку. Для захисту від подібних маніпуляцій ми використовуємо функцію DHCP Snooping у поєднанні з Dynamic ARP Inspection (DAI). Ці механізми перевіряють легітимність ARP-пакетів на портах комутатора, відсікаючи будь-які спроби отруєння ARP-кешу.

Логічна сегментація через VLAN, яку ми розглядали раніше, також потребує додаткового захисту. Існує ризик атак типу VLAN-хопінг, коли через маніпуляції з тегами 802.1Q зловмисник намагається «перестрибнути» з одного віртуального сегмента в інший. Щоб унеможливити такий сценарій, ми обов'язково відключаємо протокол DTP (Dynamic Trunking Protocol) на клієнтських портах та жорстко фіксуємо режими доступу. Це гарантує, що трафік між відділами буде проходити виключно через контрольовані маршрутизатори або міжмережеві екрани.

Бездротова частина мережі (WLAN) через свою публічну природу є ще більш вразливою до DoS-атак та спроб перехоплення. Застарілі протоколи шифрування, як-от WEP чи перші версії WPA, сьогодні є легким здобутком для хакерів. Сучасним стандартом є WPA2-AES, а в ідеалі − WPA3, який забезпечує стійкість навіть до атак методом перебору паролів. Окрім шифрування, в корпоративному секторі обов'язковим є використання корпоративного режиму (WPA-Enterprise), де кожен користувач автентифікується під власними обліковими даними, а не за спільним паролем.

Для практичної перевірки цих концепцій ми використали середовище Cisco Packet Tracer, де була змодельована типова мережа з комутатором та кінцевими вузлами (див. Рис. 1.1).

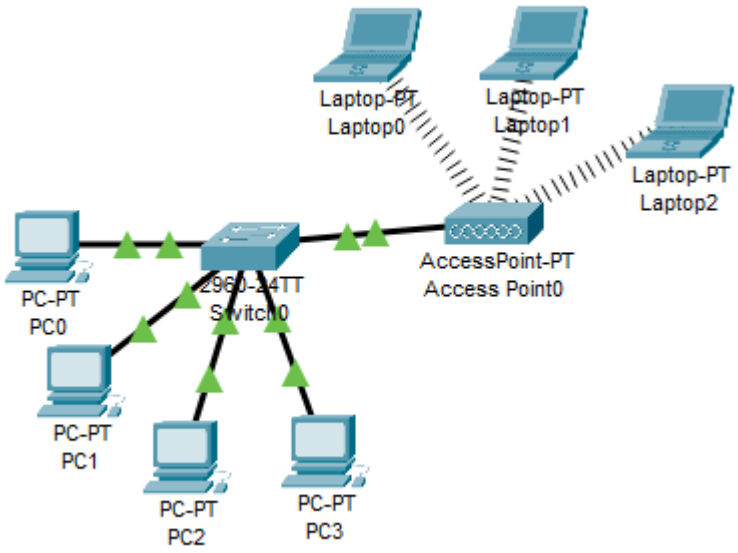

Рис. 2.1 – Базова топологія мережі для налаштування безпеки

Основним завданням було впровадження технології Port Security для запобігання підключенню стороннього обладнання до фізичних портів комутатора. Процес налаштування передбачає переведення порту в режим доступу, прив’язку до відповідного VLAN та активацію захисту з обмеженням кількості дозволених MAC-адрес (див. Рис. 1.2).

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name Office
Switch(config-vlan)#exit
Switch(config)#interface range fa0/1 - 5
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#exit
Switch(config)#interface range fa0/1 - 5
Switch(config-if-range)#switchport port-security
Switch(config-if-range)#switchport port-security maximum 2
Switch(config-if-range)#switchport port-security violation shutdown
Switch(config-if-range)#switchport port-security mac-address sticky
Switch(config-if-range)#exit
Switch(config)#
```

Рис. 2.2 – Конфігурування параметрів Port Security на комутаторі Cisco

Важливим моментом є вибір реакції комутатора на порушення політики безпеки. В нашому випадку було обрано режим shutdown, який миттєво вимикає порт при спробі підключення невідомого пристрою. Ефективність цього

налаштування наочно демонструє перевірка лімітів MAC-адрес: при перевищенні заданої кількості (наприклад, більше двох адрес на порт) система автоматично блокує інтерфейс, що відображено у звіті системи (див. Рис. 1.3).

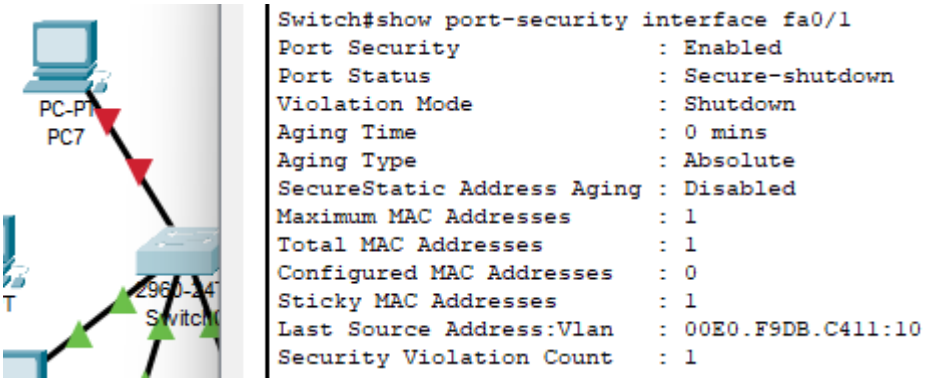

Рис. 2.3 – Результат спрацювання захисту при порушенні ліміту адрес

Аналогічний підхід застосовано і для бездротового сегмента. У середовищі моделювання було налаштовано точку доступу (Access Point) з використанням алгоритму шифрування WPA2-PSK (Pre-Shared Key). Це дозволяє імітувати захищене середовище, де доступ отримують лише авторизовані клієнти, що володіють коректним ключем доступу (див. Рис. 1.4).

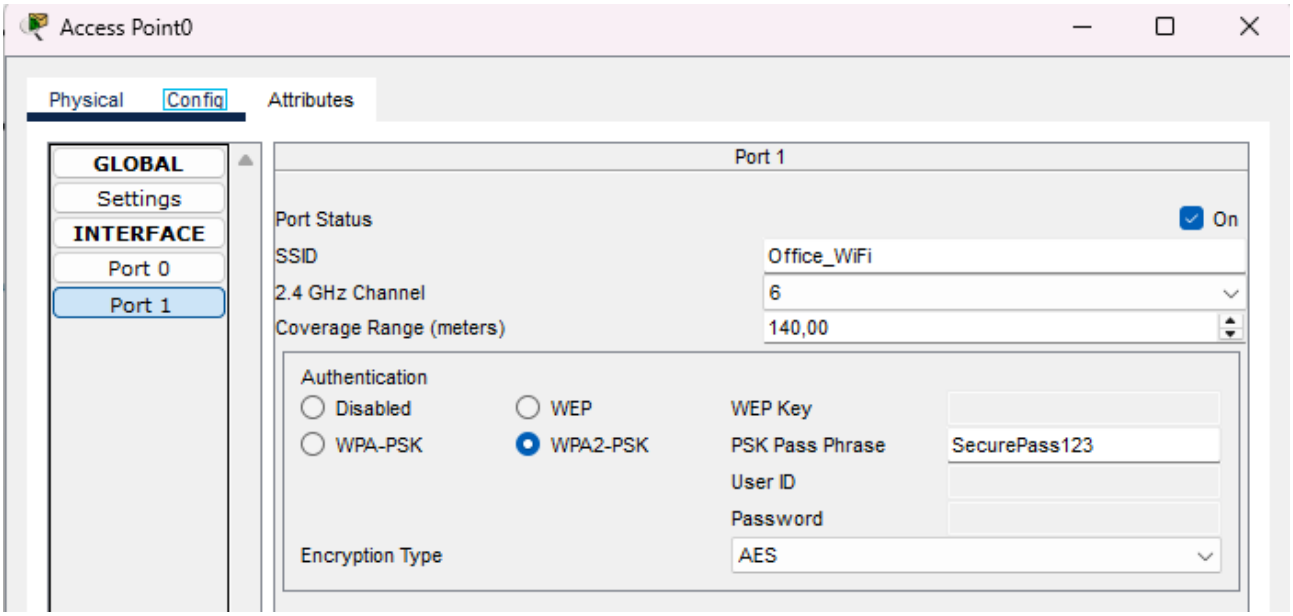

Рис. 2.4 – Параметри безпеки бездротової точки доступу

Загалом, захист другого рівня та WLAN − це не разове налаштування, а постійний процес. Він поєднує в собі фізичне обмеження доступу до портів, логічну ізоляцію через VLAN, сучасне шифрування радіоканалу та регулярний моніторинг аномалій. Такий комплексний підхід, підкріплений результатами моделювання, дозволяє створити стійку інфраструктуру, здатну протистояти більшості атак на початковому етапі передачі даних. Тільки забезпечивши «чистоту» на канальному рівні, ми можемо впевнено переходити до захисту мережевого рівня та налаштування міжмережевих екранів.

2.2. Безпека мережевого рівня

Забезпечення захисту на мережевому рівні моделі OSI (L3) є фундаментом побудови корпоративної інфраструктури, оскільки саме тут реалізується логіка взаємодії між ізольованими сегментами мережі IT-компанії. Якщо заходи захисту на рівні L2 спрямовані на запобігання атакам всередині локальних комутованих середовищ, то безпека мережевого рівня фокусується на контролі міжсегментних потоків даних, захисті процесів маршрутизації та організації безпечних каналів зв’язку через публічні мережі. У межах даної дипломної роботи мережевий рівень розглядається як основний ешелон фільтрації трафіку, де відбувається чітке розмежування доступу між адміністративним персоналом, відділами розробки та критичною серверною інфраструктурою.

Центральним інструментом реалізації політики безпеки на цьому етапі є впровадження розширених списків контролю доступу (Extended Access Control Lists). Використання ACL на інтерфейсах маршрутизаторів дозволяє здійснювати глибоку інспекцію пакетів, аналізуючи не лише IP-адреси відправника та отримувача, а й типи протоколів та конкретні номери портів транспортного рівня (TCP/UDP). Для IT-компанії це дає можливість втілити концепцію «мінімальних привілеїв»: за замовчуванням будь-який трафік забороняється (implicit deny), а дозволяються лише ті з’єднання, що є критично необхідними для виконання службових обов’язків. Наприклад, доступ розробників до виробничих баз даних

обмежується лише специфічними портами, що унеможливлює спроби сканування мережі або використання незахищених методів передачі даних. Розміщення таких фільтрів якомога ближче до джерела трафіку дозволяє суттєво економити ресурси центральних вузлів та запобігати поширенню паразитних пакетів по всій інфраструктурі (див. Рис. 2.1).

```
Router(config)#ip access-list extended SECURE_SERVER
Router(config-ext-nacl)#permit tcp 192.168.20.0 0.0.0.255 host 192.168.30.100 eq 80
Router(config-ext-nacl)#deny icmp 192.168.20.0 0.0.0.255 host 192.168.30.100
Router(config-ext-nacl)#permit ip any any
Router(config-ext-nacl)#exit
Router(config)#int g0/0.20
Router(config-subif)#ip access-group SECURE_SERVER in
```

Рис 2.1 – Схема обмеження доступу за допомогою списків ACL

Критично важливим аспектом є захист самої логіки обміну маршрутною інформацією. У динамічних середовищах, де функціонує протокол OSPF, існує ризик впровадження нелегітимного пристрою, який може підмінити таблиці маршрутизації та спрямувати потік даних через вузол зловмисника (атака Man-in-the-Middle). Для запобігання подібним сценаріям у проєкті реалізовано механізми суворої автентифікації між сусідніми маршрутизаторами. Використання криптографічного хешування (MD5/SHA) гарантує, що пристрій прийматиме оновлення лише від довірених вузлів, які володіють спільним секретним ключем. Додатково, для мінімізації площі атаки, на всіх інтерфейсах, що з'єднуються з клієнтськими робочими станціями, активовано режим пасивних інтерфейсів (passive-interface). Це блокує надсилання службових пакетів OSPF у користувацькі сегменти, де вони можуть бути використані для розвідки топології мережі (див. Рис. 2.2).

```
GW-Main(config)#int g0/0.10
GW-Main(config-subif)#ip ospf message-digest-key 1 md5 Secur3_P@ss
GW-Main(config-subif)#exit
GW-Main(config)#router ospf 1
GW-Main(config-router)#area 0 authentication message-digest
GW-Main(config-router)#exit
```

Рис 2.2 – Налаштування автентифікації протоколу OSPF та пасивних інтерфейсів

Паралельно з фільтрацією користувацького трафіку, особлива увага приділяється захисту керуючої площини (Control Plane) мережевого обладнання. Оскільки маршрутизатор є інтелектуальним ядром мережі, його перевантаження надмірною кількістю запитів (наприклад, під час DoS-атаки) може призвести до паралічу всієї компанії. Впровадження технологій обмеження швидкості (Rate Limiting) для трафіку, спрямованого безпосередньо на процесор пристрою, дозволяє зберегти працездатність маршрутизатора навіть у критичних умовах. Це досягається шляхом виділення пріоритетних черг для системних пакетів та жорсткого лімітування протоколів діагностики, таких як ICMP. Таким чином, зовнішні атаки або масоване сканування не зможуть вивести з ладу механізми управління мережею.

Не менш важливим елементом безпеки L3 є організація захищеного віддаленого доступу для розподілених офісів. Оскільки передача корпоративних даних через публічний Інтернет несе високі ризики перехоплення, у проєкті реалізовано технологію IPsec VPN. Використання тунелювання в поєднанні зі стійким шифруванням AES (Advanced Encryption Standard) та перевіркою цілісності даних дозволяє створити захищений віртуальний канал поверх відкритої мережі. Це гарантує конфіденційність програмного коду та персональних даних при їх передачі між локальним офісом та хмарними інстансами. Робота IPsec на мережевому рівні робить процес захисту прозорим для кінцевих програм, забезпечуючи надійну інкапсуляцію кожного пакета.

На завершення, безпека на рівні L3 посилюється механізмами суворого контролю адміністративного доступу. Використання застарілих протоколів, таких як Telnet, у сучасних IT-компаніях є неприпустимим через передачу паролів у відкритому вигляді. Тому в межах проєкту налаштовується виключно протокол SSH (Secure Shell) з автентифікацією за ключами або складними паролями (див. Рис. 2.3). Додатково впроваджується логування подій через протокол Syslog, що дозволяє адміністратору не лише вчасно реагувати на інциденти, а й проводити ретроспективний аналіз спроб несанкціонованого

втручання. Такий комплексний підхід створює надійну базу для наступного етапу захисту – міжмережевого екранування прикладних сервісів.

```
Router(config)#hostname GW-Main
GW-Main(config)#ip domain-name it-company.ua
GW-Main(config)#crypto key generate rsa
The name for the keys will be: GW-Main.it-company.ua
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

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

GW-Main(config)#username admin privilege 15 secret Pa$$w0rd
*Mar 1 0:4:33.473: %SSH-5-ENABLED: SSH 1.99 has been enabled
GW-Main(config)#line vty 0 4
GW-Main(config-line)#transport input ssh
GW-Main(config-line)#login local
GW-Main(config-line)#exit
```

Рис 2.3 – Конфігурація протоколу SSH для безпечного віддаленого керування

2.3. Міжмережеві екрани (Firewall)

Коли мова заходить про захист периметра сучасної IT-компанії, саме міжмережеві екрани (ME) стають тим центральним вузлом, де замикається вся стратегія безпеки. На відміну від звичайних маршрутизаторів, які просто порівнюють заголовки пакетів зі статичними списками, сучасний Firewall працює значно глибше. Він використовує технологію інспекції з контролем стану (Stateful Packet Inspection). На практиці це означає, що пристрій не просто фільтрує окремі пакети, він «розуміє» контекст і життєвий цикл кожної мережевої сесії. Система відстежує стан TCP-з'єднань (від запиту SYN до фінального ACK) і веде динамічну таблицю станів. Якщо з інтернету приходить пакет, який не був ініційований зсередини або не відповідає логіці встановленого сеансу, система його негайно знищує. Це надійно захищає інфраструктуру від спроб зловмисників обійти фільтри через підробку прапорців або ін'єкцію нелегітимних пакетів у потік даних.

В основі нашого проєкту лежить концепція логічного зонування та ієрархії рівнів безпеки (Security Levels). Це фундаментальний підхід, де кожному

інтерфейсу пристрою присвоюється цифровий пріоритет від 0 до 100. Ми розділили інфраструктуру компанії на три стратегічні зони. Перша − Inside (наша внутрішня мережа), де працюють розробники, тестувальники та зберігаються критичні вихідні коди; вона має найвищий рівень довіри (100). Друга − Outside, тобто зовнішній, абсолютно некерований світ публічного інтернету з нульовою довірою. І третя, яка є критично важливою для публічних сервісів компанії − DMZ або демілітаризована зона (рівень довіри 50).

Саме в DMZ ми виносимо веб-сервери та поштові шлюзи, які мають бути доступні клієнтам із зовнішнього світу. Проте тут є важливий нюанс: ми надійно ізолюємо DMZ від внутрішнього ядра мережі. Така конфігурація реалізує принцип ешелонованої оборони. Навіть у найгіршому сценарії, якщо хакер зламає сервер у демілітаризованій зоні, міжмережевий екран FW1 заблокує будь-які його спроби «промацати» внутрішню мережу Inside. Це створює свого роду карантинну зону, яка рятує компанію від масштабного витоку даних (див. Рис. 2.4).

```
ciscoasa(config)#interface GigabitEthernet 1/1
ciscoasa(config-if)#nameif outside
INFO: Security level for "outside" set to 0 by default.
ciscoasa(config-if)#security-level 0
ciscoasa(config-if)#ip address 203.0.113.2 255.255.255.0
ciscoasa(config-if)#no shutdown

%LINK-5-CHANGED: Interface GigabitEthernet1/1, changed state to down
ciscoasa(config-if)#exit
ciscoasa(config)#interface GigabitEthernet 1/2
ciscoasa(config-if)#nameif inside
INFO: Security level for "inside" set to 100 by default.
ciscoasa(config-if)#security-level 100
ciscoasa(config-if)#ip address 192.168.1.1 255.255.255.0
ciscoasa(config-if)#no shutdown

ciscoasa(config-if)#exit
ciscoasa(config)#
```

Рис. 2.4 – Логічне зонування інтерфейсів та ієрархія рівнів безпеки на FW1

Окрім простого розділення сегментів, наш Firewall виконує складну інтелектуальну роботу − глибоку інспекцію прикладних протоколів (Application Inspection). Система фактично «вдивляється» всередину трафіку на рівні L7, щоб відрізнити звичайні HTTP-запити від спроб просунути шкідливий код або SQL-

ін’єкцію. Більше того, для таких протоколів як FTP, SIP або H.323, які постійно потребують відкриття нових динамічних портів для передачі даних, ME діє максимально гнучко. Він відкриває потрібний «технічний» порт лише на ті мілісекунди, що необхідні для конкретної передачі, і одразу його закриває. Це радикально звужує поверхню атаки, не залишаючи зловмисникам жодних «відчинених дверей» чи стаціонарних дірок у захисті нашої інфраструктури.

Важливим кроком у приховуванні топології мережі є використання механізмів трансляції адрес (NAT та PAT). Оскільки в нашому офісі сотні пристроїв мають приватні IP-адреси (RFC 1918), ми приховуємо їх за однією або кількома публічними адресами пристрою захисту. Тут ми робимо ставку на PAT (Port Address Translation), що дозволяє всій компанії виходити в інтернет через одну IP-адресу, розрізняючи сесії за номерами портів. Для зовнішнього спостерігача внутрішня структура компанії залишається «чорною скринькою». Зловмисник не може ініціювати пряме з’єднання з робочою станцією програміста, бо вона просто не має маршрутизації в глобальному просторі. Для серверів у зоні DMZ ми налаштовуємо статичний NAT, забезпечуючи точковий доступ до веб-ресурсів лише за суворо визначеними портами, такими як 80 (HTTP) або 443 (HTTPS) (див. Рис. 2.5).

```
ciscoasa(config)#object network INTERNAL_LAN
ciscoasa(config-network-object)#subnet 192.168.1.0 255.255.255.0
ciscoasa(config-network-object)#nat (inside,outside) dynamic interface
ciscoasa(config-network-object)#exit
```

Рис. 2.5 – Налаштування трансляції адрес NAT/PAT для маскування внутрішніх вузлів

Не можна оминути і питання безпеки віддалених команд. У нашому проєкті Firewall функціонує як потужний VPN-концентратор. Використовуючи сучасні алгоритми шифрування (AES-256), ми будуємо захищені тунелі для співробітників, які працюють з дому або з інших міст. Це дає впевненість, що навіть якщо розробник підключається через сумнівний Wi-Fi у кафе, його трафік із вихідним кодом проєкту залишиться зашифрованим і недоступним для перехоплення.

Завершує цю архітектуру об’єктно-орієнтоване управління. Ми не пишемо сотні хаотичних правил для кожної IP-адреси. Замість цього ми створюємо логічні групи об’єктів (наприклад, «Developers_Network» або «Prod_Servers»). Це робить конфігурацію зрозумілою для людини та зводить до мінімуму ризик фатальної помилки через людський фактор при внесенні змін. У поєднанні з деталізацією подій через Syslog-сервер, ми отримуємо «зір» над усією мережею. Будь-яке аномальне сканування портів або сплеск UDP-трафіку (що може свідчити про початок DDoS-атаки) миттєво фіксується, дозволяючи інженерам вчасно зреагувати та зберегти працездатність бізнес-сервісів. Таким чином, Firewall у нашій мережі перетворюється з пасивного фільтра на активний інтелектуальний щит, що гарантує цілісність усіх цифрових активів підприємства.

Висновки до розділу 2

У другому розділі нами було здійснено ґрунтовний теоретичний огляд технологічних рішень, що використовуються для розгортання сучасних локальних мереж. Особливу увагу ми приділили технології VLAN як основному засобу логічної сегментації, що дозволяє оптимізувати використання мережевих ресурсів та ізолювати широкомовний трафік. Було проаналізовано принципи функціонування протоколів динамічної конфігурації вузлів (DHCP) та систем доменних імен (DNS), які забезпечують автоматизацію адміністрування та зручність користувацького доступу до ресурсів. У межах дослідження безпекових аспектів ми розглянули механізми міжмережевого екранування та багаторівневої фільтрації трафіку через списки контролю доступу (ACL). Отримані теоретичні відомості підтвердили, що лише інтеграція автоматизованих служб разом із суворими політиками безпеки на різних рівнях моделі OSI здатна забезпечити стабільне функціонування корпоративної мережі в умовах сучасних кіберзагроз.

РОЗДІЛ 3. ПРОЄКТУВАННЯ МЕРЕЖІ ІТ-КОМПАНІЇ

3.1. Загальна характеристика ІТ-компанії

В межах даного дипломного проєкту було розглянуто модель сучасної ІТ-компанії середнього масштабу. Основним вектором її діяльності є повний цикл розробки програмного забезпечення − від написання коду до супроводу складних інформаційних систем та надання хмарних сервісів. Робота в такому динамічному середовищі висуває специфічні вимоги до комп'ютерної мережі: вона має бути не просто каналом передачі даних, а гнучким інструментом, що підлаштовується під потреби різних команд.

Організаційна структура підприємства побудована за функціональним принципом. Це означає, що кожен підрозділ має свої унікальні сценарії використання мережі та різні рівні критичності доступу до даних. Основний «двигун» компанії − відділ розробки. Його фахівці генерують найбільший обсяг трафіку через постійну роботу з репозиторіями, збірку проєктів та тестування мікросервісів. На противагу їм, адміністративні підрозділи, як-от відділ кадрів (HR), оперують значно меншими обсягами даних, проте їхній трафік містить конфіденційну інформацію, що потребує суворої ізоляції від загального потоку.

Загальний штат компанії налічує від 50 до 70 співробітників. Це та «золота середина», де мережа вже занадто велика для простої топології, але ще дозволяє впроваджувати точкові налаштування безпеки. В нашій моделі ми відтворили ключові сегменти інфраструктури, що охоплюють як стаціонарні робочі місця, так і серверний парк, необхідний для життєдіяльності офісу.

Головною особливістю діяльності такої компанії є висока щільність використання мережевих сервісів. Кожен робочий процес зав'язаний на доступі до внутрішніх серверів, коректній роботі DNS-служб та автоматизованому отриманні адрес. Це робить неможливим існування мережі без чіткого розмежування доступу. Саме тому в проєкті реалізовано логічне сегментування: кожен відділ «живе» у своєму власному просторі, що не лише підвищує рівень

безпеки, а й дозволяє адміністраторам локалізувати технічні проблеми в межах однієї групи, не перериваючи роботу всієї фірми.

Детальний розподіл ресурсів та функціональні особливості кожного підрозділу, які лягли в основу нашого проєктування, систематизовані у наступній таблиці.

Таблиця 3.1 – Основні підрозділи IT-компанії

Підрозділ	Кількість працівників	Мережеві пристрої	Особливості використання мережі
Відділ розробки	25–40	Персональні комп’ютери	Активний доступ до серверів, розробка ПЗ
Відділ кадрів (HR)	5–10	Персональні комп’ютери	Робота з внутрішніми документами, обмежений доступ
Бездротові користувачі	5–10	Ноутбуки	Підключення через Wi-Fi, мобільний доступ
Серверна інфраструктура	–	Сервер (DHCP, DNS, Web)	Надання мережевих сервісів
Адміністрація мережі	1–3	Мережеві пристрої	Управління та підтримка мережі

Як бачимо, структура компанії відображає класичну модель сучасного IT-бізнесу, де кожен вузол має чітко визначену роль. Така диференціація потреб формує ідеальне підґрунтя для побудови розгалуженої системи, яка здатна масштабуватися. Впровадження розділеної архітектури гарантує, що розширення відділу розробки чи поява нових серверів не змусить нас переробляти всю мережу з нуля, а лише вимагатиме додавання нових логічних сегментів у межах вже існуючої безпечної екосистеми.

3.2. Вимоги до мережі

Проєктування мережевої інфраструктури для IT-підприємства починається з чіткого визначення функціональних вимог, які описують здатність системи підтримувати щоденні бізнес-операції. У межах нашого проєкту ми ставимо за мету створення безшовного середовища, яке об’єднує робочі станції програмістів, тестувальників та адміністраторів у єдину, керовану екосистему. Щоб ця складна взаємодія не перетворилася на хаос, ми інтегруємо в ядро мережі базові автоматизовані служби. Використання протоколу DHCP стає тут першою лінією оптимізації: динамічне керування адресним простором дозволяє нам забути про ручне налаштування кожного клієнта. Це не лише економить час, а й страхує мережу від технічних паралічів, спричинених конфліктами дубльованих IP-адрес.

Паралельно з автоматизацією адрес, висуваємо жорсткі вимоги до зручності навігації, що реалізується через службу доменних імен DNS [2]. Для сучасного розробника важливо звертатися до внутрішніх ресурсів, тестових стендів або репозиторіїв за зрозумілими символьними іменами, а не тримати в пам’яті десятки числових ідентифікаторів. Наявність внутрішнього веб-сервера з технічною документацією та базами знань робить таку службу обов’язковою умовою для прозорої роботи колективу.

Сучасна IT-інфраструктура неможлива без мобільності, тому ми закладаємо вимогу щодо створення надійного бездротового сегмента. Технологія Wi-Fi у нашому проєкті − це не просто зручність, а засіб підтримки гнучких робочих процесів. При цьому вся логіка побудови мережі тримається на сегментації через VLAN. Розглядаємо це як вимогу номер один для дотримання порядку: трафік розробників не повинен перетинатися з потоками даних HR-департаменту чи адміністрації на рівні широкомовних доменів. Взаємодія між цими ізольованими «островами» передається на рівень ядра (Inter-VLAN routing), де ми отримуємо можливість централізовано фільтрувати та контролювати кожен пакет.

Окремий блок вимог стосується нефункціональних характеристик, де на першому місці стоїть інформаційна безпека. Було впроваджено принцип «ешелонованого захисту». Наприклад, доступ до серверного парку має бути суворо регламентований списками контролю доступу (ACL). Ми не просто дозволяємо доступ, ми визначаємо конкретні порти та протоколи, якими може користуватися певна група співробітників. На фізичному рівні комутації ми висуваємо вимогу щодо активації Port Security. Це наш запобіжник від підключення стороннього обладнання: будь-який неавторизований пристрій, підключений до офісної розетки, має негайно блокуватися.

Вимоги до безпеки розповсюджуються і на бездротові мережі. Стандарт WPA2 (або WPA3 за можливості) є обов'язковим для аутентифікації співробітників. При цьому для відвідувачів офісу передбачено окремий гостьовий доступ, який має бути логічно відрізаний від внутрішніх ресурсів компанії. Гість отримує вихід у глобальну мережу, але не бачить жодного внутрішнього сервера − це базовий стандарт конфіденційності для будь-якої серйозної організації.

На завершення, закладаємо в проєкт вимоги до масштабованості та відмовостійкості. Мережа повинна не просто працювати «тут і зараз», а мати запас міцності для підключення нових відділів без глобальної переробки архітектури. Проєктуємо систему з розрахунком на те, що навіть вихід з ладу окремого вузла не призведе до зупинки бізнес-процесів. Такий комплексний підхід до формування вимог дозволяє нам створити не просто теоретичну модель, а життєздатну систему, яка відповідає високим стандартам динамічного IT-бізнесу.

3.3. Розробка логічної структури мережі

Розробка логічної структури мережі є одним із найбільш відповідальних етапів проєктування, адже саме на цьому рівні закладаються принципи взаємодії між підрозділами та визначається загальна архітектура інформаційних потоків.

Від того, наскільки правильно організовані мережеві ресурси, залежить не лише зручність адміністрування, а й фундаментальна стійкість системи до внутрішніх і зовнішніх загроз. У межах даного проєкту центральним технологічним рішенням стало впровадження віртуальних локальних мереж, відомих як VLAN. Вибір на користь цієї технології дозволяє відійти від концепції «пласкої» мережі та логічно розділити єдину фізичну інфраструктуру на кілька ізольованих сегментів, що функціонують незалежно один від одного.

Такий підхід до сегментації забезпечує розв’язання одразу декількох критичних завдань. По-перше, це дозволяє чітко відокремити трафік різних відділів компанії, запобігаючи несанкціонованому доступу до конфіденційних даних. По-друге, використання VLAN суттєво оптимізує роботу обладнання шляхом обмеження доменів широкомовлення, що зменшує обсяг надлишкового трафіку та підвищує загальну продуктивність мережі. У розробленій моделі кожен функціональний підрозділ отримав власний логічний сегмент, що дозволяє адміністратору гнучко налаштовувати права доступу та пріоритезацію трафіку залежно від потреб конкретної групи користувачів.

Зокрема, логічна структура проєкту передбачає використання декількох специфічних VLAN, кожна з яких має своє цільове призначення. Для забезпечення поточної діяльності розробників виділено VLAN 20, тоді як робота відділу кадрів організована в межах VLAN 30. Критично важлива частина мережі − серверна інфраструктура − винесена в окрему VLAN 40, що створює додатковий бар’єр безпеки навколо центральних ресурсів компанії. Окрему увагу приділено мобільності та гостьовому доступу: бездротовий сегмент для співробітників функціонує у VLAN 60, що дозволяє ізолювати ноутбуки та смартфони від дротової мережі, а для відвідувачів офісу створено гостьову VLAN 50 з обмеженими правами доступу лише до мережі Інтернет.

Оскільки повна ізоляція сегментів унеможливила б роботу компанії, для забезпечення контрольованої взаємодії між ними було реалізовано механізм міжвланової маршрутизації. Це завдання покладено на комутатор рівня ядра, де для кожної віртуальної мережі створено відповідний віртуальний інтерфейс SVI.

Ці інтерфейси виступають у ролі шлюзів за замовчуванням для кожного сегмента, дозволяючи централізовано керувати маршрутами та застосовувати правила фільтрації трафіку. Така конфігурація забезпечує баланс між безпечною ізоляцією та необхідною функціональністю, коли, наприклад, розробникам потрібен доступ до серверів, але при цьому вони не повинні бачити трафік фінансового відділу.

Важливою складовою технічного проєкту є продумана схема IP-адресації, яка базується на приватному діапазоні адрес згідно зі стандартом RFC 1918 [3]. Для кожного логічного сегмента (VLAN) виділено окрему підмережу з маскою /24. Такий вибір є оптимальним, оскільки він забезпечує достатній запас адрес для підключення великої кількості пристроїв у кожному відділі та значно спрощує подальше адміністрування та візуальну ідентифікацію трафіку в журналах подій. Розподіл адрес всередині кожної підмережі підпорядковується єдиній логіці: перша доступна адреса завжди закріплюється за шлюзом, що полегшує діагностику мережі.

Для більшості кінцевих користувачів передбачено автоматичне отримання налаштувань за допомогою протоколу DHCP, що мінімізує ризик виникнення помилок конфігурації на робочих станціях. Водночас для серверного обладнання та активних мережевих пристроїв застосовується статична адресація. Це гарантує, що ключові сервіси завжди будуть доступні за незмінними адресами, що є критично важливим для стабільної роботи внутрішніх систем. Повна структура розподілу адресного простору та відповідність номерів VLAN наведена у таблиці, яка візуалізує цілісність розробленої архітектури.

Таблиця 3.2 – IP-адресація та VLAN мережі

VLAN ID	Назва VLAN	IP-мережа	Пристрої	Комутатор	Порти
10	Management	192.168.10.0/24	Мережеві пристрої (SW1, SW2, SW3, SW4, FW1)	SW1-CORE	SVI (VLAN 10)
20	Developers	192.168.20.0/24	PC0, PC1, PC2, PC3, PC4, PC5	SW2-ACC	Fa0/2 – Fa0/7
30	HR	192.168.30.0/24	PC6, PC7, PC8, PC9	SW3-ACC	Fa0/2 – Fa0/5
40	Servers	192.168.40.0/24	SRV1 (DHCP, DNS, Web)	SW4-SERVER	Fa0/2
50	Guest	192.168.50.0/24	Гостьові пристрої (резерв)		
60	WiFi (Office)	192.168.60.0/24	Laptop0–Laptop3, AP1-WIFI	SW2-ACC	Fa0/24 (AP)

Варто підкреслити, що узгоджене поєднання технології VLAN та ієрархічної схеми IP-адресації дозволяє створити надзвичайно гнучку інфраструктуру. Така мережа є масштабованою, оскільки вона дозволяє додавати нові підрозділи або змінювати існуючі без потреби у фізичній перебудові лінійної частини [4]. Розроблена логічна структура повністю відповідає високим стандартам сучасних IT-компаній, забезпечуючи необхідну продуктивність, високий рівень безпеки та зручність у щоденному управлінні мережею.

3.4. Забезпечення безпеки мережі

Питання інформаційного захисту є одним із найбільш пріоритетних аспектів при проєктуванні корпоративної мережі IT-підприємства. Враховуючи

динамічний характер кіберзагроз, у межах даного проєкту впроваджено багатоешелоновану систему безпеки. Основна увага приділяється не лише захисту периметра, а й контролю внутрішніх інформаційних потоків, запобіганню несанкціонованим підключенням та суворому розмежуванню прав доступу до сервісів.

Фундаментом архітектури безпеки обрано логічну сегментацію на базі технології VLAN. Такий підхід дозволяє локалізувати трафік окремих підрозділів у межах власних широкомовних доменів. Завдяки ізоляції сегментів суттєво мінімізується ризик поширення шкідливого програмного забезпечення або наслідків потенційних атак типу «відмова в обслуговуванні» (DoS) між відділами. Сегментація створює необхідні умови для подальшого впровадження політик доступу до критичної серверної інфраструктури.

Для регулювання міжсегментної взаємодії застосовуються списки контролю доступу (Access Control Lists, ACL) [8]. Фільтрація трафіку на мережевому рівні здійснюється на основі аналізу IP-адрес джерела та призначення. Зокрема, у розробленій моделі впроваджено правила, що обмежують доступ персоналу відділу кадрів до специфічних ресурсів серверного сегмента, залишаючи доступними лише необхідні службові сервіси. Аналогічний підхід застосовано і до гостьової мережі, яка повністю ізольована від внутрішніх корпоративних баз даних та робочих станцій співробітників.

Централізоване управління політиками фільтрації реалізовано на комутаторі рівня ядра, що забезпечує високу продуктивність при обробці трафіку між віртуальними мережами. Проте захист від зовнішніх загроз покладено на окремий пристрій − міжмережевий екран (Firewall) [7], встановлений на межі з мережею загального користування. Основною функцією цього вузла є контроль вхідних та вихідних сесій з використанням механізмів інспекції стану з’єднань. Це гарантує, що жоден зовнішній пакет не потрапить усередину мережі, якщо він не є частиною санкціонованої сесії, ініційованої довіреним внутрішнім пристроєм.

На рівні доступу (Access Layer) реалізовано заходи фізичної безпеки за допомогою технології Port Security. Даний механізм дозволяє жорстко обмежити кількість пристроїв, що можуть бути під'єднані до одного порту комутатора. У межах проєкту встановлено ліміт на рівні двох унікальних MAC-адрес на кожен активний порт. У разі спроби підключення стороннього обладнання (наприклад, неавторизованого ноутбука або хаба) порт автоматично переходить у стан блокування (shutdown або restrict), що унеможливлює компрометацію мережі на низовому рівні.

Забезпечення захисту бездротового сегмента базується на використанні сучасного стандарту аутентифікації WPA2-PSK [10]. Застосування стійких алгоритмів шифрування запобігає перехопленню конфіденційної інформації під час її передачі через радіоканал. Доступ до Wi-Fi надається лише авторизованим користувачам, що в поєднанні з логічною ізоляцією бездротової VLAN створює надійний бар'єр для захисту мобільних робочих станцій персоналу.

Таким чином, розроблена система захисту поєднує заходи на канальному, мережевому та прикладному рівнях моделі OSI. Такий комплексний підхід відповідає актуальним вимогам до побудови захищених корпоративних інфраструктур, забезпечуючи високий рівень цілісності даних, конфіденційності та керованості мережі IT-компанії.

Висновки до розділу 3

У третьому розділі ми розробили цілісну архітектуру мережевої інфраструктури IT-компанії. На основі розроблених вимог спроєктовано логічну структуру, що базується на поділі мережі на шість функціональних VLAN-сегментів, що відповідає організаційному поділу підприємства на департаменти (розробка, кадри, сервери, гості тощо). Виконали розрахунок та планування адресного простору за стандартом RFC 1918, що забезпечує унікальність та структурованість IP-адресації в межах всієї компанії. Обґрунтували впровадження механізмів міжвланової маршрутизації на рівні ядра мережі, що

дозволяє централізовано керувати потоками даних. Запропонована схема безпеки, що включає Port Security на портах доступу та специфічні правила ACL для обмеження доступу до серверного сегмента, дозволяє досягти балансу між функціональною відкритістю для співробітників та захищеністю критичних ресурсів. Створена модель є масштабованою та готова до подальшої технічної реалізації.

РОЗДІЛ 4. РЕАЛІЗАЦІЯ ТА ТЕСТУВАННЯ МЕРЕЖІ ІТ-КОМПАНІЇ

4.1. Методика налаштування мережевого обладнання в середовищі Cisco Packet Tracer

Процес програмної реалізації мережевої інфраструктури для ІТ-компанії виконувався у спеціалізованому середовищі імітаційного моделювання Cisco Packet Tracer. Вибір даного інструментарію обумовлений його здатністю точно відтворювати поведінку реальних апаратних засобів під управлінням операційної системи Cisco IOS (Internetwork Operating System). На відміну від простого графічного малювання схем, робота в Packet Tracer передбачає повноцінне конфігурування кожного вузла через інтерфейс командного рядка (CLI − Command Line Interface), що є галузевим стандартом для мережевих інженерів.

Основним принципом методики налаштування є ієрархічний підхід до управління пристроями. В системі Cisco IOS реалізована чітка структура рівнів доступу, що дозволяє розмежувати функції перегляду стану та безпосереднього внесення змін у конфігурацію:

1. Користувацький режим (User EXEC Mode): Початковий рівень доступу, який позначається знаком >. Він призначений для базової діагностики та перегляду обмеженого набору статистичних даних.

2. Привілейований режим (Privileged EXEC Mode): Активується командою enable (знак #). Цей рівень є критично важливим для адміністратора, оскільки дозволяє виконувати команди збереження конфігурації, перегляду таблиць маршрутизації та детального аналізу роботи протоколів.

3. Режим глобальної конфігурації (Global Configuration Mode): Доступ до нього відкривається командою configure terminal. Саме на цьому рівні вносяться зміни, що впливають на роботу пристрою в цілому − від імені хоста (hostname) до налаштування алгоритмів безпеки та маршрутизації.

Технологічний цикл налаштування обладнання в межах даного проєкту включав наступні ключові аспекти:

– Конфігурування віртуальних каналів (VLAN та Trunk): Для реалізації логічної сегментації, описаної в Розділі 1, використовувався синтаксис створення VLAN-ів (vlan [ID]). Важливою частиною методики було налаштування магістральних каналів (Trunk-портів) за допомогою протоколу 802.1Q. Команда switchport mode trunk на портах комутатора SW1-CORE дозволила передавати трафік декількох підмереж через один фізичний кабель, що критично важливо для ієрархічної структури мережі IT-компанії.

– Логіка міжвланової маршрутизації (SVI): Оскільки в проєкті використано комутатор третього рівня (L3), налаштування шлюзів для кожного відділу відбувалося через створення віртуальних інтерфейсів (Switch Virtual Interfaces). Використання команди interface vlan [ID] з подальшим призначенням IP-адреси дозволило об’єднати функції комутації та маршрутизації в одному пристрої, мінімізуючи затримки при передачі даних між відділами.

– Динамічне керування маршрутами (OSPF): Для автоматизації обміну інформацією про мережі між роутером R1-EDGE, Firewall та SW1-CORE було використано протокол OSPF. Методика конфігурування передбачала визначення ідентифікатора процесу (router ospf 1) та оголошення підмереж у нульовій зоні (Area 0). Це забезпечує високу відмовостійкість: у разі виходу з ладу одного з каналів, протокол автоматично перераховує найкоротший шлях для пакетів.

– Системний контроль доступу (ACL): На міжмережевому екрані FW1 реалізована логіка фільтрації на основі розширених списків контролю доступу. На відміну від стандартних списків, розширені ACL дозволяють фільтрувати трафік не тільки за адресою відправника, а й за типом протоколу (TCP/UDP) та номером порту, що є базовим елементом захисту серверного сегмента.

Завершальним етапом будь-якої сесії налаштування була верифікація параметрів. Використання команд сімейства show (наприклад, show ip route або show vlan brief) дозволяло переконатися в коректності застосованих налаштувань ще до етапу комплексного тестування мережі. Всі внесені зміни обо’язково дублювалися в енергонезалежну пам’ять (NVRAM) командою write, що гарантує збереження працездатності мережі після перезавантаження обладнання.

4.2. Реалізація мережі в середовищі Cisco Packet Tracer

На основі розробленої архітектури та методики налаштування, описаної у попередньому підрозділі, було проведено безпосередню побудову віртуальної моделі мережі IT-компанії. Практична реалізація проєкту полягала у розміщенні активного мережевого обладнання, виборі відповідних типів кабельних з'єднань та створенні цілісної топології, що відповідає технічним вимогам замовника.

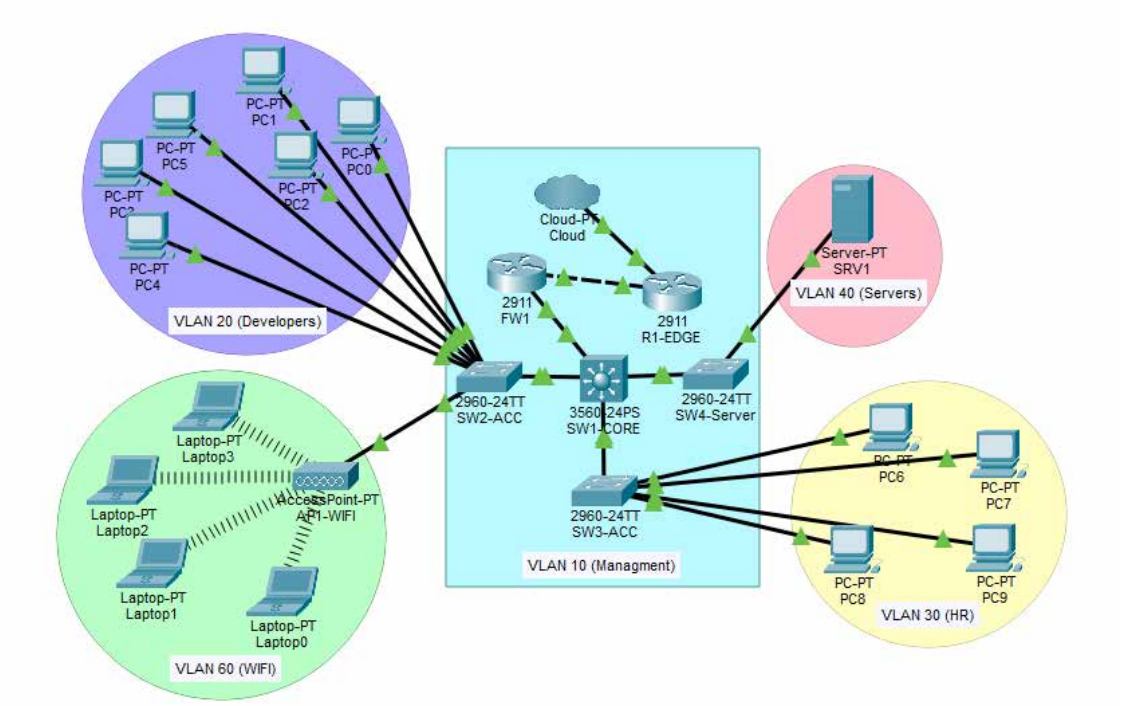

Рис 4.1 – Загальна топологія мережі

На початковому етапі було створено топологію мережі [9] відповідно до розробленої логічної структури. У середовищі моделювання розміщено основні мережеві пристрої, зокрема комутатори рівня доступу, комутатор рівня ядра, маршрутизатор, міжмережевий екран, сервер та кінцеві пристрої користувачів. Побудована топологія відображає структуру IT-компанії та забезпечує розподіл мережі на окремі сегменти.

У центрі мережі розташовано комутатор рівня ядра (SW1-CORE), який виконує функції міжвланової маршрутизації та забезпечує взаємодію між усіма сегментами мережі. До нього підключені комутатори рівня доступу, які

обслуговують окремі підрозділи компанії. Зокрема, комутатор SW2-ACC використовується для підключення робочих станцій відділу розробки та точки бездротового доступу, а комутатор SW3-ACC – для підключення пристроїв відділу кадрів. Серверна інфраструктура винесена на окремий комутатор SW4-SERVER, що дозволяє забезпечити централізоване управління серверними ресурсами.

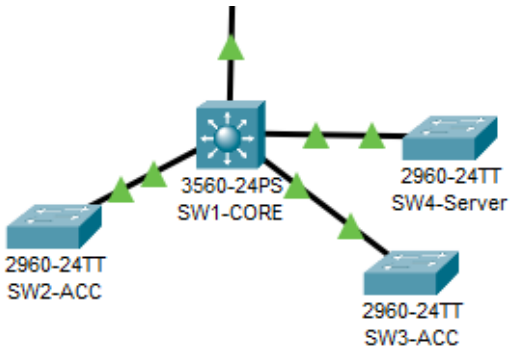

Рисунок 4.2 – Ядро мережі та комутатори доступу

Фізичне з'єднання пристроїв виконано з урахуванням їх ролі у мережі. Для підключення кінцевих пристроїв до комутаторів використано прямі мідні кабелі (Copper Straight-Through), тоді як для з'єднання мережевих пристроїв між собою застосовано відповідні типи кабелів згідно з рекомендаціями середовища моделювання. Такий підхід дозволяє коректно відтворити реальні умови функціонування мережі.

Окрему роль у мережі відіграє сервер, який забезпечує роботу ключових сервісів, зокрема DHCP, DNS та веб-сервера. Він підключений до серверного сегмента мережі, що забезпечує його ізоляцію та підвищує рівень безпеки.

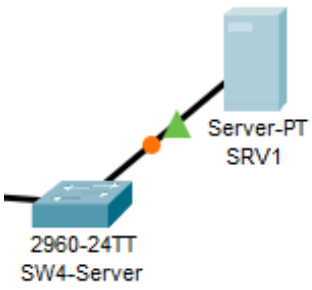

Рисунок 4.3 – Підключення серверної інфраструктури

Для того щоб мати доступ до зовнішнього світу в топології передбачено маршрутизатор (R1-EDGE), який з’єднаний із умовною хмарою (Cloud). Ця хмара імітує Інтернет. Між внутрішньою мережею і зовнішнім світом стоїть міжмережевий екран (FW1). Він фільтрує трафік і покращує безпеку.

У межах реалізації також передбачено бездротовий доступ до мережі за допомогою точки доступу (AP1-WIFI), що дозволяє підключати мобільні пристрої співробітників. Це забезпечує гнучкість використання мережі та відповідає сучасним вимогам до організації робочого середовища.

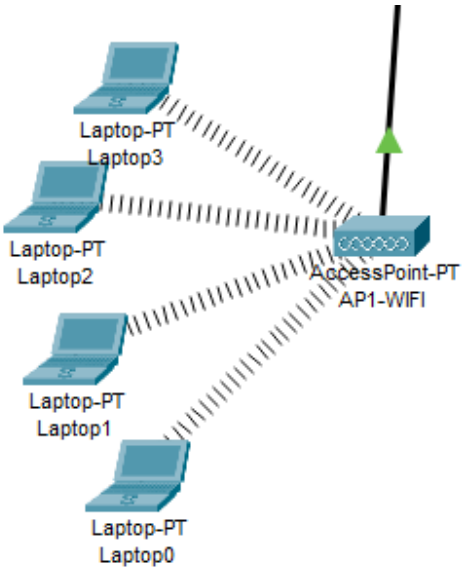

Рисунок 4.4 – Організація бездротового доступу

4.3. Налаштування мережевого обладнання

Після створення топології мережі в середовищі Cisco Packet Tracer було виконано налаштування мережевого обладнання, яке включає конфігурацію комутаторів, маршрутизацію між VLAN, а також реалізацію базових механізмів безпеки.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#ip routing
Switch(config)#vlan 10
Switch(config-vlan)#name MANAGEMENT
Switch(config-vlan)#vlan 20
Switch(config-vlan)#name DEVELOPERS
Switch(config-vlan)#vlan 30
Switch(config-vlan)#name HR
Switch(config-vlan)#vlan 40
Switch(config-vlan)#name SERVERS
Switch(config-vlan)#
Switch(config-vlan)#vlan 50
Switch(config-vlan)#name GUEST
Switch(config-vlan)#vlan 60
Switch(config-vlan)#name WIFI
```

Рисунок 4.5 – Створення VLAN на SW1-CORE

На першому етапі виконано налаштування комутатора рівня ядра, який забезпечує міжвланову маршрутизацію. Для кожного логічного сегмента створено відповідні VLAN, після чого налаштовано віртуальні інтерфейси (SVI), що виконують роль шлюзів за замовчуванням для кожної підмережі. Це дозволило організувати взаємодію між різними підрозділами компанії в межах єдиної мережі.

```
Switch(config-vlan)#interface vlan 10
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan10, changed state to up
ip address 192.168.10.1 255.255.255.0
Switch(config-if)#ip address 192.168.10.1 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#interface vlan 20
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan20, changed state to up

Switch(config-if)#ip address 192.168.20.1 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#interface vlan 30
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan30, changed state to up

Switch(config-if)#ip address 192.168.30.1 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#interface vlan 40
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan40, changed state to up

Switch(config-if)#ip address 192.168.40.1 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#interface vlan 50
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan50, changed state to up

Switch(config-if)#ip address 192.168.50.1 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#interface vlan 60
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan60, changed state to up

Switch(config-if)#ip address 192.168.60.1 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#
```

Рисунок 4.6 – налаштування SVI на комутаторі SW1-CORE

Подальшим етапом стало налаштування транкових з’єднань між комутатором ядра та комутаторами доступу. Для цього відповідні порти було переведено в режим trunk [5], що забезпечує передачу трафіку декількох VLAN через один фізичний канал. Це дозволяє зберігати логічну сегментацію мережі при використанні обмеженої кількості фізичних з’єднань.

```
Switch(config)#interface fa0/1
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#switchport mode trunk
```

Рисунок 4.7 – Налаштування trunk з’єднання між комутаторами

На комутаторах рівня доступу виконано налаштування портів у режимі access відповідно до призначення кожного підрозділу. Кожен порт було прив’язано до конкретної VLAN, що забезпечує правильний розподіл пристроїв за сегментами мережі. Такий підхід дозволяє ізолювати трафік та підвищити ефективність роботи мережі.

```
Switch>enable
Switch#configure t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 20
Switch(config-vlan)#name DEVELOPERS
Switch(config-vlan)#
Switch(config-vlan)#vlan 50
Switch(config-vlan)#name GUEST
Switch(config-vlan)#vlan 60
Switch(config-vlan)#name WIFI
Switch(config-vlan)#interface fa0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#interface range fa0/2 - 7
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 20
Switch(config-if-range)#interface fa0/24
Switch(config-if)#switchport mode trunk
```

Рисунок 4.8 – Налаштування access-портів на комутаторах доступу

З метою підвищення рівня безпеки на комутаторах доступу реалізовано механізм Port Security. Для кожного порту встановлено обмеження на кількість допустимих MAC-адрес, що дозволяє запобігти підключенню неавторизованих пристроїв. У разі порушення встановлених правил застосовується відповідна політика реагування.

```
Switch(config-if)#interface range fa0/2 - 7
Switch(config-if-range)#switchport port-security
Switch(config-if-range)#switchport port-security maximum 2
Switch(config-if-range)#switchport port-security violation restrict
Switch(config-if-range)#switchport port-security mac-address sticky
Switch(config-if-range)#end
```

Рисунок 4.9 – Налаштування Port Security

Для забезпечення взаємодії клієнтських пристроїв із сервером DHCP, який розміщений в окремому сегменті мережі, на комутаторі ядра було налаштовано механізм пересилання широкомовних запитів за допомогою команди ip helper-address. Це дозволяє коректно обслуговувати запити DHCP між різними VLAN.

```
Switch>enable
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface vlan 20
Switch(config-if)#ip helper-address 192.168.40.10
Switch(config-if)#
Switch(config-if)#interface vlan 30
Switch(config-if)#ip helper-address 192.168.40.10
Switch(config-if)#interface vlan 50
Switch(config-if)#ip helper-address 192.168.40.10
Switch(config-if)#interface vlan 60
Switch(config-if)#ip helper-address 192.168.40.10
Switch(config-if)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console
write
Building configuration...
[OK]
```

Рисунок. 4.10 – Налаштування ip helper-address

Наступним практичним етапом стала реалізація динамічного обміну маршрутами між граничним роутером R1-EDGE та міжмережевим екраном FW1 за допомогою протоколу OSPF. У ході конфігурування було активовано відповідний процес маршрутизації та оголошено суміжні підмережі в межах магістральної зони Area 0. Це дозволило автоматизувати оновлення таблиць маршрутизації на межі корпоративної мережі та забезпечити стабільний зв’язок із зовнішнім сегментом.

```
Switch>enable
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface g0/1
Switch(config-if)#no switchport
Switch(config-if)#ip address 192.168.100.2 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#router ospf 1
Switch(config-router)#network 192.168.100.0 0.0.0.255 area 0
Switch(config-router)#network 192.168.0.0 0.0.255.255 area 0
Switch(config-router)#end
Switch#
```

Рисунок 4.11 — Конфігурування протоколу динамічної маршрутизації OSPF

Окрему увагу приділено реалізації механізмів фільтрації трафіку. Для цього використано списки контролю доступу (ACL), які дозволяють обмежити взаємодію між окремими сегментами мережі. Зокрема, реалізовано заборону доступу відділу кадрів до серверного сегмента, що підвищує рівень захисту інформаційних ресурсів.

```
Switch>enable
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#access-list 110 deny ip 192.168.30.0 0.0.0.255 192.168.40.0 0.0.0.255
Switch(config)#access-list 110 permit ip any any
Switch(config)#interface vlan 30
Switch(config-if)#ip access-group 110 in
```

Рисунок 4.12 –Налаштування ACL для обмеження доступу

Таким чином у процесі налаштування мережевого обладнання було реалізовано всі необхідні функції для забезпечення роботи корпоративної мережі включаючи сегментацію, маршрутизацію та базові механізми безпеки. Отримана конфігурація відповідає вимогам до сучасних мереж і забезпечує стабільну та безпечну роботу користувачів.

4.4. Конфігурація серверних сервісів (DHCP, DNS, Web)

В рамках реалізації мережі IT-компанії був налаштований сервер, що забезпечує роботу основних мережевих сервісів, а саме DHCP, DNS та веб-сервера. Використання централізованого сервера дозволяє спростити адміністрування мережі та забезпечити стабільний доступ користувачів до необхідних ресурсів.

На першому етапі було налаштовано службу DHCP, яка відповідає за автоматичне призначення IP-адрес клієнтським пристроям. Для кожної VLAN створено окремий пул адрес, що відповідає її підмережі. У налаштуваннях DHCP вказано діапазон IP-адрес, шлюз за замовчуванням та адресу DNS-сервера. Це дозволяє клієнтським пристроям автоматично отримувати всі необхідні параметри для роботи в мережі.

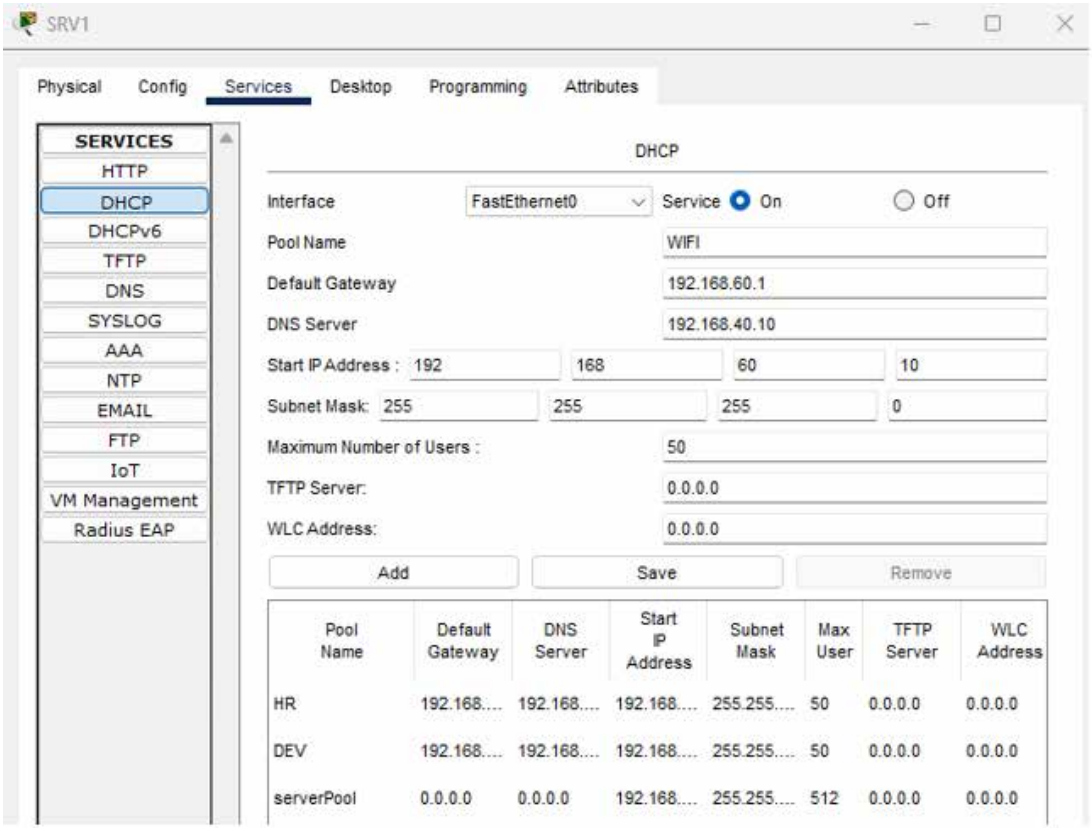

Рисунок 4.13 – Налаштування DHCP-сервера

Після налаштування DHCP було перевірено його працездатність шляхом підключення клієнтських пристроїв у різних VLAN. У результаті всі пристрої

успішно отримали IP-адреси відповідно до своєї підмережі, що підтверджує коректність налаштування служби.

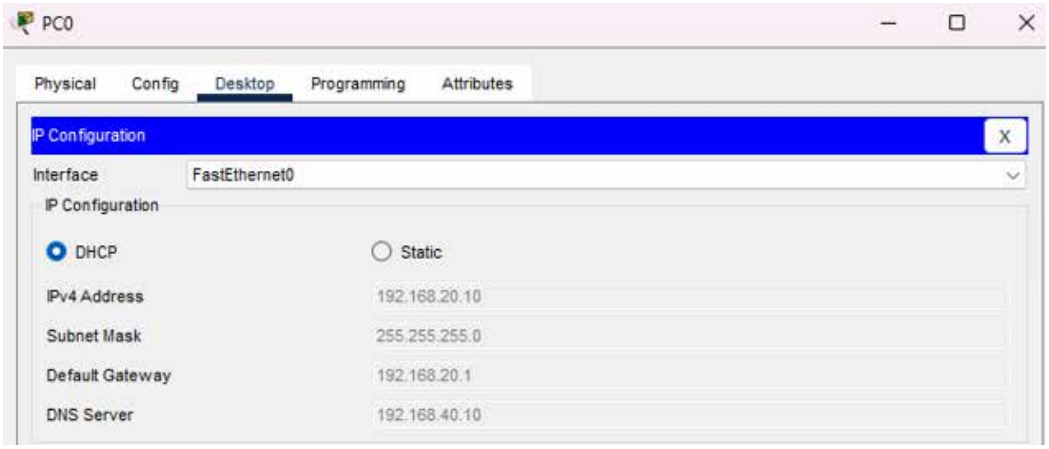

Рисунок 4.14 – Отримання IP-адреси клієнтським пристроєм (DHCP)

Наступним етапом було налаштування служби доменних імен (DNS), яка забезпечує перетворення доменних імен у IP-адреси. На сервері було створено запис для внутрішнього веб-ресурсу компанії, що дозволяє користувачам звертатися до нього за зручним символьним ім’ям.

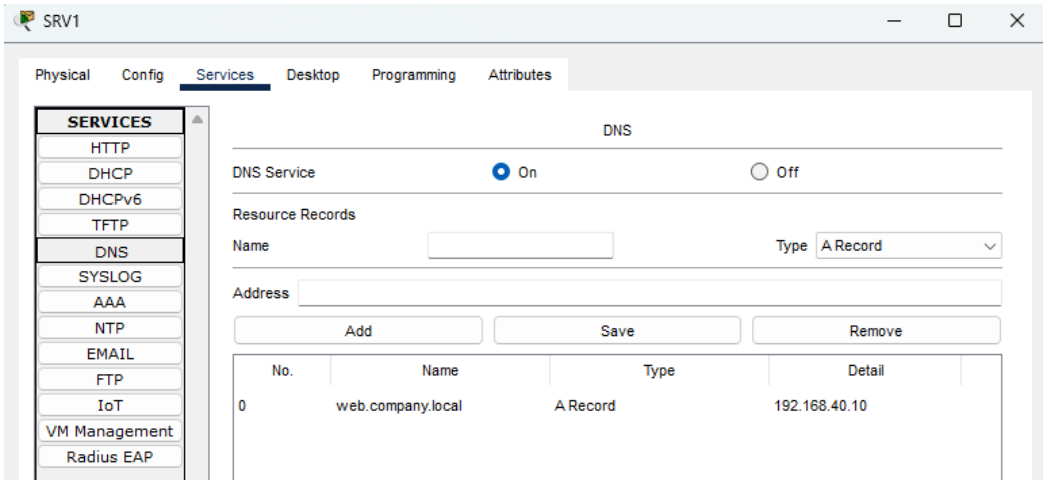

Рисунок 4.15 – Налаштування DNS-сервера

Після цього було налаштовано веб-сервер, який використовується для розміщення внутрішнього ресурсу компанії. Веб-сервер працює за протоколом HTTP та забезпечує доступ користувачів до інформаційних сторінок через браузер.

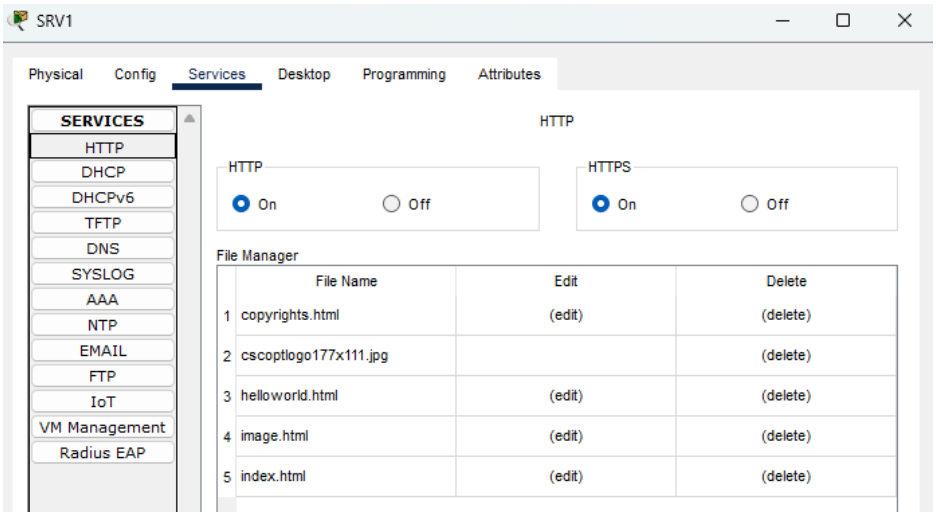

Рисунок 4.16 – Налаштування веб-сервера (HTTP)

Для перевірки роботи веб-сервера та DNS-служби було виконано підключення з клієнтського пристрою через веб-браузер із використанням доменного імені. У результаті користувач отримав доступ до веб-сторінки, що підтверджує коректну роботу всіх налаштованих сервісів.

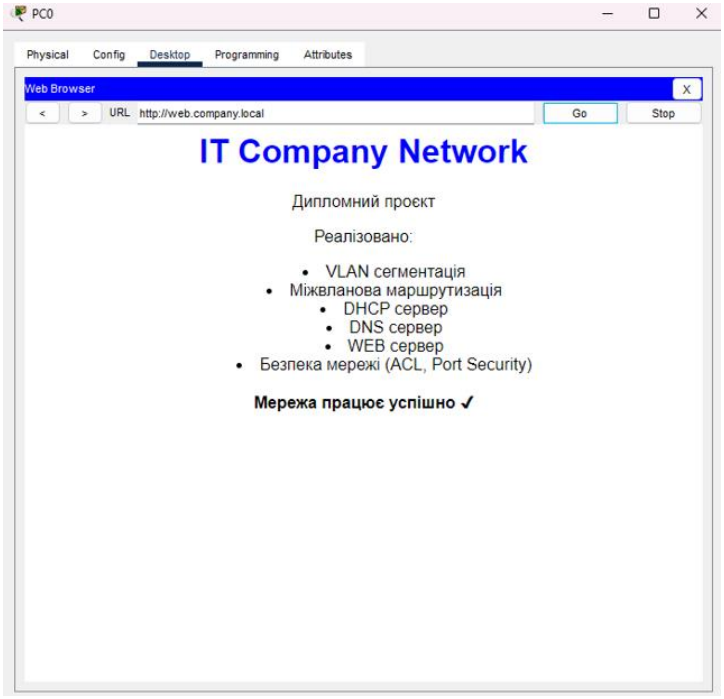

Рисунок 4.17 – Доступ до веб-сервера через браузер

Комплексне налаштування серверної підсистеми забезпечило повноцінне функціонування мережевої екосистеми, надавши користувачам необхідні інструменти для автоматизації робочих процесів та швидкого доступу до корпоративної інформації.

4.5. Тестування працездатності та продуктивності мережі

Після завершення налаштування мережевого обладнання та серверних сервісів було проведено тестування працездатності мережі. Основною метою тестування є перевірка коректності роботи всіх компонентів мережі, а також підтвердження відповідності отриманої конфігурації поставленим вимогам.

На першому етапі було перевірено коректність отримання IP-адрес клієнтськими пристроями. Для цього на робочих станціях було активовано автоматичне отримання параметрів мережі. У результаті всі пристрої отримали IP-адреси відповідно до своїх VLAN, що підтверджує правильну роботу DHCP-сервера.

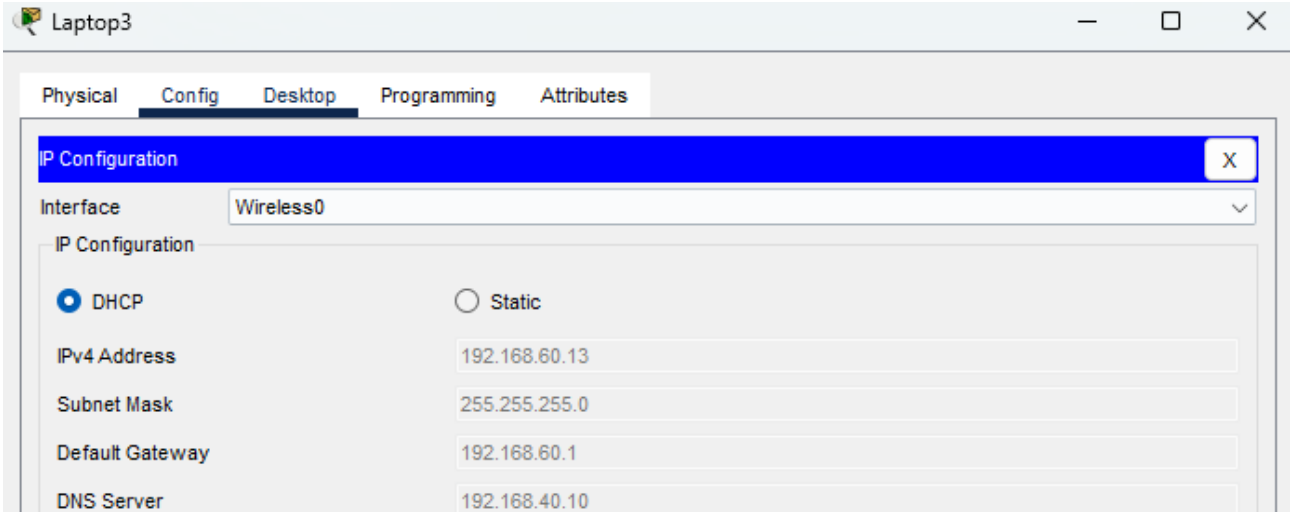

Рисунок 4.18 – Отримання IP-адреси клієнтським пристроєм

Наступним етапом було перевірено мережеву взаємодію між пристроями за допомогою утиліти ping. Зокрема, виконано перевірку доступності серверу з різних VLAN. У результаті всі запити були успішно доставлені, що свідчить про коректну роботу міжвланової маршрутизації.

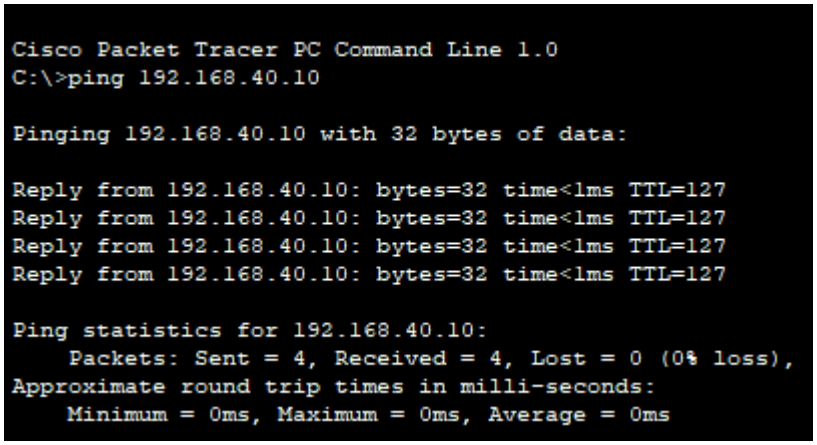

Рисунок 4.19 – Перевірка доступності сервера за допомогою ping

Також була перевірена робота служби доменних імен. Клієнтські пристрої успішно виконують перетворення доменного імені у IP-адресу, що підтверджує коректність налаштування DNS-сервера.

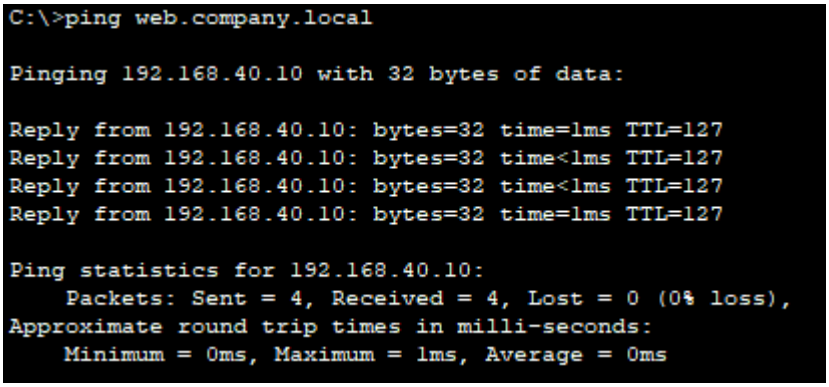

Рисунок 4.20 – Перевірка роботи DNS (ping за доменним іменем)

Окрему увагу приділено перевірці доступу до веб-сервера. Для цього з клієнтського пристрою було відкрито веб-браузер та здійснено перехід за доменним іменем. У результаті користувач отримав доступ до веб-сторінки, що підтверджує коректну роботу HTTP-сервера та DNS-служби.

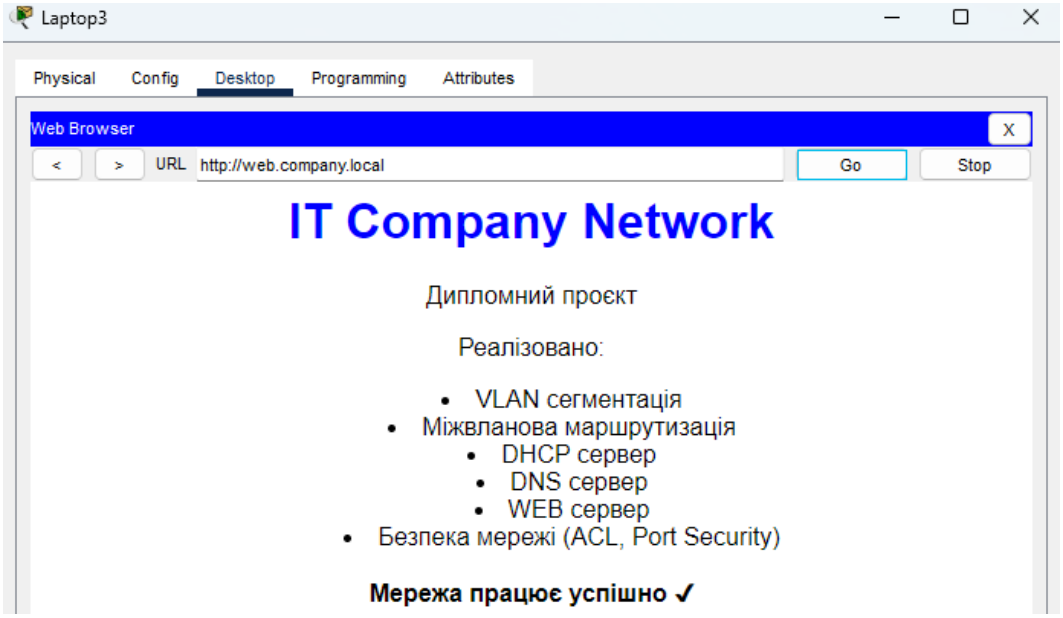

Рисунок 4.21 – Перевірка доступу до веб-сервера

У процесі тестування також перевірено роботу механізмів безпеки. Зокрема, підтверджено обмеження доступу між окремими сегментами мережі відповідно до налаштованих правил ACL. Спроба доступу до заборонених ресурсів не дала результату, що свідчить про ефективність реалізованих політик безпеки.

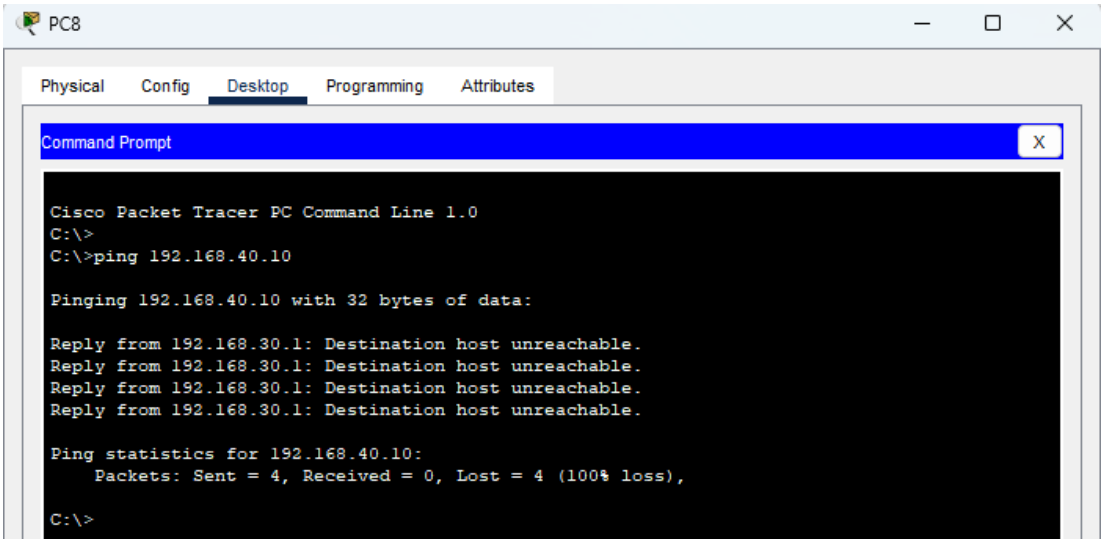

Рисунок 4.22 – Перевірка обмеження доступу (ACL)

Таким чином, у результаті тестування підтверджено працездатність усіх компонентів мережі, включаючи DHCP, DNS, веб-сервер та механізми

маршрутизації. Реалізовані засоби безпеки функціонують коректно та забезпечують контроль доступу до ресурсів мережі.

Отримані результати свідчать про те, що розроблена мережа відповідає поставленим вимогам і може бути використана як модель корпоративної мережевої інфраструктури IT-компанії.

Висновки до розділу 4

У четвертому розділі ми провели практичну реалізацію та детальну апробацію розробленого проєкту в середовищі імітаційного моделювання Cisco Packet Tracer. У ході виконання робіт було успішно сконфігуровано активне мережеве обладнання, включаючи комутатори доступу та ядро мережі з налаштуванням інтерфейсів SVI та транкових з’єднань. Розгорнуто та протестовано ключові мережеві служби: сервер DHCP забезпечує автоматичну видачу адрес у різних підмережах, служба DNS коректно інтерпретує доменні імена внутрішнього веб-ресурсу, а HTTP-сервер надає доступ до корпоративної інформації. Етап верифікації за допомогою утиліт діагностики (ping, браузер) підтвердив цілісність маршрутизації та коректність роботи фільтрів безпеки ACL. Наше тестування показало, що розроблена інфраструктура повністю відповідає критеріям продуктивності та надійності. Отримана віртуальна модель є працездатною і може слугувати прототипом для впровадження реальної мережевої системи на базі обладнання Cisco.

ВИСНОВКИ

Під час виконання роботи нами було спроєктовано та практично реалізовано мережеву інфраструктуру IT-компанії, яка забезпечує стабільну роботу для 50-70 користувачів. На основі аналізу вимог було обрано ієрархічну модель побудови, де центральним вузлом виступає комутатор ядра L3 (SW1-CORE). Це рішення дозволило нам об’єднати функції високошвидкісної комутації та міжвланової маршрутизації в одному пристрої, що критично важливо для мінімізації затримок у передачі даних між відділами компанії.

Основою логічної структури стала глибока сегментація мережі на вісім віртуальних підмереж (VLAN 10-80). Такий підхід дозволив ізолювати трафік відділу розробки, HR-підрозділу, менеджменту та гостьового сегмента. Використання технології 802.1Q (Trunking) на магістральних портах забезпечило коректну передачу тегованого трафіку між комутаторами ядра та доступу, що значно підвищило керованість мережі та дозволило ефективно контролювати широкомовні шторми.

Для автоматизації налаштування робочих станцій було розгорнуто серверний сегмент із підтримкою служб DHCP, DNS та HTTP. Важливим технічним етапом стало налаштування механізму ip helper-address на віртуальних інтерфейсах комутатора ядра. Це дозволило централізованому DHCP-серверу динамічно видавати адреси клієнтам у різних VLAN-ах, що повністю усуває проблему ручного конфігурування IP-параметрів та конфліктів адрес у мережі.

Система безпеки проєкту реалізована через поєднання механізмів на канальному та мережевому рівнях. На портах доступу впроваджено технологію Port Security, яка обмежує кількість підключених MAC-адрес, захищаючи мережу від несанкціонованого фізичного доступу. На межі з Інтернетом встановлено міжмережевий екран FW1, де за допомогою розширених списків контролю доступу (ACL) реалізовано правила фільтрації. Зокрема, налаштовано заборону передачі трафіку між певними підмережами (наприклад, HR та Management), що гарантує конфіденційність внутрішньої інформації.

Налагодження зв’язку між внутрішньою інфраструктурою та граничним маршрутизатором R1-EDGE було виконано за допомогою протоколу динамічної маршрутизації OSPF. Оголошення мереж у нульовій зоні (Area 0) забезпечило автоматичну побудову таблиць маршрутизації та відмовостійкість системи. Підсумкова верифікація в середовищі Cisco Packet Tracer підтвердила працездатність усіх вузлів, коректність видачі адрес та надійність встановлених бар’єрів безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Комп’ютерні мережі : навч. посіб. / А. І. Блозва та ін. Київ : ЦП Компринт, 2017. 840 с. URL: https://nubip.edu.ua/sites/default/files/u34/posibnik_-_kompyuterni_merezhi.pdf (дата звернення: 23.03.2026).
2. Networking Fundamentals : training manual. Cisco Systems, Inc. 2006. 38 p. URL: https://www.cisco.com/c/dam/global/fi_fi/assets/docs/SMB_University_120307_Networking_Fundamentals.pdf (дата звернення: 23.03.2026).
3. Kurose J. F., Ross K. W. Computer Networking: A Top-Down Approach. 8th ed. Boston : Pearson, 2020. 864 p.
4. Peterson L. L., Davie B. S. Computer Networks: A Systems Approach. 6th ed. Boston : Morgan Kaufmann, 2021. 864 p.
5. Avery G. Network Warrior. 2nd ed. Sebastopol, CA : O’Reilly Media, 2014. 688 p.
6. Оліфер В. Г., Оліфер Н. П. Комп’ютерні мережі. Принципи, технології, протоколи. 6-те вид. Київ : Бук-Друк, 2021. 992 с.
7. Santos O. Cisco ASA: All-in-One Next-Generation Firewall, IPS, and VPN Services. 3rd ed. Indianapolis : Cisco Press, 2014. 1032 p.
8. Stewart J. M. Network Security, Firewalls and VPNs. 2nd ed. Burlington, MA : Jones & Bartlett Learning, 2013. 554 p.
9. Lammle T. CCNA Certification Study Guide, Volume 2: Exam 200-301. Indianapolis : John Wiley & Sons, 2020. 608 p.
10. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection − Information security management systems − Requirements. URL: https://www.iso.org/standard/27001 (дата звернення: 25.04.2026).

ДОДАТКИ

Додаток А Налаштування R1-EDGE

```
enable
conf t
interface g0/0
no shutdown
exit
interface g0/1
ip address 192.168.200.2 255.255.255.0
no shutdown
exit
router ospf 1
network 192.168.200.0 0.0.0.255 area 0
exit
end
write
```

Додаток Б Налаштування FW1

```
enable
conf t
interface g0/0
ip address 192.168.200.1 255.255.255.0
no shutdown
exit
interface g0/1
ip address 192.168.100.1 255.255.255.0
no shutdown
exit
router ospf 1
network 192.168.200.0 0.0.0.255 area 0
network 192.168.100.0 0.0.0.255 area 0
exit
access-list 100 deny ip 192.168.30.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 100 permit ip any any
interface g0/1
ip access-group 100 in
exit
end
write
```

Додаток В Налаштування SW1-CORE

```
enable
conf t
ip routing
vlan 10
name MANAGEMENT
exit
vlan 20
name DEVELOPERS
exit
vlan 30
name HR
exit
vlan 40
name SERVERS
exit
vlan 50
name GUEST
exit
vlan 60
name WIFI
exit
interface vlan 10
ip address 192.168.10.1 255.255.255.0
no shutdown
exit
interface vlan 20
ip address 192.168.20.1 255.255.255.0
no shutdown
exit
interface vlan 30
ip address 192.168.30.1 255.255.255.0
no shutdown
exit
interface vlan 40
ip address 192.168.40.1 255.255.255.0
no shutdown
exit
interface vlan 50
ip address 192.168.50.1 255.255.255.0
no shutdown
```

```
exit
interface vlan 60
ip address 192.168.60.1 255.255.255.0
no shutdown
exit
interface fa0/1
switchport trunk encapsulation dot1q
switchport mode trunk
exit
interface fa0/2
switchport trunk encapsulation dot1q
switchport mode trunk
exit
interface fa0/3
switchport trunk encapsulation dot1q
switchport mode trunk
exit
interface g0/1
switchport trunk encapsulation dot1q
switchport mode trunk
exit
access-list 110 deny icmp 192.168.30.0 0.0.0.255 host
192.168.40.10
access-list 110 permit ip any any
interface vlan 30
ip access-group 110 in
exit
access-list 120 deny ip 192.168.50.0 0.0.0.255 any
access-list 120 permit ip any any
interface vlan 50
ip access-group 120 in
exit
end
write
```

Додаток Г Налаштування SW2-ACC

```
enable
conf t
vlan 20
name DEVELOPERS
exit
vlan 60
name WIFI
exit
interface range fa0/2 - 7
switchport mode access
switchport access vlan 20
switchport port-security
switchport port-security maximum 2
switchport port-security violation restrict
exit
interface fa0/1
switchport trunk encapsulation dot1q
switchport mode trunk
exit
end
write
```

Додаток Д Налаштування SW3-ACC

```
enable
conf t
vlan 30
name HR
exit
interface range fa0/2 - 7
switchport mode access
switchport access vlan 30
switchport port-security
switchport port-security maximum 2
switchport port-security violation restrict
exit
interface fa0/1
switchport trunk encapsulation dot1q
switchport mode trunk
exit
end
write
```

Додаток Е Налаштування SW4-SERVER

```
enable
conf t
vlan 40
name SERVERS
exit
interface range fa0/2 - 4
switchport mode access
switchport access vlan 40
exit
interface fa0/1
switchport trunk encapsulation dot1q
switchport mode trunk
exit
end
write
```