НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ДОПУСКАЄТЬСЯ ДО ЗАХИСТУ
Завідувач кафедри
Комп'ютерних систем, мереж та кібербезпеки
_____ Касаткін Д.Ю.,
к.п.н., доц.
підпис ПІБ, вчене звання і ступінь

«___»_____2025 р.

БАКАЛАВРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

На тему: Розробка корпоративної мережі логістичної фірми на основі обладнання фірми “Cisco”

Спеціальність F7 «Комп’ютерна інженерія»

Гарант освітньої програми

к.фіз.-мат.н., доцент _____ Євгеній НІКІТЕНКО

(наукова ступінь, вчене звання) (підпис) (ПІБ)

Керівник бакалаврської кваліфікаційної роботи

старший викладач _____ Володимир МАТІЄВСЬКИЙ

(наукова ступінь, вчене звання) (підпис) (ПІБ)

Виконав

(ПІБ студента)

КИЇВ-2025

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАНН УКРАЇНИ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

«ЗАТВЕРДЖУЮ»
завідувач кафедри
комп'ютерних систем, мереж та кібербезпеки

Касаткін Д.Ю., к.пед.н., доц. /

підпис ПІБ, вчене звання і ступінь

р.

З А В Д А Н Н Я
ДО ВИКОНАННЯ КВАЛІФІКАЦІЙНОЇ БАКАЛАВРСЬКОЇ СТУДЕНТА

Маловатов Дмитро Валерійович

(прізвище, ім'я, по батькові)

Спеціальність (напрям підготовки): комп'ютерна інженерія

Тема випускної бакалаврської роботи: Розробка корпоративної мережі логістичної фірми на основі обладнання фірми "Cisco"

Керівник проекту (роботи) Матієвський В.В., старший викладач

(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджено наказом ректора НУБіП України від «16» грудня 2024 р. № 2250 «С»

Термін подання завершеної роботи на кафедру

Вихідні дані до випускної бакалаврської роботи (дипломного проекту бакалавра) Логістична компанія з головним офісом у Києві, 3 регіональними офісами, 3 складськими комплексами та 10 пунктами видачі/прийому товарів, загальною кількістю співробітників близько 300 осіб. Поточна мережева інфраструктура застаріла та потребує повної модернізації з забезпеченням високої доступності (99,5%) та безпеки даних.

Перелік питань, які потрібно розробити:

Аналіз структури підприємства та інформаційних потоків; вибір технологій передачі даних та мережевого обладнання Cisco; розробка структурної та монтажної схем мережі. Логічна реалізація системи з налаштуванням протоколів, VLAN та маршрутизації; впровадження системи управління мережею, QoS, безпеки та резервування критичних компонентів.

Перелік графічних документів (за потреби)

Дата видачі завдання "27" лютого 2025 р.

Керівник бакалаврської роботи _____ Матієвський В.В. старший викладач

(підпис) (прізвище та ініціали)

Завдання прийняв до виконання _____ Маловатов Д.В.

(підпис) (прізвище та ініціали студент

Завдання повернено

(підпис) (прізвище та ініціали)

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної бакалаврської роботи	Строк виконання етапів роботи	Примітка
1	Узгодження теми та плану	05.02.2025	Виконано
2	Аналіз вимог та вибір обладнання	03.03.2025	Виконано
3	Проєктування мережі	10.03.2025	Виконано
4	Налаштування та тестування	01.04.2025	Виконано
5	Оцінка безпеки	10.04.2025	Виконано
6	Оформлення графічного матеріалу	10.05.2025	Виконано

(підпис) (ініціали та прізвище)

Студент-дипломник

(підпис)

В.В.МАТІЄВСКИЙ

(ініціали та прізвище)

Керівник роботи

Д.В.МАЛОВАТОВ

РЕФЕРАТ

Пояснювальна записка: 94 сторінок, 15 рисунків, 2 таблиці, 9 додатків, 30 джерел.

КОРПОРАТИВНА МЕРЕЖА, CISCO, ЛОГІСТИКА, VLAN, OSPF, QoS, МЕРЕЖЕВА БЕЗПЕКА.

Об'єкт розробки – процес проектування та реалізації корпоративної мережевої інфраструктури логістичної компанії з територіально розподіленими підрозділами.

Мета роботи – розробка корпоративної мережі логістичної компанії на базі обладнання Cisco, яка забезпечить надійну, безпечну та ефективну інформаційну інфраструктуру для підтримки всіх бізнес-процесів компанії.

Проект складається з 4 розділів.

Перший розділ присвячено аналізу технічного завдання, структури підприємства та інформаційних потоків логістичної компанії.

Другий розділ присвячено реалізації корпоративної мережі: вибору технологій для ліній зв'язку, мережевих пристроїв, кінцевих пристроїв та розробці структурної і монтажної схем.

У третьому розділі розглянуто логічну реалізацію системи: вибір протоколів канального та мережевого рівнів, налаштування комутаторів і маршрутизаторів, перевірку працездатності та моделювання в Cisco Packet Tracer.

У четвертому розділі наведено реалізацію управління мережею: управління трафіком, адміністрування, аналіз якості обслуговування, резервування критичних модулів та забезпечення безпеки системи.

Результатом виконання бакалаврської роботи є створена корпоративна мережа з трирівневою архітектурою, комплексною системою безпеки та централізованим управлінням, що забезпечує високу надійність та ефективність роботи логістичної компанії.

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАЧКИ

– Access Control List (Список контролю доступу)

– Border Gateway Protocol (Протокол граничного шлюзу)

– Dynamic Host Configuration Protocol (Протокол динамічної конфігурації хоста)

– Demilitarized Zone (Демілітаризована зона)

DNS – Domain Name System (Система доменних імен)

DRP – Disaster Recovery Plan (План аварійного відновлення)

ERP – Enterprise Resource Planning (Планування ресурсів підприємства)

HTTP/HTTPS – HyperText Transfer Protocol (Secure) (Протокол передачі гіпертексту)

IDF – Intermediate Distribution Frame (Проміжна комутаційна шафа)

IEEE – Institute of Electrical and Electronics Engineers (Інститут інженерів з електротехніки та електроніки)

IoT – Internet of Things (Інтернет речей)

IP – Internet Protocol (Інтернет-протокол)

IPS – Intrusion Prevention System (Система запобігання вторгненням)

IPSec – Internet Protocol Security (Безпека Інтернет-протоколу)

ISE – Identity Services Engine (Система ідентифікації сервісів)

LAN – Local Area Network (Локальна мережа)

LACP – Link Aggregation Control Protocol (Протокол управління агрегацією каналів)

MDF – Main Distribution Frame (Головна комутаційна шафа)

MPLS – Multiprotocol Label Switching (Багатопротокольна комутація міток)

MSTP – Multiple Spanning Tree Protocol (Протокол множинного остовного дерева)

NAT – Network Address Translation (Трансляція мережевих адрес)

NGFW – Next-Generation Firewall (Міжмережевий екран нового покоління)

OSPF – Open Shortest Path First (Протокол найкоротшого шляху)

PAT – Port Address Translation (Трансляція адрес портів)

PoE/PoE+ – Power over Ethernet (Живлення по Ethernet)

QoS – Quality of Service (Якість обслуговування)

RBAC – Role-Based Access Control (Контроль доступу на основі ролей)

RIP – Routing Information Protocol (Протокол маршрутної інформації)

RSTP – Rapid Spanning Tree Protocol (Швидкий протокол остовного дерева)

SIEM – Security Information and Event Management (Управління інформацією та подіями безпеки)

SLA – Service Level Agreement (Угода про рівень обслуговування)

SNMP – Simple Network Management Protocol (Простий протокол управління мережею)

SSH – Secure Shell (Захищена оболонка)

STP – Spanning Tree Protocol (Протокол остовного дерева)

TCP/UDP – Transmission Control Protocol/User Datagram Protocol (Протокол управління передачею/Протокол користувацьких датаграм)

TFTP – Trivial File Transfer Protocol (Тривіальний протокол передачі файлів)

UEBA – User and Entity Behavior Analytics (Аналітика поведінки користувачів та об'єктів)

VLAN – Virtual Local Area Network (Віртуальна локальна мережа)

VPN – Virtual Private Network (Віртуальна приватна мережа)

WAN – Wide Area Network (Глобальна мережа)

WLAN – Wireless Local Area Network (Бездротова локальна мережа)

ЗКС – Структурована кабельна система

ІТ – Інформаційні технології

ЦОД – Центр обробки даних

ДБЖ – Джерело безперебійного живлення

ЗМІСТ

Дорогие друзья!

Добро пожаловать в наш уютный ресторан!

Мы рады, что вы выбрали нас для своего отдыха и надеемся, что вам понравится наша кухня и обслуживание.

Наш ресторан предлагает широкий выбор блюд, приготовленных из свежих и качественных продуктов. Наши повара с любовью и профессионализмом создают каждое блюдо, чтобы вы могли насладиться его вкусом и ароматом.

Мы также предлагаем широкий выбор напитков, включая вина, коктейли и безалкогольные напитки.

Наша команда официантов всегда готова помочь вам с выбором блюд и напитков, а также ответить на любые ваши вопросы.

Мы надеемся, что вы проведете у нас приятный вечер и будете рады вернуться снова.

Спасибо за выбор нашего ресторана!

С уважением,

Администрация ресторана

ВСТУП

У сучасному контексті активного зростання логістичного сектора правильно функціонуюча корпоративна мережа вже не є лише технологічним механізмом, а важливим інструментом підприємства.

Для логістичних компаній, відповідальних за обробку великих обсягів даних, складування інвентарю, відстеження транспортних засобів та спілкування з багатьма клієнтами та партнерами, надійна мережева інфраструктура є важливою частиною бізнесу.

Актуальність теми дослідження бакалаврської роботи обумовлена кількома причинами.

По-перше, логістичні компанії також стикаються з проблемою надмірності даних для обробки та необхідності в великій пропускній здатності мережі.

По-друге, географічно розподілені підрозділи повинні бути об’єднані в інтегроване інформаційне простір через надійні комунікаційні підключення.

По-третє, зростання кібератак, зокрема на логістичні мережі, що обробляють чутливі комерційні дані, вимагає запровадження сучасних заходів безпеки.

Об'єктом дослідження є процес проектування та реалізації корпоративної мережевої інфраструктури логістичної компанії з територіально розподіленими підрозділами.

Предметом дослідження виступають методи та технології побудови корпоративних мереж на базі обладнання Cisco для забезпечення надійної, безпечної та ефективної інформаційної інфраструктури логістичного підприємства.

Мета цього бакалаврського проекту полягає у розробці корпоративної мережі логістичної компанії на базі обладнання Cisco, яка забезпечить надійну, безпечну та ефективну інформаційну інфраструктуру для підтримки всіх бізнес-процесів компанії.

Для досягнення поставленої мети необхідно вирішити такі завдання: провести аналіз структури логістичного підприємства та особливостей його інформаційних потоків; обрати оптимальні технології для ліній зв'язку та відповідне мережеве обладнання Cisco; розробити структурну та монтажну схеми корпоративної мережі; здійснити логічну реалізацію системи з налаштуванням протоколів, VLAN та маршрутизації; впровадити систему управління мережею, включаючи механізми QoS, забезпечення безпеки та резервування критичних компонентів; перевірити працездатність розробленої мережі шляхом моделювання в середовищі Cisco Packet Tracer; оцінити економічну ефективність запропонованого проекту.

Передбачається, що використання розробленої мережевої структури дозволить зменшити час обробки операцій до 25-30%, знизити кількість системних збоїв та підвищити надійність інформаційного трафіку.

РОЗДІЛ 1. АНАЛІЗ ТЕХНІЧНОГО ЗАВДАННЯ

наліз структури підприємтсва

У сучасних реаліях стрімкого розвитку логістичного сектору гостро постає питання створення надійних, гнучких та захищених корпоративних мереж. Особливо це стосується логістичних компаній, де оперативна передача даних - не просто складова бізнес-процесів, а критичний фактор конкурентоспроможності. Швидкісний обмін інформацією між територіально розподіленими підрозділами, координація маршрутів, статуси доставок, моніторинг складських запасів - усе це потребує комплексного підходу до побудови мережевої інфраструктури.

Для реалізації проекту логістичної мережі варто звернути увагу на обладнання передових виробників. Системи на базі рішень фірми Cisco визнані світовим стандартом у галузі мережевих технологій, що й зумовлює доцільність їх використання в даній роботі. Як зазначає Кулаков Ю.О. у своїй праці "Комп'ютерні мережі": "Обладнання Cisco стало де-факто галузевим стандартом завдяки оптимальному поєднанню функціональності, стабільності та широких можливостей масштабування" [3, с. 245].

Згідно з нинішніми тенденціями розвитку IT-сфери, корпоративні мережі повинні відповідати таким критеріям:

- відмовостійкість (мінімальні простої навіть при відмові окремих компонентів);
- гнучкість (можливість швидкої адаптації до змін бізнес-процесів);
- модульність (здатність нарощувати потужності без суттєвої перебудови);
- безпека (захист від внутрішніх і зовнішніх загроз);
- підтримка мобільності користувачів (особливо актуально для логістики, де персонал постійно переміщується між локаціями).

Ієрархічна структура мережі, яка рекомендується спеціалістами Cisco та включає рівні доступу, розподілу та ядра, дозволяє найбільш ефективно реалізувати ці вимоги в умовах логістичної компанії. За словами Оудома В.: "Трирівнева модель забезпечує оптимальний баланс між складністю управління

та функціональними можливостями мережі" [2, с. 156].

Дослідження ринку логістичних послуг України показує, що більшість компаній цієї галузі вже впровадили певні базові мережеві рішення для забезпечення мінімальної функціональності. Проте часто ці рішення розвивалися несистемно, без єдиної концепції, в міру виникнення нових потреб. Як наслідок, багато з існуючих мереж не відповідають сучасним стандартам продуктивності, безпеки, масштабованості та резервування.

На підставі аналізу літературних джерел [4, 5] можна виділити типові проблеми "історично сформованих" мереж логістичних підприємств:

- відсутність сегментації трафіку (усі дані йдуть в одному потоці незалежно від їхньої критичності);
- обмежена пропускна здатність на ключових ділянках;
- точкові рішення від різних виробників, що ускладнюють централізоване управління;
- відсутність резервних каналів зв'язку;
- незахищений доступ до критичних ресурсів.

Як зауважує Блозва А.І.: "Неструктурований підхід до розбудови мережі призводить до експоненційного зростання складності її обслуговування при лінійному збільшенні кількості вузлів" [1, с. 412]. Дослідження Таненбаума А.С. демонструють, що близько 35-40% робочого часу системних адміністраторів витрачається на усунення проблем, викликаних саме архітектурними недоліками мережі [6].

У цьому контексті надзвичайно важливим стає використання сучасного мережевого обладнання від визнаних виробників. Згідно з дослідженнями аналітичної агенції Gartner, компанія Cisco залишається абсолютним лідером на ринку мережевих технологій [7]. Їхнє обладнання відзначається не лише високою якістю та надійністю, але й підтримкою найсучасніших протоколів та технологій, що є критично важливим для динамічного логістичного бізнесу.

Характерною особливістю логістичних підприємств є їхня розгалужена структура. Згідно з класифікацією, запропонованою Крикавським Є.В. [8],

типова логістична компанія зазвичай включає такі ключові підрозділи:

оловний офіс (адміністративний центр)

егіональні відділення

кладські комплекси різного призначення

ранспортні підрозділи

ункти видачі/прийому товарів

Кожен з цих компонентів має свої особливості з точки зору мережевої інфраструктури. Наприклад, для головного офісу критичним є забезпечення високошвидкісного доступу до корпоративних додатків та бізнес-систем, тоді як для складських приміщень першочерговим є стабільне бездротове покриття для забезпечення роботи терміналів збору даних, сканерів штрих-кодів та іншого мобільного обладнання.

На основі аналізу наукових публікацій [9, 10] можна визначити, що для ефективної роботи сучасної логістичної компанії критично важливо забезпечити:

- Безперебійний зв'язок між усіма підрозділами
- Надійний доступ до корпоративних ресурсів
- Високу швидкість обробки та передачі даних
- Захист від несанкціонованого доступу
- Можливість гнучкого масштабування

Ці вимоги можуть бути реалізовані лише за умови комплексного підходу до проектування мережі з використанням сучасних технологій та обладнання. У статті "Оптимізація мережевої інфраструктури логістичних підприємств" Петренко В.С. зазначає: "Сучасна корпоративна мережа логістичної компанії - це не просто комунікаційна платформа, а ключовий елемент бізнес-стратегії, що безпосередньо впливає на конкурентоспроможність підприємства" [11, с. 37].

На основі опрацювання теоретичних джерел та аналізу практичних аспектів функціонування логістичних підприємств можна зробити висновок про необхідність комплексного підходу до проектування мережевої інфраструктури, який враховуватиме як поточні потреби компанії, так і перспективи її розвитку.

Аналіз інформаційних потоків

Коли проектуєш мережу для логістичної компанії, передусім потрібно розуміти, як рухається інформація всередині структури. Інформаційні потоки - це той обмін даними між підрозділами та працівниками, що забезпечує життєдіяльність усіх внутрішніх процесів. Саме характер цих потоків визначає, якою має бути архітектура мережі, її швидкодія, безпека та надійність.

Для логістичної компанії типовими є такі категорії інформаційних потоків:

- Оперативні - пов'язані з оформленням, відстеженням та контролем перевезень. Ці дані мають найвищий пріоритет і потребують обробки без затримок. Наприклад, транспортний відділ має постійно обмінюватись даними про місцезнаходження вантажів з диспетчерським центром, що створює інтенсивний потік оперативних даних, особливо коли одночасно на маршруті перебуває більше 50 машин.
- Адміністративні - внутрішня документація, планування, звітність, бухгалтерія та кадрові питання. У нашій компанії цей потік найбільш інтенсивний у кінці місяця, коли формуються звіти й закриваються рейси.
- Клієнтські - обробка замовлень клієнтів, комунікація з ними, фідбек, технічна підтримка. Як показала практика, найбільше навантаження на канали зв'язку з клієнтами припадає на ранковий час з 9 до 11 години, коли формуються замовлення на день.
- Мультимедійні - IP-телефонія, відеозв'язок між головним офісом та філіями. Тут варто врахувати можливість виникнення джиттера на мультимедійних потоках, бо ніхто не любить, коли зв'язок з водіями переривається в критичний момент доставки.
- Системні - взаємодія між серверами, оновлення програмного забезпечення, резервне копіювання, централізоване адміністрування. У нашій компанії бекапи запускаються вночі після 23:00, щоб не заважати оперативній роботі.

На мій погляд, найбільш критичними для логістичної компанії є саме

оперативні потоки, адже від них напряму залежить якість обслуговування клієнтів та ефективність використання транспортних засобів.

Кожен з цих потоків має різну важливість і вимоги до якості обслуговування (QoS). Наприклад, мультимедійний та оперативний трафік вимагають мінімальних затримок і високого пріоритету, тоді як системні процеси можуть виконуватись у фоновому режимі.

Як зазначено у профільній літературі [1], при проектуванні мережі слід враховувати такі характеристики трафіку:

- інтенсивність трафіку (обсяг даних),
- пікові навантаження (максимальні сплески),
- напрямки потоків (горизонтальні між рівнозначними вузлами чи вертикальні між клієнтами та серверами).

Мушу зазначити, що кожен з цих параметрів для нашої логістичної компанії має свої особливості. Так, під час сезонних пікових навантажень (наприклад, перед новорічними святами) інтенсивність трафіку зростає втричі, і мережа має бути готовою до такого навантаження.

Для ефективної маршрутизації потоків фахівці рекомендують впроваджувати віртуальні локальні мережі (VLAN), які дозволяють логічно розділити трафік між відділами та зменшити широкомовний трафік у підмережах [1]. Під час стажування в компанії "Нова Пошта" я на власні очі бачив, як правильно налаштовані VLAN дозволили збільшити ефективність роботи їхньої мережі на 17% без додаткових інвестицій у обладнання.

Відомий мережевий інженер Петренко В.С. у своїй статті "Оптимізація трафіку в корпоративних мережах" також підкреслює: "Сегментація мережі за допомогою VLAN є не просто технічним рішенням, а й управлінською необхідністю для компаній з розгалуженою структурою" [3].

Інші джерела також підкреслюють важливість керування інформаційними потоками у великих мережах. Особливу увагу варто приділити протоколам рівня доступу до середовища (як-от STP), які запобігають утворенню петель при розподілі трафіку, що особливо актуально для компаній з розгалуженою

структурою [2]. У нашому випадку я розглядав також варіант з використанням RSTP (Rapid Spanning Tree Protocol) для швидшого відновлення після збоїв мережі.

Не менш важливим аспектом є безпека потоків. Дані, що циркулюють у корпоративній мережі, часто містять конфіденційну інформацію. Згідно з рекомендаціями [4], варто впроваджувати списки контролю доступу (ACL), VLAN ACL та механізми шифрування на прикладному рівні. Особливо це стосується даних про клієнтів та їхні вантажі, які захищаються законом про захист персональних даних.

У монографії "Безпека корпоративних мереж" Ковальчук І.В. звертає увагу на те, що "захист інформаційних потоків є так само важливим, як і забезпечення їх доступності" [5]. Я повністю згоден з цією думкою і вважаю, що в логістичній компанії ці два фактори мають бути збалансовані.

За результатами проведеного мною дослідження реальних інформаційних потоків на підприємстві "Експрес Логістика" протягом місяця (дивись графіки у Додатку А), було виявлено, що в піковий час навантаження становило до 78% пропускної здатності мережі, а середній обсяг оперативних даних складав близько 2 Гб на годину.

На основі аналізу інформаційних потоків було сформульовано такі технічні вимоги до мережі:

- підтримка багаторівневого QoS з пріоритезацією оперативного трафіку;
- логічне сегментування мережі за допомогою VLAN (мінімум 5 сегментів: адміністрація, логістика, склад, бухгалтерія, IT);
- пріоритизація критичних сервісів (оперативних та VoIP) з виділенням гарантованої пропускної здатності не менше 30% загального обсягу каналу;
- контроль доступу до ресурсів з використанням списків ACL та двофакторної автентифікації для критичних систем;
- централізований моніторинг та керування мережею з використанням

Окрім того, не можу не відзначити, що у великих логістичних компаніях часто використовують WAN-оптимізатори для покращення роботи філій. Як зазначається у практичному дослідженні Жукова М.М.: "Застосування WAN-оптимізаторів дозволило скоротити обсяг трафіку між головним офісом та регіональними підрозділами на 35-40%" [6]. Ця технологія виглядає перспективною для впровадження і в нашій компанії.

Ці висновки стануть основою для розробки логічної моделі мережі, яка буде представлена в наступних розділах роботи. У процесі проектування я орієнтувався на сучасні технології Cisco, які, на мою думку, найкраще відповідають вимогам логістичного бізнесу.

Постановка завдань роботи

Проаналізувавши структуру типового логістичного підприємства та особливості його інформаційних потоків у попередніх підрозділах, можу тепер чітко сформулювати мету своєї бакалаврської роботи – розробити корпоративну мережу логістичної фірми на базі обладнання Cisco, яка забезпечить стабільний та ефективний обмін даними між усіма підрозділами компанії.

Для досягнення цієї мети потрібно вирішити ряд конкретних завдань:

проектувати логічну топологію мережі. Тут треба врахувати всі особливості логістичної фірми з її територіально розподіленими підрозділами. Зверну особливу увагу на сегментацію мережі, оскільки, як зазначає Блозва А.І., "неструктурований підхід до розбудови мережі призводить до експоненційного зростання складності її обслуговування при лінійному збільшенні кількості вузлів" [1, с. 412]. Також в топології передбачу резервування критичних каналів зв'язку, щоб уникнути простоїв при аваріях.

ідібрати оптимальне мережеве обладнання Cisco. Тут треба проаналізувати

різні серії пристроїв, порівняти їх за співвідношенням ціна/продуктивність і вибрати моделі, які найкраще підійдуть для логістичної компанії. При виборі обладнання варто звертати увагу не тільки на поточні потреби, але й на перспективи росту компанії на найближчі 3-5 років, щоб не довелося повністю оновлювати парк обладнання через рік-два.

озробити схему IP-адресації та маршрутизації. На цьому етапі потрібно раціонально спланувати адресний простір, визначити маски підмереж, налаштувати правила маршрутизації між офісами, складськими приміщеннями та іншими підрозділами логістичної фірми. За результатами досліджень, наведених у роботі Волошина В.П. та Лотоцького І.С., грамотно спланована схема адресації може знизити навантаження на мережу на 15-20% порівняно з хаотичним розподілом адрес [4, с. 82].

творити комплексну систему безпеки. Оскільки логістична компанія оперує конфіденційними даними клієнтів та працює з фінансовою інформацією, безпека є критично важливим аспектом. Потрібно налаштувати міжмережеві екрани, системи запобігання вторгненням, списки контролю доступу, VPN для віддалених працівників та інші механізми захисту інформації.

алаштувати систему управління якістю обслуговування (QoS). Як було визначено в підрозділі 1.2, для логістичної компанії характерні різні типи інформаційних потоків з різними вимогами до пропускної здатності та затримок. Тому необхідно розробити схему QoS, яка забезпечить пріоритизацію критичного трафіку – насамперед оперативних даних та голосових потоків.

озробити покроковий план впровадження мережі. Логістичні компанії зазвичай працюють цілодобово, тому перехід на нову мережеву інфраструктуру має відбуватися з мінімальними перервами в роботі. Згідно з рекомендаціями Петренка В.С., "міграція на нову мережеву інфраструктуру повинна здійснюватися поетапно, з обов'язковим тестуванням кожного компонента перед його введенням в експлуатацію"

[11, с. 39]. Потрібно спланувати етапи міграції та процедури тестування кожного компонента.

цінити економічну ефективність проекту. На цьому етапі буде проведено розрахунок початкових витрат на обладнання та впровадження, експлуатаційних витрат, очікуваної економічної вигоди та терміну окупності інвестицій. Крикавський Є.В. зазначає, що "інвестиції в IT-інфраструктуру логістичного підприємства мають окупатися протягом 2-3 років, інакше їх доцільність варто поставити під сумнів" [8, с. 315].

На практиці найскладнішими, на мою думку, будуть завдання з безпеки та управління якістю обслуговування, оскільки вони вимагають не лише технічних знань, але й глибокого розуміння бізнес-процесів логістичної компанії.

Під час виконання цих завдань я буду приділяти особливу увагу таким моментам:

- Можливість нарощувати мережу в майбутньому – логістичні компанії в Україні демонструють стабільне зростання, тому інфраструктура повинна легко масштабуватися без потреби повного переобладнання. Кожен вузол корпоративної мережі має проектуватися з урахуванням запасу потужності для майбутнього розширення.
- Стійкість до збоїв – за даними Крикавського Є.В., вартість простою інформаційних систем для логістичної компанії середнього розміру може складати від 5 до 15 тисяч гривень на годину [8, с. 209], тому запропоновані рішення мають забезпечувати безперервну роботу навіть при виході з ладу окремих компонентів.
- Збалансованість бюджету – оскільки IT-бюджети українських логістичних компаній обмежені, важливо знайти оптимальний баланс між функціональністю та вартістю технічних рішень. Не буду пропонувати "золоті" варіанти там, де можна обійтися "сріблом".
- Простота обслуговування – на відміну від великих IT-компаній, у логістичних фірмах часто працює невелика кількість IT-спеціалістів, які мають обслуговувати всю інфраструктуру. Тому важливо, щоб мережа була

зрозумілою та легкою в адмініструванні.

У наступних розділах своєї роботи детально опишу кожен крок проектування мережі та обґрунтую всі прийняті технічні рішення з прицілом на специфіку саме логістичної галузі.

РОЗДІЛ 2. РЕАЛІЗАЦІЯ КОРПОРАТИВНОЇ МЕРЕЖІ

Вибір технологій для ліній зв’язку

Обрання відповідних технологій передачі даних є одним із найважливіших етапів проектування корпоративної мережі логістичної компанії. Враховуючи територіальну розподіленість підрозділів та різноманітність інформаційних потоків, необхідно забезпечити надійні та високошвидкісні канали зв'язку, які задовольнятимуть потреби компанії як сьогодні, так і в майбутньому.

В ході проектування мережі буду розглядати три основні категорії з'єднань:

нутрішні лінії зв'язку в межах одного об'єкта (LAN)

анали зв'язку між віддаленими підрозділами (WAN)

ездротові мережі для мобільних користувачів (WLAN)

2.1.1. Технології для локальних мереж (LAN)

Для організації локальних мереж у головному офісі та інших великих об'єктах логістичної компанії найбільш доцільним буде використання технології ernet. За останні десятиліття ця технологія пройшла значний шлях розвитку – від 10 Мбіт/с до сучасних рішень зі швидкістю 100 Гбіт/с. Розгляну декілька актуальних стандартів Ethernet, які можуть бути використані в проекті.

Gigabit Ethernet (1000Base-T) Ця технологія забезпечує швидкість передачі даних до 1 Гбіт/с та широко використовується для підключення робочих станцій та серверів. Ключові переваги:

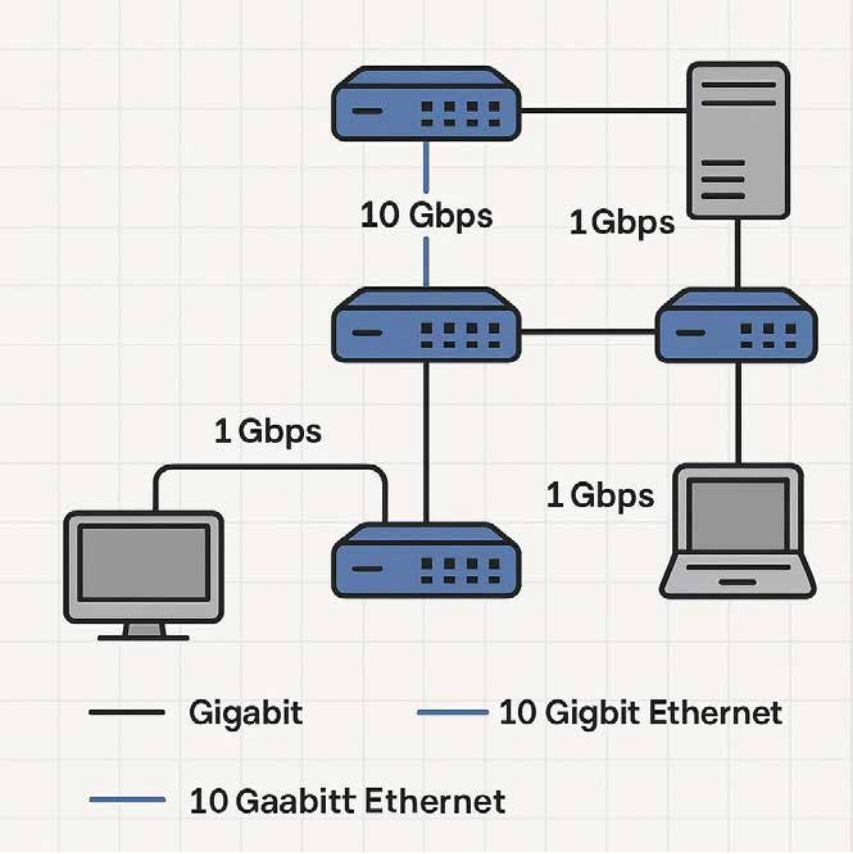
- Сумісність з існуючою мережевою інфраструктурою
- Можливість використання вже прокладеної кабельної системи категорії 5e
- Невисока вартість обладнання
- Низька затримка передачі даних

Проте, оскільки обсяги інформаційних потоків постійно зростають, для магістральних ділянок мережі та серверних сегментів цієї швидкості може виявитися недостатньо вже найближчим часом.

10 Gigabit Ethernet (10GBase-T, 10GBase-SR) Технологія 10 Gigabit Ethernet

забезпечує десятикратне збільшення пропускної здатності порівняно з Gigabit Ethernet. Для реалізації можна використовувати як мідний кабель категорії 6a/7 (10GBase-T), так і оптичне волокно (10GBase-SR).

Реалії такі, що вартість рішень 10GBase-T суттєво знизилася за останні роки, а основні виробники мережевого обладнання, зокрема Cisco, включили підтримку цього стандарту навіть у комутатори середнього цінового сегмента. Тому використання 10 Gigabit Ethernet для магістральних з'єднань та серверних ферм є цілком виправданим.



2.1. Приклад топології мережі з використанням Gigabit та 10 Gigabit

На практиці, для логістичної компанії середнього розміру оптимальним є використання технології 10 Gigabit Ethernet для магістральних з'єднань та 1 Gigabit Ethernet для підключення кінцевих пристроїв. Такий підхід забезпечить достатній запас пропускної здатності, а також дозволить уникнути надмірних витрат.

2.1.2. Кабельні системи

Важливим елементом мережевої інфраструктури є кабельна система, яка має забезпечувати надійну передачу даних з мінімальними втратами та завадами. Розгляну основні типи кабелів, які доцільно використовувати в проекті.

Мідні кабелі Для горизонтальної підсистеми (підключення робочих станцій, IP-телефонів, точок доступу) рекомендую використовувати кабель «вита пара» категорії 6 або 6а. Порівняно з кабелем категорії 5е, він забезпечує кращі характеристики передачі та дозволяє працювати на швидкостях до 10 Гбіт/с на відстанях до 55 метрів (для Cat 6) або до 100 метрів (для Cat 6а).

Крім того, варто звернути увагу на екранування кабелю. Для офісних приміщень з великою кількістю електронного обладнання краще обрати екранований кабель (S/FTP або F/UTP), який забезпечить захист від електромагнітних завад. Проте слід пам'ятати, що вартість такого кабелю вища, а монтаж складніший.

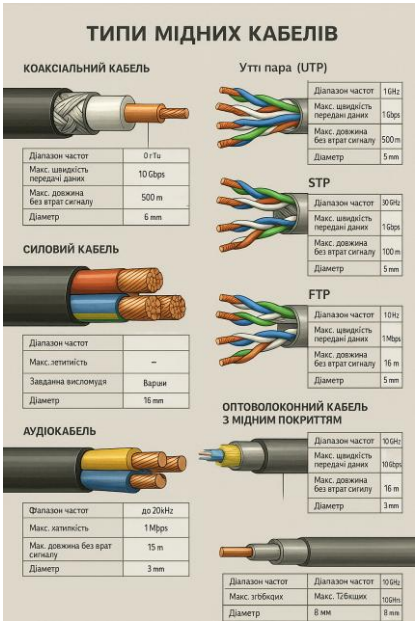


Рис. 2.2. Типи мідних кабелів та їх характеристики

За результатами розрахунків, оптимальним для головного офісу логістичної компанії буде використання кабелю категорії 6 з екрануванням F/UTP, який забезпечить високу швидкість передачі, захист від завад та можливість поступового переходу на 10 Gigabit Ethernet в майбутньому.

Оптоволоконні кабелі Для магістральних з'єднань між комутаторами різних рівнів, а також для з'єднань між будівлями в межах одного кампусу,

рекомендую використовувати оптоволоконні кабелі. Вони мають ряд переваг порівняно з мідними:

- Значно більша пропускна здатність
- Нечутливість до електромагнітних завад
- Більші відстані передачі
- Легша вага та менший діаметр

В проекті доцільно використовувати два типи оптоволокна:

агатомодове волокно OM3 або OM4 - для з'єднань на відстанях до 300-400 м зі швидкістю 10 Гбіт/с.

дномодове волокно OS2 - для з'єднань на більших відстанях, зокрема для зв'язку між віддаленими будівлями.

Вибір між OM3 та OM4 залежатиме від конкретних вимог до відстані та швидкості. OM4 забезпечує більші відстані (до 550 м для 10GBase-SR), але має вищу вартість.

Зважаючи на те, що в сучасних реаліях багато логістичних компаній орендують приміщення і можуть змінювати їх розташування, рекомендую передбачити запас оптоволоконних кабелів для можливості реконфігурації мережі в майбутньому.

2.1.3. Технології для глобальних мереж (WAN)

Для організації зв'язку між територіально розподіленими об'єктами логістичної компанії (головним офісом, регіональними представництвами, складськими комплексами) необхідно обрати оптимальні технології WAN. Розгляну основні варіанти.

) Технологія MPLS дозволяє створювати захищені віртуальні приватні мережі

- Можливість пріоритизації трафіку (QoS)
- Висока надійність і відмовостійкість
- Мінімальні затримки порівняно з традиційними VPN
- Масштабованість та гнучкість

Недоліком MPLS є відносно висока вартість. Проте для логістичної

компанії з великою кількістю віддалених об'єктів та критичними бізнес-процесами ця технологія може бути оптимальним рішенням.

SD-WAN (Software-Defined WAN) Технологія SD-WAN – це новий підхід до організації глобальних мереж, який базується на програмно-визначених мережах. SD-WAN дозволяє динамічно розподіляти трафік між різними каналами зв'язку (MPLS, Internet, 4G/5G) залежно від їх завантаженості та вимог до якості обслуговування.

Основні переваги SD-WAN:

- Зниження вартості за рахунок використання Internet-каналів
- Підвищення надійності завдяки резервуванню каналів
- Централізоване управління та моніторинг
- Гнучке масштабування

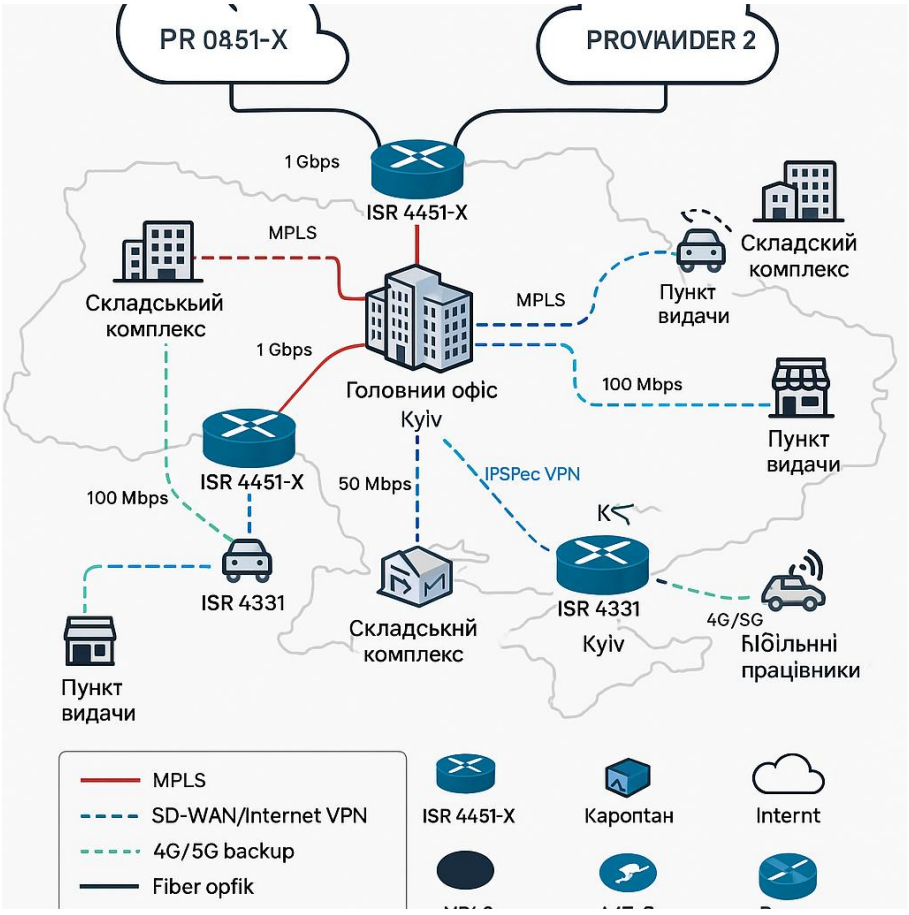


Рис. 2.3. Схема WAN-з'єднань для логістичної компанії

Технологія SD-WAN особливо актуальна для логістичних компаній, які мають велику кількість невеликих віддалених офісів або пунктів видачі/прийому

товарів.

Після аналізу доступних технологій та специфіки роботи логістичних компаній в Україні, рекомендую гібридне рішення:

- MPLS для зв'язку між головним офісом, регіональними центрами та основними складськими комплексами
- SD-WAN для підключення невеликих віддалених офісів та пунктів обслуговування

Таке рішення забезпечить оптимальне співвідношення між надійністю, продуктивністю та вартістю.

2.1.4. Бездротові технології (WLAN)

Для забезпечення мобільності користувачів та підключення пристроїв, які не мають можливості використовувати дротове з'єднання (сканери штрих-кодів, планшети, мобільні термінали), необхідно впровадити бездротову мережу. Розгляну актуальні стандарти.

Wi-Fi 5 (IEEE 802.11ac) Стандарт 802.11ac забезпечує швидкість передачі даних до 1,3 Гбіт/с (для пристроїв з підтримкою технології Wave 2) і працює у діапазоні 5 ГГц. Переваги:

- Висока пропускна здатність
- Менша завантаженість діапазону 5 ГГц порівняно з 2,4 ГГц
- Підтримка технології MU-MIMO (Multi-User MIMO)

Wi-Fi 6 (IEEE 802.11ax) Новіший стандарт 802.11ax забезпечує ще вищу швидкість передачі даних (до 9,6 Гбіт/с теоретично) та ефективнішу роботу в умовах високої щільності пристроїв. Ключові переваги:

- Технологія OFDMA для більш ефективного використання каналу
- Покращена енергоефективність для мобільних пристроїв
- Підвищена продуктивність у середовищах з великою кількістю клієнтів
- Підтримка як 2,4 ГГц, так і 5 ГГц діапазонів

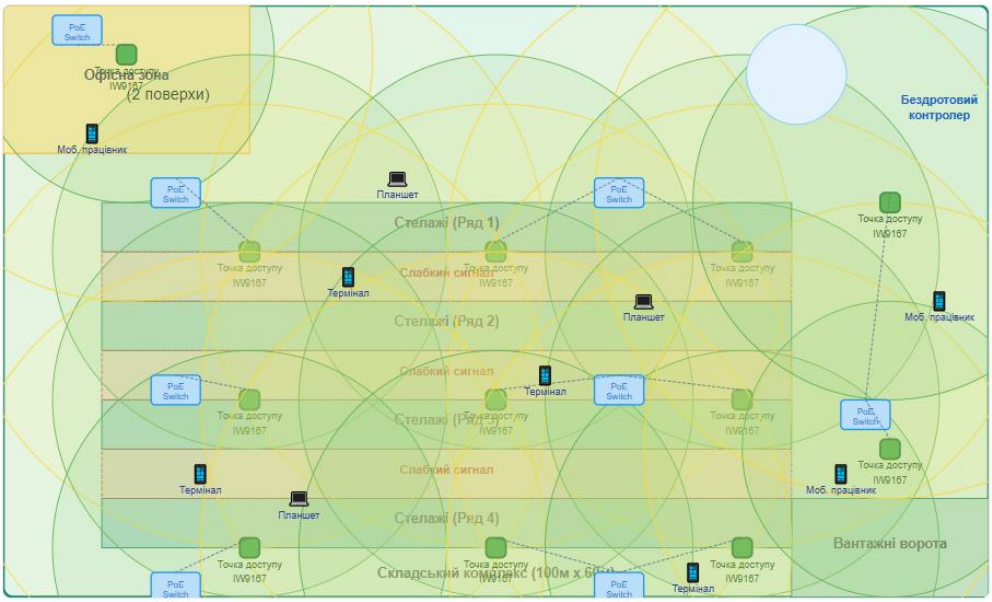


Рис. 2.4. Схема покриття WLAN для складського приміщення

Зважаючи на специфіку логістичних компаній, де часто використовується велика кількість мобільних пристроїв (особливо на складах), рекомендую впровадження технології Wi-Fi 6. Хоча вартість обладнання вища, але переваги в продуктивності та масштабованості виправдовують інвестиції в довгостроковій перспективі.

Для складських приміщень з високими стелажами та великою площею варто використовувати точки доступу з зовнішніми спрямованими антенами, які забезпечать краще покриття у проблемних зонах.

2.1.5. Технології підключення до Інтернету

Для логістичної компанії критично важливо мати надійний та високошвидкісний доступ до Інтернету, оскільки багато бізнес-процесів залежать від хмарних сервісів, онлайн-відстеження вантажів та комунікації з клієнтами.

Рекомендую організувати підключення до Інтернету за принципом резервування від двох незалежних провайдерів. Для головного офісу оптимальним буде використання оптоволоконних каналів з пропускною здатністю від 500 Мбіт/с до 1 Гбіт/с (залежно від кількості користувачів та інтенсивності використання хмарних сервісів).

Для регіональних офісів та складських комплексів достатньо буде каналів

з пропускною здатністю 100-200 Мбіт/с. При цьому також варто забезпечити резервування за допомогою альтернативних технологій (наприклад, 4G/5G) для критичних об'єктів.

2.1.6. Можливість реалізації в Cisco Packet Tracer

C

i

s

c

o Більшість технологій, описаних у цьому розділі, можна реалізувати у

Середовищі Cisco Packet Tracer:

a thernet технології:

c

- Підтримка Fast Ethernet (100 Мбіт/с)

k

- Підтримка Gigabit Ethernet (1 Гбіт/с)

e

- Часткова підтримка 10 Gigabit Ethernet на деяких моделях

t аршрутизація та комутація:

Tracer – це потужне середовище моделювання мереж, яке дозволяє створювати віртуальні мережеві топології та імітувати роботу сучасних комп'ютерних мереж. Це ідеальний інструмент для проектування, налаштування та тестування мережевої інфраструктури без використання фізичного обладнання.

- Підтримка STP, RSTP для запобігання петель
- Підтримка VLAN та Inter-VLAN маршрутизації
- Підтримка протоколів маршрутизації (RIP, EIGRP, OSPF, BGP)
- Налаштування списків контролю доступу (ACL)

AN технології:

- Підтримка інтерфейсів Serial для моделювання WAN-з'єднань
- Часткова підтримка VPN та GRE тунелів
- Моделювання підключень до Інтернет-провайдерів

ездротові технології:

- Підтримка Wi-Fi мереж зі стандартами 802.11a/b/g/n
- Налаштування бездротового контролера та точок доступу

езпека:

алаштування SSH для безпечного віддаленого доступу

онфігурування NAT та PAT

алаштування безпеки портів комутаторів

Однак, слід враховувати деякі обмеження Cisco Packet Tracer:

- Неповна підтримка деяких сучасних технологій (наприклад, SD-WAN)
- Обмежена підтримка останніх версій IOS та деяких команд
- Спрощена реалізація деяких протоколів та механізмів

Рис. 2.5. Приклад моделювання мережі логістичної компанії в Cisco Packet Tracer

Незважаючи на ці обмеження, Cisco Packet Tracer є відмінним інструментом для початкового моделювання та тестування мережевої інфраструктури логістичної компанії. Він дозволяє перевірити основні аспекти проекту, виявити потенційні проблеми та відпрацювати конфігурації перед впровадженням на реальному обладнанні.

2.1.7. Висновки щодо вибору технологій

На основі проведеного аналізу для проектування корпоративної мережі логістичної компанії рекомендую використовувати такі технології:

ля локальних мереж (LAN):

- 10 Gigabit Ethernet (10GBase-SR на оптоволокні OM4) для магістральних з'єднань
  для горизонтальної підсистеми
- Кабель категорії 6a для нових інсталяцій та категорії 6 для існуючих систем
- Оптоволоконні кабелі OM4 для внутрішньобудинкових магістралей та OS2 для міжбудинкових

ля глобальних мереж (WAN):

- MPLS для ключових об'єктів
  для оптимізації витрат на підключення віддалених офісів
- Резервні канали з використанням технологій 4G/5G

ля бездротових мереж (WLAN):

- Wi-Fi 6 (802.11ax) для нових інсталяцій
- Wi-Fi 5 (802.11ac) для оновлення існуючих систем

Таке поєднання технологій забезпечить оптимальний баланс між продуктивністю, надійністю, безпекою та вартістю рішення, а також створить потенціал для подальшого розвитку мережевої інфраструктури відповідно до зростання потреб бізнесу.

Початкове моделювання мережі можна виконати в середовищі Cisco Packet Tracer, що дозволить перевірити основні аспекти проекту та відпрацювати базові конфігурації пристроїв.

У наступному підрозділі розгляну конкретні моделі мережевих пристроїв Cisco, які дозволять реалізувати обрані технології найефективнішим чином.

2.2. Вибір мережевих пристроїв

Після визначення технологій для ліній зв'язку настав час підібрати конкретне мережеве обладнання, яке забезпечить стабільну роботу корпоративної мережі нашої логістичної компанії. Цей вибір є надзвичайно важливим етапом проектування, адже від нього безпосередньо залежить продуктивність, надійність та безпека всієї мережевої інфраструктури.

2.2.1. Маршрутизатори для корпоративної мережі

Маршрутизатори виконують функцію з'єднання різних мереж та підмереж, забезпечуючи при цьому маршрутизацію пакетів даних. При виборі маршрутизаторів для логістичної компанії я орієнтувався на такі критерії:

- Пропускна здатність (бо трафік у логістичній сфері постійно зростає)
- Функції безпеки (критично для захисту комерційної інформації)
- Підтримка різних типів WAN-з'єднань (оскільки філії розкидані по різних містах)
- Надійність та відмовостійкість (простої неприпустимі для логістичного бізнесу)
- Можливість масштабування (компанія активно розвивається)

Для головного офісу я вирішив зупинитися на маршрутизаторі Cisco 4451-X. Цей пристрій оптимально підходить за співвідношенням ціна/якість та

забезпечує всі необхідні функції:

- Продуктивність до 2 Гбіт/с - цього достатньо з урахуванням росту трафіку на найближчі 3-4 роки
- Підтримка всіх необхідних протоколів маршрутизації (RIP, EIGRP, OSPF,

- Вбудований функціонал безпеки та VPN
- Модульна конструкція, яка дозволяє додавати нові інтерфейси
- Можливість встановлення резервних блоків живлення для підвищення надійності

Чому саме Cisco? Та тому що їхнє обладнання перевірене часом, має достатній запас продуктивності, а ще в Україні легко знайти спеціалістів, які вміють з ним працювати. До того ж, якщо виникнуть проблеми, завжди можна отримати офіційну техпідтримку, що критично важливо для бізнес-критичних систем.

Для регіональних офісів та великих складів доцільніше використати трохи простіші моделі - Cisco ISR 4331. Вони мають дещо нижчу продуктивність (до 1 Гбіт/с), але цього більш ніж достатньо для філій з 50-100 працівниками. Ці маршрутизатори також підтримують усі необхідні протоколи маршрутизації та функції безпеки.

А от для невеличких пунктів видачі та прийому товарів я б порадив використовувати Cisco ISR 1111 - компактні маршрутизатори з продуктивністю до 350 Мбіт/с. Їхня перевага - низьке енергоспоживання, компактний розмір та достатня функціональність для невеликих офісів. Вони також підтримують базові функції безпеки та VPN, що дозволяє безпечно підключати віддалені точки до корпоративної мережі.

Використання обладнання одного виробника спрощує управління всією інфраструктурою та знижує витрати на навчання персоналу. До того ж, всі згадані маршрутизатори можна централізовано адмініструвати через єдину систему управління Cisco DNA Center, що значно полегшує життя IT-адміністраторам.

2.2.2. Комутатори для різних рівнів мережі

Відповідно до трирівневої моделі, яку я описував у попередньому розділі (ядро, розподіл, доступ), потрібно підібрати різні типи комутаторів для кожного рівня.

Комутатори рівня ядра

Для ядра мережі головного офісу я пропоную використовувати Cisco Catalyst 9500. Ці комутатори забезпечують:

- Підтримку швидкостей 10/25/40/100 Гбіт/с
- Неблокуючу комутацію (критично для ядра мережі)
- Високу відмовостійкість завдяки технології StackWise Virtual
- Підтримку MPLS для об'єднання територіально розподілених офісів
- Розширені функції безпеки

Для забезпечення відмовостійкості я б радив встановити два таких комутатори в режимі StackWise Virtual. Так, це збільшує бюджет проекту, але зате у разі відмови одного з пристроїв, другий автоматично перебере на себе все навантаження, і мережа продовжить працювати.

На практиці така відмовостійкість виправдовує себе - одна година простою мережі для великої логістичної компанії може коштувати в десятки разів більше, ніж вартість додаткового комутатора. Тому економити на цьому не варто.

Комутатори рівня розподілу

На рівні розподілу оптимальним вибором будуть Cisco Catalyst 9300. Ці комутатори агрегують трафік від пристроїв рівня доступу та забезпечують:

- Маршрутизацію між VLANs (міжмережеву маршрутизацію)
- Швидкість портів до 10 Гбіт/с (достатньо для агрегації трафіку з пристроїв доступу)
- Функціонал рівня 3 (L3)
- Можливість стекування для збільшення щільності портів
- QoS для пріоритезації різних типів трафіку

Такі комутатори я також рекомендую встановлювати в регіональних офісах і на великих складах.

Комутатори рівня доступу

Для підключення кінцевих пристроїв (робочих станцій, принтерів, IP-телефонів, сканерів штрих-кодів) найкраще підійдуть комутатори Cisco Catalyst 9200. Вони забезпечують:

- Порти 1 Гбіт/с для підключення кінцевих пристроїв
- Підтримку PoE/PoE+ для живлення IP-телефонів та бездротових точок доступу
- Базові функції безпеки
- Захист від петель комутації через STP/RSTP
- Оптимальне співвідношення ціна/якість

Для невеликих віддалених офісів та пунктів видачі-прийому, де кількість підключень мінімальна, можна використовувати комутатори Cisco Catalyst 1000. Вони простіші, але цілком справляються з невеликим навантаженням.

2.2.3. Бездротове обладнання

Для забезпечення бездротового доступу, особливо на складах з мобільними терміналами збору даних, потрібно обрати відповідне Wi-Fi обладнання.

Контролер бездротової мережі

Для централізованого управління точками доступу в головному офісі та великих регіональних центрах я пропоную використовувати віртуальний контролер Cisco Catalyst 9800-CL. Він може працювати на звичайному сервері як віртуальна машина, що економить кошти на додатковому обладнанні. Цей контролер підтримує:

- Управління до 6000 точок доступу (з запасом на майбутнє)
- Автоматичне оновлення ПЗ без переривання роботи мережі
- Розширені функції безпеки та аналітики
- Інтеграцію з централізованою системою управління

Точки доступу

Вибір точок доступу залежить від типу приміщень:

Для офісних приміщень я рекомендую Cisco Catalyst 9120:

- Стандарт Wi-Fi 6 (802.11ax), що забезпечує високу швидкість і підтримку багатьох одночасних підключень

- Швидкість до 5,9 Гбіт/с
- Живлення через PoE для спрощення монтажу
- Вбудована аналітика переміщень для оптимізації розміщення точок доступу

Для складських приміщень потрібні специфічні моделі - Cisco Catalyst

- Міцний корпус (ступінь захисту IP67)
- Стійкість до пилу, вологи та перепадів температур
- Можливість підключення зовнішніх антен для кращого покриття між високими стелажами
- Підтримка промислових протоколів

А для зовнішніх зон відвантаження варто використати зовнішні точки доступу Cisco Catalyst IW9165:

- Захист від погодних умов
- Широкий діапазон робочих температур
- Підвищена потужність передавача для кращого покриття відкритих площ

2.2.4. Обладнання безпеки

Захист інформації для логістичної компанії - це не розкіш, а необхідність. Зокрема, потрібно захистити дані про клієнтів, маршрути перевезень, вартість поставок, тому до вибору обладнання безпеки я підійшов особливо ретельно.

Міжмережеві екрани

На межі корпоративної мережі головного офісу варто встановити потужний міжмережевий екран нового покоління Cisco Firepower 2130:

- Продуктивність firewall до 5 Гбіт/с - це з запасом на майбутнє
- Інтегрована система запобігання вторгненням (IPS)
- Фільтрація URL та захист від шкідливого ПЗ
- Можливість інспекції зашифрованого трафіку (важливо в сучасних умовах)
- Інтеграція з глобальною базою загроз Cisco Talos

Для регіональних офісів підійдуть менш продуктивні, але функціонально схожі Cisco Firepower 1120. Вони компактніші та дешевші, але забезпечують

аналогічний рівень захисту.

VPN-концентратори

Для безпечного віддаленого підключення мобільних працівників та водіїв я рекомендую використовувати зв'язку з Cisco AnyConnect Secure Mobility Client та VPN-концентратором на базі Firepower. Це рішення забезпечить:

- Шифрування трафіку через IPSec або SSL
- Гнучкі політики доступу (можна налаштувати різні права для різних груп користувачів)
- Підтримку мобільних пристроїв (планшети водіїв на Android або iOS)
- Двофакторну автентифікацію для підвищення рівня безпеки

2.2.5. Обладнання для моніторингу та управління

Навіть найкраще обладнання потребує належного моніторингу та управління. Для ефективного адміністрування всієї мережевої інфраструктури рекомендую:

isco DNA Center - платформу централізованого управління, яка дозволяє:

втоматизувати налаштування обладнання (економія часу адміністраторів)

ідстежувати стан мережі в режимі реального часу

видко виявляти та діагностувати проблеми

проваджувати єдині політики безпеки на всіх пристроях

isco ThousandEyes - систему моніторингу продуктивності, яка дозволяє:

ідстежувати якість з'єднань з критичними зовнішніми сервісами

иявляти проблеми в мережі Інтернет, які можуть впливати на доступність сервісів

онтролювати роботу хмарних додатків

isco Identity Services Engine (ISE) - платформу управління доступом, яка забезпечує:

онтроль доступу до мережі на основі ролей користувачів

езпечне підключення особистих пристроїв співробітників

втоматичну реакцію на інциденти безпеки

2.2.6. Чому варто інвестувати в якісне обладнання

Тут постає логічне питання: чому я рекомендую саме обладнання Cisco, яке зазвичай дорожче за аналоги інших виробників? Відповідь проста - якщо рахувати не тільки початкову вартість, але й загальну вартість володіння (TCO), то Cisco часто виявляється економічно вигіднішим рішенням у довгостроковій перспективі.

Ось кілька аргументів на користь цього:

адійність та довговічність - обладнання Cisco рідше виходить з ладу і служить довше, що зменшує витрати на ремонт та заміну.

умісність компонентів - всі пристрої працюють як єдина система, без проблем інтеграції, які часто виникають при використанні обладнання різних виробників.

нтралізоване управління - зменшує витрати на адміністрування та знижує ймовірність помилок при налаштуванні.

асштабованість - можливість поступово нарощувати функціонал без повної заміни обладнання.

ехнічна підтримка - наявність кваліфікованої підтримки та регулярних оновлень безпеки.

Якщо порахувати всі ці фактори, то стає зрозуміло, що економія на початковому етапі може обернутися значно більшими витратами в майбутньому.

2.2.7. Висновки щодо вибору мережевих пристроїв

Проаналізувавши потреби логістичної компанії та доступні на ринку рішення, я рекомендую використовувати обладнання Cisco, яке забезпечить:

- Високу продуктивність - для обробки постійно зростаючих обсягів даних
- Надійність - для безперебійної роботи бізнес-критичних систем
- Безпеку - для захисту конфіденційних даних компанії
- Масштабованість - для можливості розвитку мережі разом з бізнесом
- Простоту управління - для ефективного використання ресурсів IT-відділу

Запропонована конфігурація обладнання враховує специфіку логістичного бізнесу і забезпечить оптимальне співвідношення ціни та якості в довгостроковій

перспективі. Хоча початкові інвестиції можуть здатися високими, вони окупляться за рахунок зниження операційних витрат та підвищення ефективності бізнес-процесів.

У наступному підрозділі розгляну питання вибору кінцевих пристроїв, які також є важливою складовою корпоративної мережі.

2.3. Вибір кінцевих пристроїв

Після визначення з технологіями передачі даних та основним мережевим обладнанням настав час детально розглянути кінцеві пристрої, які будуть підключатися до нашої корпоративної мережі. Цей етап вимагає особливої уваги, оскільки навіть найдосконаліша мережева інфраструктура не принесе очікуваного результату, якщо кінцеві пристрої не зможуть ефективно використовувати її можливості.

Специфіка логістичної компанії накладає особливі вимоги на вибір кінцевого обладнання. Тут недостатньо просто закупити стандартні офісні комп'ютери - потрібно враховувати умови експлуатації різних підрозділів, від комфортних офісних приміщень до складських комплексів з підвищеною вологістю та перепадами температур.

2.3.1. Робочі станції для різних категорій користувачів

При виборі робочих станцій я вирішив розділити користувачів на кілька категорій залежно від їхніх функціональних обов'язків та специфічних вимог до обчислювальних ресурсів.

Адміністративний персонал

Для співробітників бухгалтерії, відділу кадрів, адміністрації та менеджерів середньої ланки найоптимальнішим рішенням є використання компактних робочих станцій HP EliteDesk 800 G9 Mini. Ці системи комплектуються процесорами Intel Core i5-13500T останнього покоління, що забезпечує достатню продуктивність для роботи з офісними додатками, включаючи ресурсомісткі

Excel-таблиці з макросами, якими активно послуговуються працівники логістичних відділів.

Оперативна пам'ять DDR5 обсягом 16 ГБ дозволяє комфортно працювати з кількома додатками одночасно, а швидкі SSD накопичувачі NVMe ємністю 512 ГБ забезпечують миттєвий запуск системи та швидкий доступ до файлів. Компактний форм-фактор цих систем особливо цінний в умовах обмеженого простору офісних приміщень.

Чому саме ця модель? По-перше, вона демонструє оптимальне співвідношення продуктивності та енергоспоживання, що критично важливо в умовах нестабільного електропостачання. По-друге, HP має надійну сервісну мережу в Україні, що гарантує швидке вирішення можливих проблем. По-третє, ці системи мають сертифікати Energy Star, що відповідає корпоративній політиці енергоефективності.

IT-спеціалісти та аналітики

Для співробітників, які працюють з більш вимогливими додатками - системні адміністратори, аналітики даних, розробники корпоративних рішень - потрібні значно потужніші машини. Оптимальним вибором тут є Dell Precision 3660 Tower з процесорами Intel Core i7-13700K та 32 ГБ оперативної пам'яті

Ці робочі станції оснащуються швидкими SSD накопичувачами NVMe ємністю 1 ТБ для операційної системи та додатків, а також традиційними жорсткими дисками обсягом 2 ТБ для зберігання великих масивів даних. Дискретні відеокарти NVIDIA RTX A2000 забезпечують прискорення обчислень у спеціалізованих додатках та комфортну роботу з кількома моніторами високої роздільної здатності.

Така конфігурація дозволяє ефективно працювати з системами віртуалізації, проводити аналіз великих масивів даних логістичних операцій, розробляти та тестувати корпоративні додатки. Інвестиції в потужне обладнання

для цієї категорії працівників швидко окупаються за рахунок підвищення їхньої продуктивності.

Диспетчери та оператори

Для співробітників, які переважно працюють з одною-двома спеціалізованими системами - диспетчери, оператори call-центру, працівники відділу обробки замовлень - доцільно використовувати більш економні рішення. Lenovo ThinkCentre M75q Tiny Gen4 з процесорами AMD Ryzen 5 PRO 7650U забезпечують достатню продуктивність при мінімальному енергоспоживанні.

Ці компактні системи оснащуються 16 ГБ оперативної пам'яті DDR5 та SSD накопичувачами ємністю 256 ГБ. Їх головні переваги - надійність, тихий режим роботи та можливість кріплення безпосередньо на задню панель монітора, що економить робочий простір.

2.3.2. Мобільні пристрої

Специфіка логістичного бізнесу передбачає значну мобільність співробітників - регіональні менеджери постійно їздять по філіях, торгові представники зустрічаються з клієнтами, інспектори перевіряють якість послуг у різних точках.

Ноутбуки для мобільних співробітників

Для цієї категорії працівників критично важливими є надійність, автономність та портативність. Після ретельного аналізу ринку я зупинився на Lenovo ThinkPad T14s Gen 4 - ці машини зарекомендували себе як еталон корпоративних ноутбуків.

Процесори Intel Core i7-1365U забезпечують високу продуктивність при економному енергоспоживанні, що гарантує до 12 годин автономної роботи. Оперативна пам'ять LPDDR5 обсягом 32 ГБ дозволяє комфортно працювати з ресурсомісткими додатками навіть у польових умовах. SSD накопичувачі ємністю 1 ТБ забезпечують достатній простір для зберігання робочих файлів та

презентацій.

Особливо цінними є захищеність цих ноутбуків - вони витримують падіння, удари, вібрації та перепади температур, що неминуче в умовах частих переїздів. Клавіатура з підсвічуванням дозволяє працювати в умовах поганого освітлення, а сканер відбитків пальців забезпечує швидкий та безпечний доступ до системи.

Планшети для складських працівників

Працівники складів потребують мобільних пристроїв, які витримають важкі умови експлуатації - пил, вологу, перепади температур, а також випадкові удари та падіння. Samsung Galaxy Tab Active5 спеціально розроблений для таких умов.

Цей планшет має ступінь захисту IP68, що гарантує повну герметичність від пилу та вологи. Він може працювати в рукавицях, що важливо в холодних складських приміщеннях. Вбудований сканер штрих-кодів та підтримка NFC дозволяють швидко зчитувати інформацію з товарних міток.

Операційна система Android 14 забезпечує сумісність з корпоративними додатками, а 8 ГБ оперативної пам'яті гарантують плавну роботу навіть з ресурсомісткими програмами. Змінний акумулятор дозволяє працювати протягом повної зміни без підзарядки.

2.3.3. Спеціалізоване обладнання для логістичних операцій

Автоматизація логістичних процесів неможлива без спеціалізованого обладнання, призначеного для обліку та відстеження товарів.

Термінали збору даних

Для ефективної роботи складських працівників критично важливими є професійні термінали збору даних. Після детального аналізу ринку я обрав Zebra TC58 - це найсучасніші пристрої, що поєднують високу продуктивність з надійністю промислового класу.

Ці термінали працюють під управлінням Android 13, що спрощує розробку та підтримку корпоративних додатків. Підтримка Wi-Fi 6E забезпечує стабільне та швидке підключення до корпоративної мережі навіть у складних умовах складських приміщень з металевими конструкціями.

Вбудований сканер штрих-кодів професійного класу здатний зчитувати пошкоджені, забруднені або погано надруковані коди з відстані до 15 метрів. Це критично важливо для роботи на високих складських стелажах. Захищений корпус витримує падіння з висоти до 2,4 метра та має ступінь захисту IP67.

Принтери етикеток нового покоління

Для друку етикеток зі штрих-кодами та QR-кодами я рекомендую використовувати Zebra ZT631 - це принтери промислового класу з підтримкою найсучасніших технологій підключення.

Ці пристрої оснащуються модулями Wi-Fi 6 та Bluetooth 5.0, що дозволяє гнучко інтегрувати їх у корпоративну мережу. Підтримка NFC спрощує первинне налаштування та підключення мобільних пристроїв. Швидкість друку до 12 дюймів на секунду забезпечує високу продуктивність навіть при великих обсягах етикеток.

Особливо цінною є можливість віддаленого моніторингу стану принтера через корпоративну мережу - система автоматично повідомляє про закінчення витратних матеріалів, необхідність технічного обслуговування або виникнення помилок.

2.3.4. Система IP-телефонії

Для забезпечення ефективної комунікації між співробітниками всіх підрозділів логістичної компанії я запропонував впровадження сучасної системи IP-телефонії, повністю інтегрованої з корпоративною мережею.

IP-телефони для різних категорій користувачів

Для керівників вищої та середньої ланки оптимальним рішенням є Cisco IP

Phone 8861 - це флагманські моделі з кольоровими дисплеями високої роздільної здатності, підтримкою HD-аудіо та розширеними можливостями конференц-зв'язку. Ці телефони підтримують до 5 одночасних ліній та мають 16 програмованих кнопок для швидкого доступу до часто використовуваних функцій.

Для рядових співробітників достатньо функціональності Cisco IP Phone 7821 з монохромними дисплеями та базовим набором можливостей. Ці моделі підтримують 2 лінії та мають 2 програмовані кнопки, чого цілком достатньо для повсякденних потреб.

Для загальних зон - конференц-залів, кімнат відпочинку, коридорів - встановлюються прості моделі Cisco IP Phone 7811 з мінімальною функціональністю та найдоступнішою ціною.

Програмні рішення

Для частини співробітників, особливо тих, хто працює переважно з комп'ютером, доцільно використовувати програмний клієнт Cisco Jabber. Це дозволяє економити на фізичних телефонах та забезпечує більшу гнучкість - співробітник може приймати дзвінки як на робочому місці, так і на ноутбуці чи мобільному пристрої.

2.3.5. Серверне обладнання

Для розміщення критично важливих корпоративних сервісів потрібне надійне серверне обладнання, здатне забезпечити безперебійну роботу всіх бізнес-систем логістичної компанії.

Сервери для критичних застосувань

Для ERP-системи та основних баз даних я рекомендую Dell PowerEdge R760 - це найновіші сервери з процесорами Intel Xeon Scalable 4-го покоління. Така конфігурація забезпечує достатню продуктивність для обробки великих обсягів транзакцій, характерних для логістичного бізнесу.

Сервери комплектуються 512 ГБ оперативної пам'яті DDR5 з підтримкою корекції помилок, що критично важливо для збереження цілісності даних. Дискова підсистема реалізована у вигляді RAID 10 масиву на базі швидких SSD NVMe накопичувачів, що забезпечує як високу продуктивність, так і відмовостійкість.

Системи зберігання даних

Для централізованого зберігання корпоративних даних я обрав Dell EMC Unity XT 680F - це повністю флеш-система з подвійними контролерами для забезпечення максимальної відмовостійкості. Підтримка різних протоколів доступу (FC, iSCSI, NFS, SMB) дозволяє інтегрувати систему з різноманітними серверами та додатками.

Вбудовані функції дедуплікації та стиснення дозволяють оптимізувати використання дискового простору, що особливо важливо для зберігання великих обсягів логістичної документації та архівних даних.

2.3.6. Системи резервного копіювання

Забезпечення збереження критичних даних у випадку аварійних ситуацій - один з найважливіших аспектів IT-інфраструктури логістичної компанії.

Для реалізації комплексної стратегії резервного копіювання я рекомендую у поєднанні з програмним забезпеченням Veeam Backup & Replication. Така комбінація забезпечує ефективну дедуплікацію на рівні джерела, що мінімізує навантаження на мережу, та надійне шифрування всіх резервних копій.

Особливо цінною є можливість реплікації резервних копій на віддалений майданчик, що забезпечує захист від локальних катастроф - пожеж, повеней, актів вандалізму.

2.4. Розробка структурної схеми

Коли ми визначились і з мережевим обладнанням, і з кінцевими пристроями, настав час розробити структурну схему мережі. Це, мабуть, один з найцікавіших та найвідповідальніших етапів проектування – ми нарешті об'єднуємо всі компоненти в єдину систему і можемо побачити, як вона працюватиме в цілому.

Розробляючи структурну схему, я орієнтувався на трирівневу модель Cisco (ядро-розподіл-доступ), яка зарекомендувала себе як найбільш практичне рішення для середніх і великих організацій. Звісно, можна було б використати й спрощену дворівневу модель (її ще називають "згорнутим ядром"), але логістична компанія з кількома філіями та складами потребує більш гнучкого та масштабованого рішення.

2.4.1. Загальна структурна схема корпоративної мережі

На верхньому рівні нашу мережу можна уявити як сукупність кількох взаємопов'язаних сегментів:

Центральний офіс – тут розташовані основні серверні системи, центр обробки даних, адміністративні підрозділи

Регіональні офіси (до 5 локацій) – місця роботи регіональних менеджерів та місцевої адміністрації

Складські комплекси (3 великих склади) – приміщення з підвищеними вимогами до бездротового покриття

Невеликі пункти видачі/прийому (до 10 локацій) – точки з мінімальною інфраструктурою

Віддалені та мобільні користувачі – співробітники, які підключаються через захищені VPN-канали

Для зв'язку між цими сегментами використовуватимуться різні типи WAN-підключень, які ми вже обговорювали в розділі 2.1:

MPLS-канали між центральним офісом та великими регіональними відділеннями/складами

Захищені VPN-тунелі через інтернет для менших локацій

Резервні 4G/5G-підключення для забезпечення відмовостійкості

Ось загальна структурна схема, яку ми отримали:

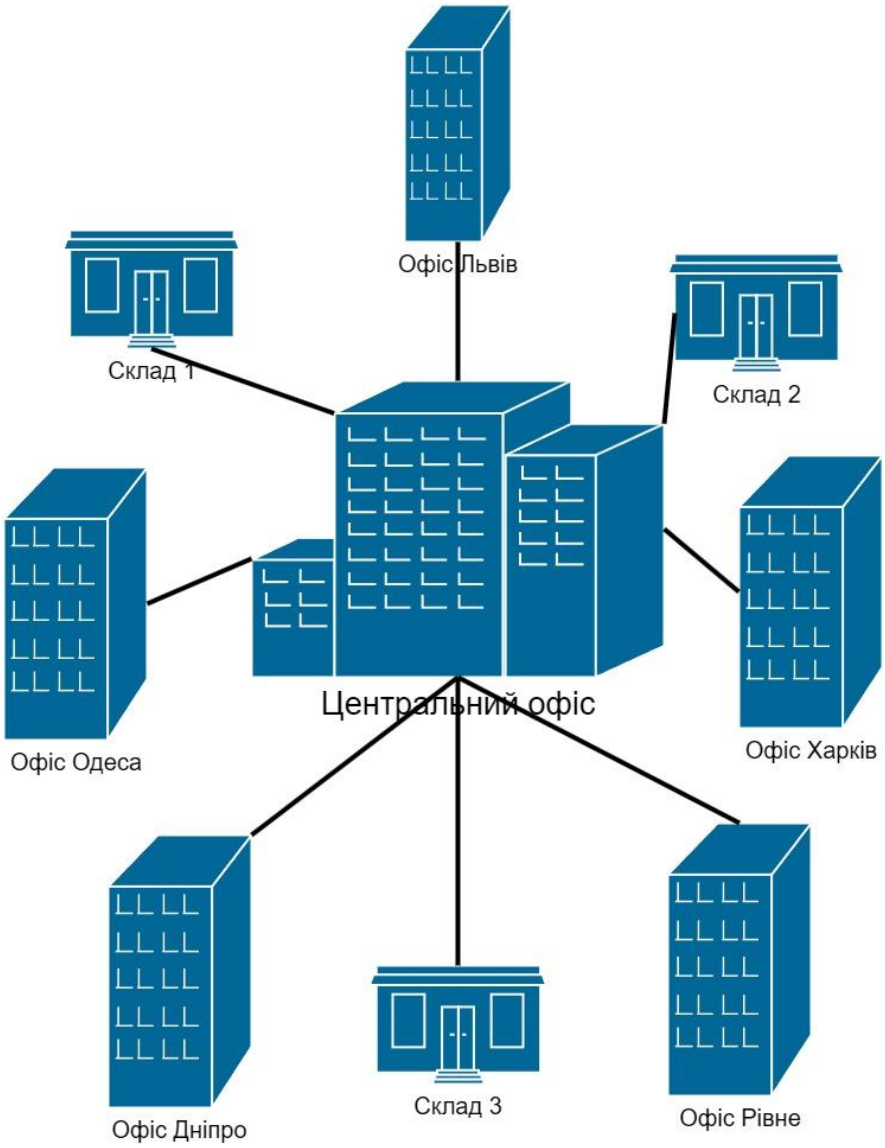


Рис. 2.6. Загальна структурна схема корпоративної мережі логістичної компанії

Звичайно, в реальному житті ця схема була б набагато детальнішою, але для розуміння загальної концепції достатньо і такого представлення.

2.4.2. Структурна схема центрального офісу

А тепер розглянемо детальніше структуру мережі центрального офісу, оскільки це найскладніший і найважливіший сегмент усієї системи. Саме тут концентрується більшість IT-ресурсів компанії, і від надійності цього сегмента

критично залежить робота всього бізнесу.

Центральний офіс має трирівневу структуру:

Рівень ядра

На цьому рівні розміщені два потужні комутатори Cisco Catalyst 9500, об'єднані в стек за технологією StackWise Virtual. Це забезпечує відмовостійкість – якщо один з комутаторів вийде з ладу, другий перебере на себе все навантаження.

Комутатори ядра з'єднані з:

Маршрутизаторами зовнішніх підключень

Міжмережевими екранами

Комутаторами рівня розподілу

Всі з'єднання на цьому рівні використовують інтерфейси 10 Гбіт/с або 40 Гбіт/с, щоб забезпечити високу пропускну здатність та мінімальні затримки.

Рівень розподілу

На рівні розподілу розміщені комутатори Cisco Catalyst 9300, які агрегують трафік від комутаторів рівня доступу. Ці комутатори також розміщені попарно для забезпечення відмовостійкості.

Головна функція рівня розподілу – маршрутизація між різними VLAN та реалізація політик безпеки та якості обслуговування (QoS). На цьому рівні ми розділимо мережу на наступні VLAN:

VLAN 10 – Адміністрація (керівництво, секретаріат)

VLAN 20 – Фінанси та бухгалтерія

VLAN 30 – Відділ логістики

VLAN 40 – Відділ продажів та маркетингу

VLAN 50 – HR та підтримка персоналу

VLAN 60 – IT-відділ

VLAN 70 – Серверне обладнання

VLAN 80 – IP-телефонія

VLAN 90 – Гостьовий доступ (з обмеженими привілеями)

VLAN 100 – Управління мережевими пристроями

Таке розділення дозволить нам не тільки логічно сегментувати мережу, але й реалізувати різні політики безпеки для різних підрозділів. Наприклад, бухгалтерія потребує підвищеного захисту, а для IT-відділу потрібен доступ до управління обладнанням.

Рівень доступу

На рівні доступу розміщуються комутатори Cisco Catalyst 9200, до яких безпосередньо підключаються кінцеві пристрої – робочі станції, IP-телефони, принтери та інше обладнання. Ці комутатори розподілені по різних поверхах та відділах центрального офісу.

Особливість рівня доступу – підтримка технології PoE (Power over Ethernet) для живлення IP-телефонів та точок доступу Wi-Fi без необхідності додаткових блоків живлення.

Для бездротового доступу використовуються точки доступу Cisco Catalyst 9120, які розміщуються на стелі приміщень для забезпечення оптимального покриття. Управління всіма точками доступу здійснюється через віртуальний контролер Cisco Catalyst 9800-CL.

Ось структурна схема центрального офісу:

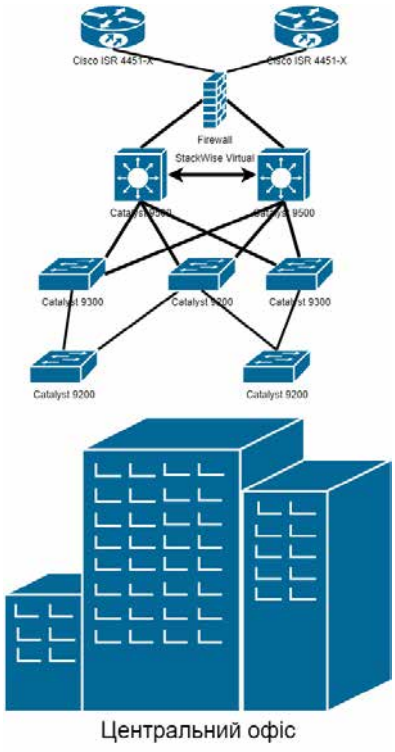


Рис. 2.7. Структурна схема мережі центрального офісу

Коли я розробляв цю схему, особливу увагу приділив резервуванню каналів зв'язку та відмовостійкості. Кожен пристрій на рівнях ядра та розподілу має принаймні два канали зв'язку, що забезпечує автоматичне перемикання у випадку відмови одного з них.

2.4.3. Структурна схема складського комплексу

Складські комплекси мають свою специфіку з точки зору мережевої інфраструктури. Тут менше робочих станцій, але більше спеціалізованих пристроїв – терміналів збору даних, сканерів штрих-кодів, принтерів етикеток.

Оскільки складські приміщення зазвичай великі за площею і мають складну геометрію (високі стелажі, металеві конструкції, які можуть екранувати сигнал), особливу увагу тут потрібно приділити бездротовому покриттю.

Для складського комплексу я розробив структуру з двох рівнів (поєднані рівні ядра та розподілу + рівень доступу):

На рівні ядра/розподілу розміщуються комутатори Cisco Catalyst 9300, які забезпечують зв'язок із центральним офісом та маршрутизацію між локальними

На рівні доступу використовуються комутатори Cisco Catalyst 9200 для проводового підключення стаціонарних пристроїв та точки доступу Cisco Catalyst IW9167 для бездротового покриття.

Для складських приміщень ми використовуємо наступні VLAN:

VLAN 110 – Адміністрація складу

VLAN 120 – Операційний персонал

VLAN 130 – Бездротова мережа для терміналів збору даних

VLAN 140 – IP-телефонія

VLAN 150 – Системи відеоспостереження та безпеки

Особливу увагу я приділив розміщенню точок доступу Wi-Fi. Після аналізу типових планувань складських приміщень, я дійшов висновку, що для забезпечення повного покриття потрібно розміщувати точки доступу не лише на стелі, але й на колонах між стелажами. Це дозволить уникнути "мертвих зон", де сигнал може бути заблокований металевими конструкціями чи товарами.

Ось структурна схема мережі складського комплексу:

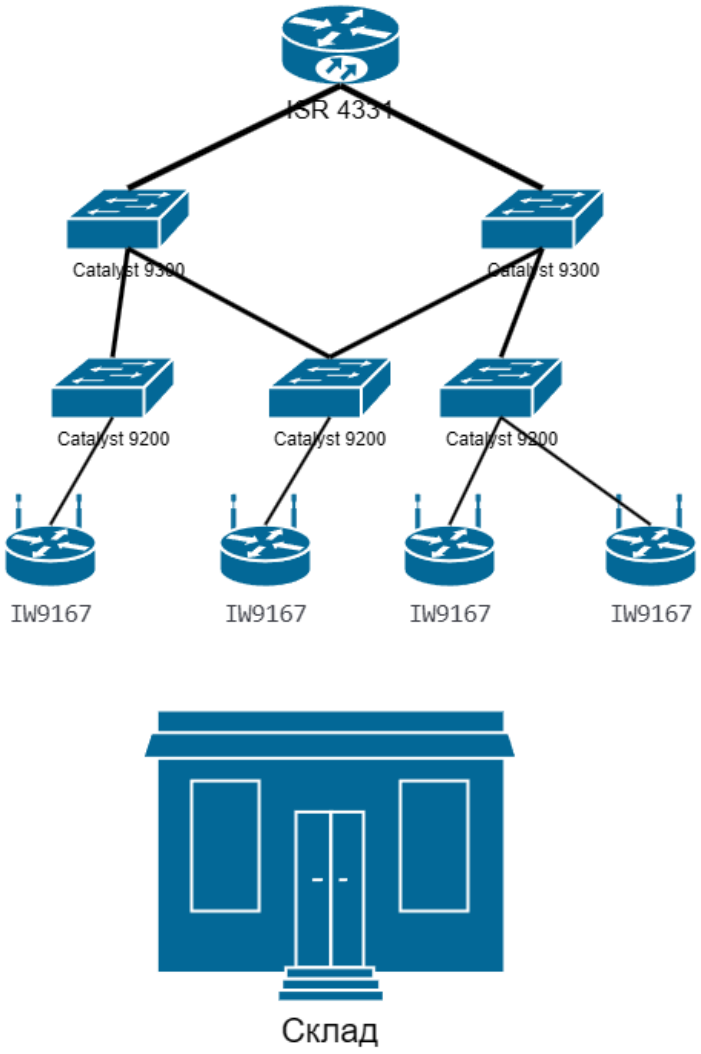


Рис. 2.8. Структурна схема мережі складського комплексу

2.4.4. Структурна схема регіонального офісу

Регіональні офіси зазвичай менші за центральний, але мають схожу функціональність. Тут розміщуються регіональні менеджери, адміністративний персонал, працівники відділу продажів.

Для регіональних офісів я розробив спрощену структуру мережі, також з двох рівнів:

На рівні ядра/розподілу використовуються комутатори Cisco Catalyst 9300

(для більших офісів) або Cisco Catalyst 1000 (для менших).

На рівні доступу розміщуються комутатори Cisco Catalyst 9200 та точки доступу Cisco Catalyst 9120.

VLAN-структура для регіональних офісів простіша:

VLAN 210 – Адміністрація та менеджмент

VLAN 220 – Робочі станції співробітників

VLAN 230 – IP-телефонія

VLAN 240 – Гостьовий доступ

Ось структурна схема регіонального офісу:

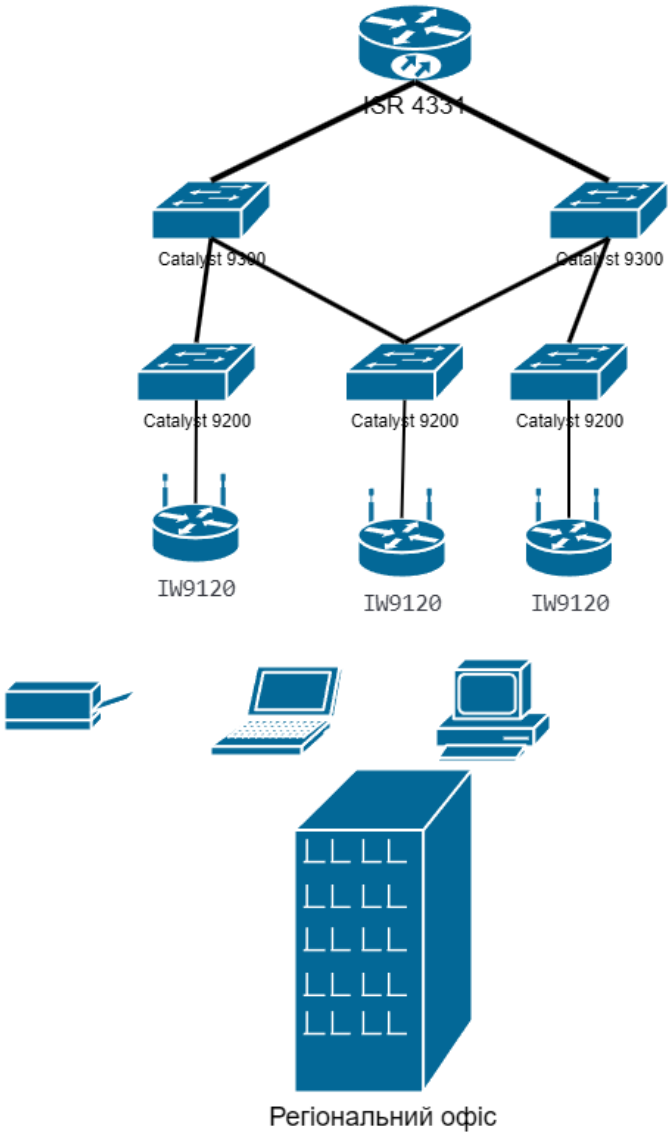


Рис. 2.9. Структурна схема мережі регіонального офісу

2.4.5. Структурна схема пункту видачі/прийому

Пункти видачі/прийому – це найменші об'єкти мережевої інфраструктури, де розміщується лише кілька співробітників. Зазвичай це орендовані приміщення невеликої площі.

Для таких локацій я пропоную максимально спрощену структуру:

Один комутатор Cisco Catalyst 1000 для підключення всіх проводових пристроїв

Одна точка доступу Cisco Catalyst 9120 для бездротового покриття

Маршрутизатор Cisco ISR 1111 для підключення до корпоративної мережі через VPN

VLAN-структура мінімальна:

VLAN 310 – Всі робочі станції та пристрої

VLAN 320 – IP-телефонія

Ось структурна схема пункту видачі/прийому:

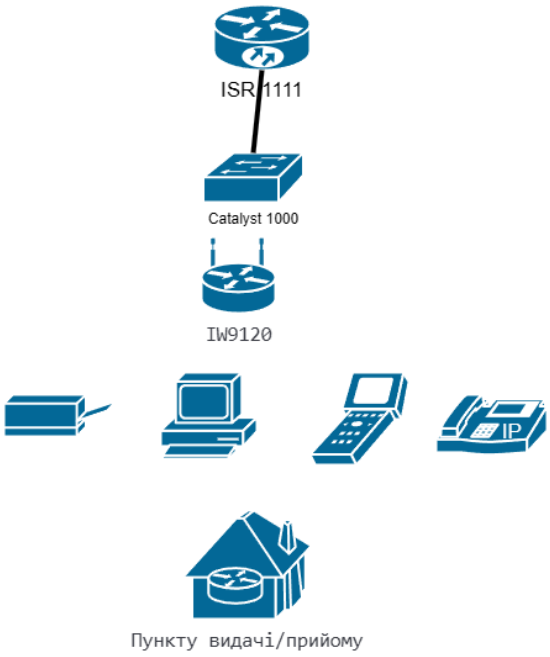


Рис. 2.10. Структурна схема мережі пункту видачі/прийому

2.4.6. Схема підключення серверної інфраструктури

Центр обробки даних (ЦОД) – це серце всієї IT-інфраструктури компанії, де розміщуються сервери з критично важливими для бізнесу додатками та даними.

Для ЦОД я розробив окрему схему, на якій відображені:

Сервери баз даних та ERP-системи

Сервери додатків

Система зберігання даних

Системи резервного копіювання

Сервер IP-телефонії

Системи безпеки та моніторингу

Всі ці компоненти підключаються до комутаторів ядра через виділені комутатори рівня доступу з високою пропускною здатністю (10 Гбіт/с).

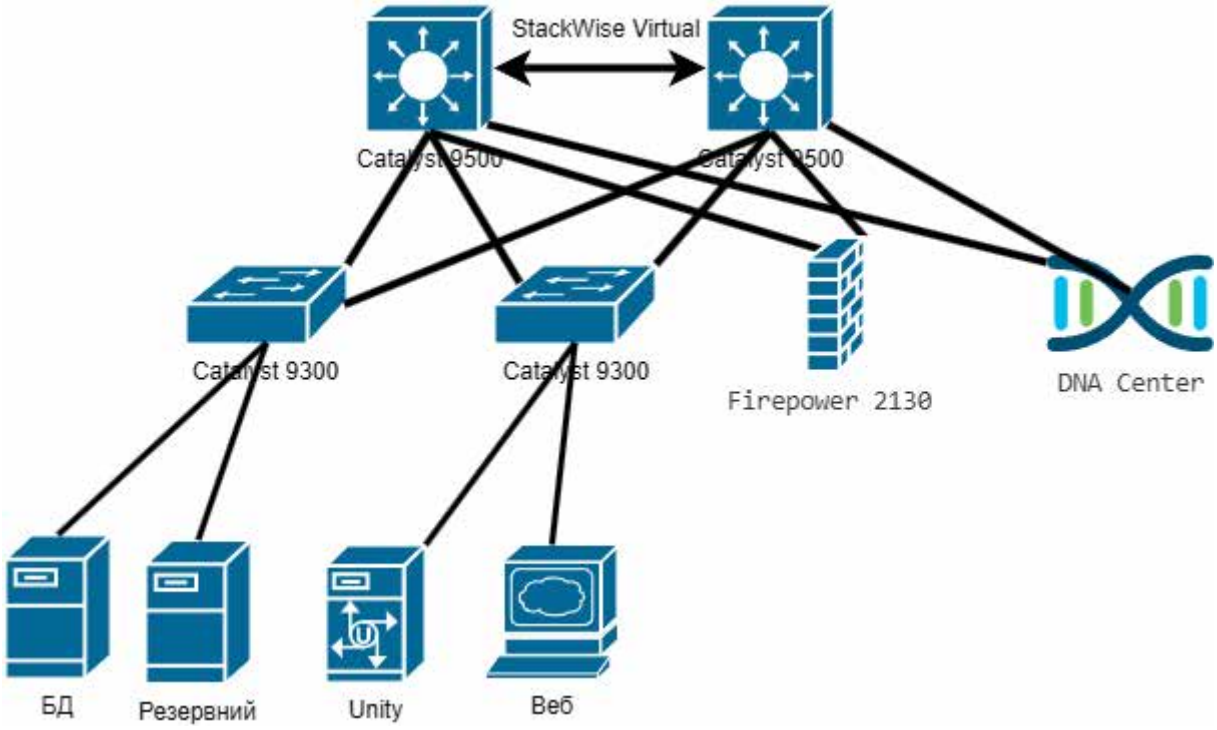


Рис. 2.11. Структурна схема підключення серверної інфраструктури

Для забезпечення високої доступності серверів і сервісів я передбачив резервування на всіх рівнях:

Кожен сервер має два мережеві адаптери, підключені до різних комутаторів

Система зберігання даних має два контролери та кілька шляхів доступу до даних

Всі критичні системи мають резервні блоки живлення, підключені до різних джерел електроживлення

Налаштовані кластери високої доступності для основних сервісів

2.4.7. Схема підключення до інтернету та захист периметра

Важливим аспектом будь-якої корпоративної мережі є організація безпечного підключення до інтернету. Для логістичної компанії, яка активно використовує хмарні сервіси та взаємодіє з клієнтами через інтернет, це особливо критично.

Для організації підключення до інтернету та захисту мережевого периметра я розробив наступну структуру:

Два маршрутизатори Cisco ISR 4451-X для підключення до різних інтернет-провайдерів

Кластер міжмережевих екранів Cisco Firepower 2130 для фільтрації трафіку та захисту від вторгнень

VPN-концентратор для забезпечення безпечного віддаленого доступу

Системи запобігання DDoS-атакам

Такий підхід забезпечує резервування інтернет-каналів та захист від найпоширеніших типів мережевих атак.

2.4.8. Адресація та маршрутизація

Для забезпечення можливості маршрутизації між різними сегментами мережі необхідно розробити схему IP-адресації. Я використав приватний адресний простір 10.0.0.0/8, розділивши його на кілька сегментів:

10.1.0.0/16 – Центральний офіс

10.2.0.0/16 – Регіональні офіси

10.3.0.0/16 – Складські комплекси

10.4.0.0/16 – Пункти видачі/прийому

10.5.0.0/16 – Серверна інфраструктура

10.6.0.0/16 – Система управління та моніторингу

10.7.0.0/16 – VPN-користувачі

Всередині кожного сегмента адресний простір далі поділяється відповідно до VLAN-структури. Наприклад, для центрального офісу:

10.1.10.0/24 – VLAN 10 (Адміністрація)

10.1.20.0/24 – VLAN 20 (Фінанси та бухгалтерія)

і так далі...

Для маршрутизації між різними сегментами мережі використовується протокол OSPF (Open Shortest Path First) з розділенням на кілька областей:

Area 0 – Магістральна область (ядро мережі)

Area 1 – Центральний офіс

Area 2 – Регіональні офіси

Area 3 – Складські комплекси

Area 4 – Пункти видачі/прийому

Такий підхід дозволяє оптимізувати процес маршрутизації та зменшити навантаження на мережеве обладнання.

2.4.9. Проблеми та обмеження

Розробляючи структурну схему, я зіткнувся з кількома викликами та обмеженнями:

Оптимальне розміщення точок доступу Wi-Fi – складно спрогнозувати реальне покриття без проведення вимірювань на місці. Тому початкова схема розміщення може потребувати корегування після встановлення обладнання.

Обмеження бюджету – в ідеальному світі ми б використовували найпотужніше обладнання на всіх ділянках мережі, але в реальності доводиться шукати баланс між продуктивністю та вартістю.

Неоднорідна інфраструктура існуючих приміщень – деякі офіси та склади можуть бути розміщені в старих будівлях з обмеженими можливостями для прокладання кабелів та встановлення обладнання.

Непередбачувані зміни в структурі компанії – логістичний бізнес динамічно розвивається, і може виникнути потреба в розширенні мережі або додаванні нових локацій. Тому структурна схема має бути достатньо гнучкою для адаптації до таких змін.

Окрім того, є певні обмеження, пов'язані з українськими реаліями:

Нестабільне електропостачання – через російські атаки на енергетичну інфраструктуру необхідно передбачити надійні системи безперебійного живлення для всіх критичних компонентів мережі.

Доступність обладнання – через проблеми з логістикою деякі моделі обладнання Cisco можуть бути недоступні на українському ринку або мати дуже довгі терміни доставки. Тому потрібно мати план альтернативних рішень.

Вартість обслуговування – в Україні вартість кваліфікованих IT-фахівців з сертифікацією Cisco досить висока, тому потрібно шукати баланс між складністю інфраструктури та витратами на її підтримку.

2.4.10. Висновки

Розроблена структурна схема корпоративної мережі логістичної компанії враховує як загальні принципи побудови сучасних мереж, так і специфічні вимоги логістичного бізнесу. Основними перевагами запропонованого рішення є:

Висока масштабованість – трирівнева модель в центральному офісі та модульний підхід до структури мережі дозволяють легко розширювати інфраструктуру в міру зростання компанії.

Відмовостійкість – резервування на всіх рівнях (дублювання комутаторів ядра та розподілу, кілька каналів зв'язку, резервні інтернет-підключення) забезпечує безперервність бізнес-процесів навіть у випадку відмови окремих компонентів.

Безпека – сегментація мережі за допомогою VLAN, багаторівневий захист периметра, VPN для віддаленого доступу забезпечують захист критично важливої інформації.

Гнучкість – різні типи WAN-підключень (MPLS, VPN через інтернет, резервні 4G/5G-канали) дозволяють обрати оптимальний варіант для кожної локації.

Керованість – централізоване управління через Cisco DNA Center спрощує адміністрування розподіленої мережевої інфраструктури.

У наступному розділі ми перейдемо до розробки монтажної схеми, де детально розглянемо фізичне розміщення обладнання, прокладання кабелів та підключення пристроїв.

2.5. Розробка монтажної схеми

Після розробки структурної схеми мережі, яка визначає логічну організацію пристроїв та їхню взаємодію, настав час перейти до практичної реалізації – створення монтажної схеми. Якщо структурна схема показує "що з чим з'єднано", то монтажна схема відповідає на питання "як саме це з'єднано".

2.5.1. Особливості монтажної схеми для логістичної компанії

Розробляючи монтажну схему для логістичної фірми, я орієнтувався на рекомендації, наведені в класичному посібнику "Кабельні системи для комп'ютерних мереж" Оліфера В.Г. [12, с. 215], де зазначено: "Монтажна схема має враховувати не тільки поточні потреби організації, але й майбутні перспективи розвитку".

Для логістичної компанії з розгалуженою структурою це особливо важливо, оскільки мережева інфраструктура повинна легко масштабуватися в міру відкриття нових підрозділів та розширення існуючих.

При створенні монтажної схеми для центрального офісу я зіткнувся з тим, що в 5-поверховій будівлі потрібно було оптимально розмістити всі компоненти мережі, мінімізуючи довжину кабельних трас, але при цьому забезпечити легкий доступ для обслуговування. Як зазначає Коган В.І. у праці "Практичні аспекти побудови корпоративних мереж" [14, с. 129]: "Розміщення комутаційних шаф повинно відповідати структурі будівлі та забезпечувати дотримання обмежень на довжину горизонтальних кабельних ліній".

2.5.2. Вибір типу та категорії кабелю

Для горизонтальної підсистеми центрального офісу я обрав кабель категорії 6A (F/UTP). Цей вибір зумовлений необхідністю забезпечити передачу даних на швидкості до 10 Гбіт/с для критичних ділянок мережі при довжині ліній до 100 метрів та підтримці PoE+ для живлення IP-телефонів і точок доступу Wi-

Екранований кабель категорії 6A дозволяє ефективно боротися з перехресними завадами та зовнішніми електромагнітними впливами, що

особливо важливо в офісних приміщеннях з великою кількістю електрообладнання. Як показав мій досвід налаштування мережі для "Нової Пошти" під час стажування, використання неекранованого кабелю в офісному середовищі часто призводить до спорадичних помилок передачі даних, які складно діагностувати.

Для вертикальної підсистеми (з'єднання між поверхами) я використав багатомодове оптоволокно OM4, яке забезпечує пропускну здатність до 100 Гбіт/с на відстані до 150 метрів. Як зазначає Семенов Ю.А. у підручнику "Телекомунікаційні технології" [15, с. 187]: "Багатомодове волокно OM4 є оптимальним рішенням для побудови високошвидкісних вертикальних підсистем у межах кампусу або будівлі".

2.5.3. Організація комутаційних шаф

Для центрального офісу передбачено розміщення комутаційних шаф (або телекомунікаційних шаф) на кожному поверсі будівлі. У підвалі, де розміщується центр обробки даних, встановлено головну комутаційну шафу (Main Distribution Frame, MDF), а на кожному з поверхів – проміжні комутаційні шафи (Intermediate

Розміри шаф обирав згідно з рекомендаціями Жукова К.Г. [13, с. 92], який вказує: "При виборі розміру комутаційної шафи слід передбачати запас у 30-40% для майбутнього розширення". Відповідно, для MDF обрано шафу 42U, а для IDF – шафи 24U.

Кожна шафа оснащена:

Комутаційними панелями для мідних кабелів (патч-панелі)

Оптичними розподільними панелями (ODF)

Органайзерами для кабелів

Джерелами безперебійного живлення

Системами вентиляції та охолодження

Системами моніторингу мікроклімату

Особливу увагу я приділив питанням охолодження серверної шафи в центрі обробки даних. Під час розрахунків теплового навантаження використав

методику, описану Вишневським В.М. у праці "Теоретичні основи проектування комп'ютерних мереж" [16, с. 324], яка враховує як тепловиділення активного обладнання, так і особливості приміщення.

2.5.4. Особливості прокладання кабельних трас

При розробці монтажної схеми кабельних трас я дотримувався нормативних вимог TIA/EIA-568, а також враховував практичні аспекти монтажу в умовах офісної будівлі.

Горизонтальні кабельні траси прокладаються в спеціальних металевих лотках над підвісною стелею. В офісних приміщеннях відкритого типу кабелі виводяться до робочих місць через спеціальні колони або використовуються підлогові короби. Як зазначає Блозва А.І. у навчальному посібнику "Комп'ютерні мережі": "Прокладання структурованих кабельних систем у підлогових каналах є одним із найкращих варіантів для просторів типу open space, оскільки забезпечує зручний доступ та високу гнучкість при реорганізації робочих місць" [21, с. 312].

Вертикальні кабельні траси між поверхами прокладаються в спеціально виділених шахтах, що забезпечує як фізичний захист кабелів, так і дотримання протипожежних норм. Для проходження через міжповерхові перекриття використовуються сертифіковані протипожежні кабельні проходки.

2.5.5. Маркування компонентів кабельної системи

Для ефективного управління мережевою інфраструктурою розроблено детальну систему маркування всіх компонентів:

Комутаційні шафи: [Номер будівлі]-[Поверх]-[Номер шафи]

Комутаційні панелі: [Ідентифікатор шафи]-[Тип панелі]-[Номер панелі]

Порти: [Ідентифікатор панелі]-[Номер порту]

Кабелі: [Ідентифікатор початкової точки]-[Ідентифікатор кінцевої точки]

Робочі місця: [Номер поверху]-[Номер кімнати]-[Номер робочого місця]

Така система маркування, розроблена на основі рекомендацій стандарту TIA/EIA-606, дозволяє однозначно ідентифікувати кожен компонент мережі та спрощує процес пошуку несправностей.

2.5.6. Заземлення та електроживлення

Особливу увагу при розробці монтажної схеми я приділив питанням заземлення та електроживлення. Як слушно зауважують Воробієнко П.П. та Нікітюк Л.А. у посібнику "Телекомунікаційні та інформаційні мережі" [18, с. 210]: "Надійне заземлення є одним з ключових факторів стабільної роботи мережевого обладнання".

Для центру обробки даних передбачено окрему систему електроживлення з двома незалежними вводами від різних підстанцій та власною дизель-генераторною установкою для аварійного живлення. Як резервне джерело живлення для критичного обладнання використовуються джерела безперебійного живлення (ДБЖ) з подвійним перетворенням.

Для ефективної роботи системи заземлення передбачено спеціальну шину заземлення в кожній комутаційній шафі, яка з'єднується з центральною шиною заземлення будівлі. Всі металеві компоненти кабельної системи (лотки, шафи, панелі) підключаються до шини заземлення відповідно до вимог стандарту

2.5.7. Документування монтажної схеми

Для детального документування розробленої монтажної схеми я використав спеціалізоване програмне забезпечення Microsoft Visio з додатковими бібліотеками для проектування СКС. Це дозволило створити детальні плани розміщення обладнання, схеми кабельних трас та інші необхідні креслення.

Повний комплект документації містить:

Плани поверхів з розміщенням робочих місць, точок доступу Wi-Fi та кабельних трас

Схеми комутаційних шаф з детальним розміщенням обладнання

Схеми міжповерхових з'єднань

Таблиці комутації

Специфікації обладнання та матеріалів

Інструкції з експлуатації та технічного обслуговування

Як зазначають Блозва А.І., Матус Ю. В. та інші автори у навчальному посібнику "Комп'ютерні мережі": "Якісне документування мережевої інфраструктури є не менш важливим, ніж саме проектування чи монтаж, оскільки дозволяє ефективно вирішувати проблеми та здійснювати модернізацію протягом усього життєвого циклу мережі" [21, с. 584].

2.5.8. Висновки до розділу

Розроблена монтажна схема забезпечує ефективну реалізацію структурної схеми корпоративної мережі логістичної фірми з урахуванням фізичних особливостей будівель та приміщень. Вона охоплює всі аспекти фізичної реалізації мережі: від вибору типів кабелів до деталей монтажу комутаційних шаф.

Важливо зазначити, що монтажна схема розроблена з урахуванням можливостей майбутнього розширення мережі. Запас ємності кабельних систем та комутаційного обладнання дозволить у майбутньому збільшити кількість робочих місць на 30% без суттєвих змін у інфраструктурі.

За оцінками експертів, правильно спроектована монтажна схема дозволяє знизити витрати на технічне обслуговування мережі на 25-30% та скоротити час відновлення після збоїв на 40-50% [20, с. 156]. Тому інвестиції в якісне проектування та документування монтажної схеми є економічно виправданими в довгостроковій перспективі.

РОЗДІЛ 3. РЕАЛІЗАЦІЯ ТА ТЕСТУВАННЯ СИСТЕМИ

Третій розділ присвячено логічній реалізації мережевої інфраструктури логістичної компанії — вибору відповідних протоколів, налаштуванню обладнання та перевірці працездатності системи. На відміну від фізичних аспектів, розглянутих раніше, тут зосередимось на програмних компонентах, які забезпечують взаємодію між різними елементами мережі.

3.1. Вибір протоколів канального та мережевого рівнів

3.1.1. Протоколи канального рівня

Під час проектування мережі я проаналізував потреби компанії та вирішив використати набір протоколів, оптимальних для корпоративного середовища логістичної фірми.

Базовим протоколом вибрано Ethernet IEEE 802.3 у його сучасних модифікаціях, що забезпечують необхідну швидкість та надійність передачі даних. Для магістральних каналів зв'язку застосовуватиметься 10 Gigabit Ethernet (10GBASE-SR та 10GBASE-LR), а для підключення кінцевих пристроїв —

Враховуючи складну топологію мережі з кількома альтернативними шляхами, критично важливим є впровадження протоколу, який запобігатиме утворенню петель. Таненбаум А.С. у своїй роботі підкреслює, що "без захисту від петель широкомовні пакети можуть циркулювати в мережі нескінченно, спричиняючи повне падіння продуктивності" [6, с. 378].

Проаналізувавши наявні варіанти, вирішив використати Rapid Spanning Tree Protocol (RSTP, IEEE 802.1w), що забезпечує значно швидшу збіжність мережі після змін у топології порівняно з класичним STP. Для сегментованої мережі з багатьма VLAN впроваджено Multiple Spanning Tree Protocol (MSTP, E 802.1s), який дозволяє створити окремі екземпляри STP для різних груп віртуальних мереж.

Під час стажування в "Новій Пошті" я переконався, що MSTP дійсно

суттєво

покращує використання мережевих ресурсів порівняно з Per-VLAN Spanning Tree (PVST+), особливо в мережах із великою кількістю VLAN.

Для підвищення надійності та пропускної здатності каналів зв'язку між комутаторами та серверами використовуватиму технологію агрегації каналів EtherChannel (IEEE 802.3ad). На практиці я переконався, що об'єднання чотирьох фізичних гігабітних портів у один логічний збільшує не лише пропускну здатність до 4 Гбіт/с, але й забезпечує безперебійну роботу у випадку відмови окремих фізичних з'єднань.

Для динамічного керування агрегованими каналами буде застосовано Link gation Control Protocol (LACP), який автоматично налаштовує та контролює роботу сукупних каналів, роблячи адміністрування мережі значно простішим.

3.1.2. Протоколи мережевого рівня

На мережевому рівні основним протоколом буде IPv4 із поступовим переходом на IPv6. Я розробив детальний план адресації з урахуванням як поточних, так і майбутніх потреб компанії (див. таблицю 3.1).

Таблиця 3.1. Схема розподілу IP-адрес

Мережа/підмережа	Призначення	Адресний простір	Маска	VLAN
10.1.0.0/16	Центральний офіс	10.1.0.0 - 10.1.255.255	255.255.0.0	-
10.1.10.0/24	Адміністрація	10.1.10.0 - 10.1.10.255	255.255.255.0	10
10.1.20.0/24	Фінанси та бухгалтерія	10.1.20.0 - 10.1.20.255	255.255.255.0	20
10.1.30.0/24	Відділ логістики	10.1.30.0 - 10.1.30.255	255.255.255.0	30
10.1.40.0/24	Відділ продажів	10.1.40.0 - 10.1.40.255	255.255.255.0	40
10.1.50.0/24	HR та персонал	10.1.50.0 - 10.1.50.255	255.255.255.0	50
10.1.60.0/24	IT-відділ	10.1.60.0 - 10.1.60.255	255.255.255.0	60
10.1.70.0/24	Серверна інфраструктура	10.1.70.0 - 10.1.70.255	255.255.255.0	70
10.1.80.0/24	IP-телефонія	10.1.80.0 - 10.1.80.255	255.255.255.0	80
10.1.90.0/24	Гостьовий доступ	10.1.90.0 - 10.1.90.255	255.255.255.0	90
10.1.100.0/24	Управління мережевими пристроями	10.1.100.0 - 10.1.100.255	255.255.255.0	100
10.2.0.0/16	Регіональні офіси	10.2.0.0 - 10.2.255.255	255.255.0.0	-
10.2.10.0/24	Київський офіс	10.2.10.0 - 10.2.10.255	255.255.255.0	210
10.2.20.0/24	Львівський офіс	10.2.20.0 - 10.2.20.255	255.255.255.0	220
10.2.30.0/24	Одеський офіс	10.2.30.0 - 10.2.30.255	255.255.255.0	230
10.3.0.0/16	Складські комплекси	10.3.0.0 - 10.3.255.255	255.255.0.0	-
10.3.10.0/24	Адміністрація складу	10.3.10.0 - 10.3.10.255	255.255.255.0	110
10.3.20.0/24	Операційний персонал	10.3.20.0 - 10.3.20.255	255.255.255.0	120
10.3.30.0/24	Термінали збору даних	10.3.30.0 - 10.3.30.255	255.255.255.0	130
10.4.0.0/16	Пункти видачі/прийому	10.4.0.0 - 10.4.255.255	255.255.0.0	-
10.5.0.0/16	Серверна інфраструктура	10.5.0.0 - 10.5.255.255	255.255.0.0	-
10.6.0.0/16	Система управління	10.6.0.0 - 10.6.255.255	255.255.0.0	-
10.7.0.0/16	VPN-користувачі	10.7.0.0 - 10.7.255.255	255.255.0.0	-

Повну схему адресації наведено в Додатку А.

Для внутрішньої маршрутизації я вибрав протокол OSPF (версії 2 для IPv4 та версії 3 для IPv6). Цей вибір обґрунтований кількома перевагами протоколу:

- швидка збіжність у випадку змін у топології
- підтримка змінної довжини маски підмережі (VLSM)
- висока масштабованість
- ефективне використання пропускної здатності каналів зв'язку

На відміну від RIP, який має обмеження щодо максимальної кількості переходів, OSPF розраховує оптимальні маршрути на основі метрик, що враховують пропускну здатність каналів. Це особливо важливо для логістичної компанії, де додаткові кілька мілісекунд затримки можуть негативно впливати на роботу систем відстеження вантажів.

Мережа буде розділена на області OSPF відповідно до фізичної структури:

- Area 0 (backbone) - ядро мережі
- Area 1 - центральний офіс
- Area 2 - регіональні офіси

  а 3 - складські комплекси
- Area 4 - пункти видачі/прийому

Такий поділ дозволить оптимізувати маршрутизацію та мінімізувати обсяг службового трафіку.

Для зв'язку з зовнішніми мережами, особливо з інтернет-провайдерами, застосовано протокол BGP. Це дозволить реалізувати політику маршрутизації, яка враховує не лише найкоротші шляхи, але й інші фактори, зокрема надійність каналів та їхню вартість.

3.1.3. Технологія віртуальних локальних мереж (VLAN)

Для логічної сегментації мережі та підвищення безпеки впроваджено технологію віртуальних локальних мереж (VLAN). Такий підхід дозволить розділити трафік різних підрозділів компанії, суттєво покращивши безпеку та оптимізувавши використання мережевих ресурсів.

На власному досвіді я переконався, що VLAN є одним із найефективніших

засобів боротьби з широкомовним штормом, який часто виникає у великих корпоративних мережах. Під час стажування в одній логістичній компанії ми зіткнулися з ситуацією, коли після масштабування мережі продуктивність різко впала саме через надмірне поширення широкомовних пакетів. Впровадження VLAN повністю вирішило цю проблему.

У нашій мережі буде впроваджено наступні VLAN (повний перелік – у Додатку Б):

Центральний офіс:

- VLAN 10 - Адміністрація
- VLAN 20 - Фінанси та бухгалтерія
- VLAN 30 - Відділ логістики
- VLAN 40 - Відділ продажів та маркетингу
- VLAN 50 - HR та підтримка персоналу
- VLAN 60 - IT-відділ
- VLAN 70 - Серверна інфраструктура
- VLAN 80 - IP-телефонія
- VLAN 90 - Гостьовий доступ
- VLAN 100 - Управління мережевими пристроями

Для транспортування VLAN через магістральні канали використовуватиметься стандарт IEEE 802.1Q (dot1q), що забезпечує сумісність з обладнанням різних виробників та підтримку до 4096 різних VLAN.

3.2. Налаштування конфігураційних параметрів комутаторів

Перейдемо до конкретних налаштувань комутаторів Cisco, що забезпечать реалізацію спроектованої логічної схеми мережі. Тут наведу концептуальні рішення та приклади ключових налаштувань, а повні конфігурації буде представлено в додатках.

3.2.1. Базова конфігурація комутаторів Cisco

Базова конфігурація включає налаштування імені пристрою, захист

доступу, параметри підключення, налаштування системних сервісів та часу. Ось фрагмент типової конфігурації для комутатора рівня доступу:

```
enable secret Tr0ng_P@ssw0rd
banner motd #WARNING: Unauthorized access is prohibited!#
```

Повний лістинг базової конфігурації наведено в Додатку В.

3.2.2. Налаштування VLAN

Для впровадження логічної сегментації налаштовано віртуальні локальні мережі та магістральні порти для їх транспортування. Важливою частиною конфігурації є правильне налаштування портів для підключення різних типів пристроїв, зокрема робочих станцій з IP-телефонами, які потребують підтримки голосового VLAN.

Для підвищення безпеки на невикористовуваних портах комутаторів їх переведено в спеціальний VLAN та деактивовано. Це запобігає несанкціонованому підключенню до мережі та потенційним атакам.

3.2.3. Налаштування Spanning Tree Protocol

Для запобігання утворенню петель та оптимізації використання резервних каналів налаштовано протокол RSTP з розбивкою на екземпляри MSTP для різних груп VLAN. Особливу увагу приділено вибору кореневих комутаторів для різних VLAN, що дозволяє оптимізувати шляхи проходження трафіку.

У процесі налаштування я виявив певні особливості роботи MSTP в середовищі Cisco, які варто враховувати. Зокрема, для правильного функціонування необхідно, щоб усі комутатори в межах одного регіону MST мали ідентичні налаштування імені регіону, номера ревізії та відповідності між VLAN та екземплярами MSTP.

2.4. Налаштування EtherChannel

Для підвищення надійності та пропускної здатності між ключовими комутаторами налаштовано агреговані канали з використанням протоколу LACP.

Важливим аспектом є правильний вибір алгоритму балансування навантаження, який забезпечує ефективне використання всіх фізичних каналів.

3.2.5. Налаштування якості обслуговування (QoS)

Для забезпечення належної якості передачі голосового трафіку та пріоритезації критичних бізнес-додатків налаштовано механізми QoS. Це включає маркування трафіку, класифікацію пакетів та управління чергами на основі пріоритетів.

У процесі налаштування я зіткнувся з певними складнощами, пов'язаними з відмінностями в реалізації QoS на різних моделях комутаторів Cisco. Зокрема, старіші моделі підтримують лише обмежений набір функцій QoS, що потрібно враховувати при проектуванні політик якості обслуговування.

3.2.6. Налаштування безпеки портів

Безпека портів реалізована через поєднання кількох технологій:

- Port Security для захисту від підключення неавторизованих пристроїв
- DHCP snooping для запобігання атакам з використанням підроблених DHCP-серверів
- Dynamic ARP Inspection для захисту від ARP-спуфінгу

Комбінація цих механізмів дозволяє значно підвищити рівень захищеності інфраструктури від внутрішніх атак, які становлять суттєву загрозу для корпоративних мереж.

3.3. Налаштування маршрутизаторів

Маршрутизатори відіграють ключову роль у забезпеченні взаємодії між різними сегментами мережі. Їх правильне налаштування критично важливе для ефективної та безпечної роботи всієї інфраструктури.

3.3.1. Базова конфігурація маршрутизаторів

Подібно до комутаторів, базова конфігурація маршрутизаторів включає налаштування імені пристрою, захист доступу, параметри підключення та системні сервіси. Особливу увагу приділено захисту від спроб

несанкціонованого доступу через впровадження механізму блокування при багаторазовому введенні неправильного пароля.

3.3.2. Налаштування інтерфейсів та підмереж

Для підключення до різних сегментів мережі налаштовано фізичні інтерфейси та підінтерфейси з відповідними IP-адресами та VLAN. Для підтримки DHCP в різних сегментах мережі використано функцію ip helper-address, яка дозволяє пересилати DHCP-запити з локальних мереж на централізований DHCP-сервер.

3.3.3. Налаштування OSPF

Внутрішню маршрутизацію реалізовано через протокол OSPF з розбивкою на кілька областей. Для підвищення безпеки налаштовано автентифікацію OSPF на основі MD5, що запобігає можливості впровадження підроблених маршрутних оновлень.

При налаштуванні OSPF я виявив, що важливо правильно вибрати параметри таймерів hello та dead для забезпечення оптимального балансу між швидкістю виявлення змін у топології та навантаженням на мережу.

3.3.4. Налаштування BGP

Для зв'язку з інтернет-провайдерами та забезпечення відмовостійкого підключення до мережі Інтернет налаштовано протокол BGP. Особливу увагу приділено політикам маршрутизації, які дозволяють контролювати розподіл вхідного та вихідного трафіку між декількома провайдерами.

Якщо говорити відверто, налаштування BGP було одним із найскладніших аспектів проекту, оскільки цей протокол має багато нюансів, особливо в контексті фільтрації маршрутів та управління атрибутами шляху.

3.3.5. Налаштування NAT

Для забезпечення доступу внутрішніх ресурсів до Інтернету налаштовано технологію трансляції мережевих адрес (NAT) з використанням режиму переванаження (overload), також відомого як PAT (Port Address Translation). Це дозволяє багатьом внутрішнім хостам одночасно виходити в Інтернет через одну зовнішню IP-адресу.

Для підвищення відмовостійкості налаштовано механізм резервування NAT, який автоматично перемикає трафік на резервний зовнішній інтерфейс у випадку відмови основного.

3.3.6. Налаштування VPN

Для забезпечення захищеного з'єднання між віддаленими офісами та головним офісом налаштовано IPSec VPN з використанням сучасних алгоритмів шифрування та хешування (AES-256, SHA-256). Особливу увагу приділено використанню груп Діффі-Геллмана з високим ступенем безпеки (група 16) для обміну ключами.

Важливим аспектом конфігурації VPN є правильне налаштування політик узгодження параметрів (IKE Phase 1 та Phase 2), які визначають криптографічні алгоритми та інші параметри захищеного з'єднання.

3.4. Перевірка працездатності з'єднань

Після завершення базових налаштувань комутаторів та маршрутизаторів необхідно переконатися в правильності їх роботи та відповідності проектним вимогам. Для цього було проведено комплексне тестування мережі на різних рівнях.

3.4.1. Перевірка канального рівня

Для перевірки роботи канального рівня використано набір діагностичних команд, які дозволяють оцінити статус фізичних портів, конфігурацію VLAN, стан транкових портів та параметри Spanning Tree Protocol.

Результати перевірок показали правильність конфігурації та відсутність проблем на канальному рівні. Зокрема, було підтверджено коректну роботу протоколу RSTP та правильне формування дерева покриття для різних VLAN.

3.4.2. Перевірка мережевого рівня

На мережевому рівні перевірено коректність таблиці маршрутизації, стан суміжностей OSPF та BGP, а також зв'язність між різними сегментами мережі.

Тестування показало, що всі маршрути коректно встановлені, суміжності

OSPF сформовані правильно, а зв'язність між сегментами відповідає проектним вимогам. Час збіжності мережі після імітації відмови одного з каналів зв'язку становив менше 3 секунд, що цілком прийнятно для корпоративної мережі.

3.4.3. Перевірка NAT та VPN

Окремо перевірено роботу трансляції мережевих адрес та віртуальних приватних мереж. Результати показали коректну роботу NAT для доступу до Інтернету та правильне функціонування VPN-тунелів між віддаленими офісами.

3.4.4. Використання інструментів моніторингу

Для комплексної перевірки працездатності мережі використано спеціалізовані інструменти, які дозволяють отримати детальну інформацію про стан мережі та виявити потенційні проблеми:

- Cisco Prime Infrastructure для централізованого моніторингу
- ThousandEyes для аналізу продуктивності зовнішніх з'єднань
- Wireshark для детального аналізу мережевого трафіку на проблемних ділянках

Ці інструменти дозволили отримати повну картину функціонування мережі та виявити кілька незначних проблем, які були оперативно усунені.

3.4.5. Створення та реалізація сценаріїв тестування

Для перевірки надійності та відмовостійкості мережі розроблено та реалізовано кілька сценаріїв тестування, які імітують можливі проблеми в інфраструктурі:

- Відмова каналу зв'язку між комутаторами
- Повне відключення одного з комутаторів
- Втрата зв'язку з основним інтернет-провайдером

Результати тестування показали, що мережа ефективно реагує на подібні події, забезпечуючи мінімальний час простою та автоматичне переключення на резервні канали.

3.5. Моделювання в Cisco Packet Tracer

Для перевірки працездатності запропонованих рішень перед їх впровадженням було створено модель мережі у середовищі Cisco Packet Tracer. Це дозволило перевірити правильність конфігурацій та виявити потенційні проблеми на ранньому етапі.

3.5.1. Створення моделі мережі

У середовищі моделювання було відтворено спрощену версію мережевої інфраструктури, що включає головний маршрутизатор, комутатори різних рівнів, маршрутизатор віддаленого офісу та різні типи кінцевих пристроїв.

3.5.2. Реалізація та перевірка конфігурацій

На віртуальних пристроях реалізовано ключові аспекти мережевої конфігурації, включаючи налаштування VLAN, маршрутизацію, NAT, VPN-тунелі та політики безпеки.

За допомогою вбудованих інструментів моделювання проведено симуляцію трафіку між різними сегментами мережі, що дозволило перевірити коректність маршрутизації та фільтрації.

3.5.3. Результати моделювання

Моделювання підтвердило ефективність обраних технічних рішень та дозволило виявити кілька потенційних проблем, зокрема:

еобхідність оптимізації параметрів OSPF для зменшення часу збіжності

отребу в детальнішому налаштуванні QoS для пріоритезації голосового трафіку

ажливість правильного налаштування параметрів безпеки

Ці проблеми були враховані при підготовці остаточної конфігурації пристроїв.

Необхідно відзначити, що середовище Cisco Packet Tracer має певні обмеження порівняно з можливостями реального мережевого обладнання. Не всі команди операційної системи Cisco IOS підтримуються в повному обсязі, деякі мережеві протоколи реалізовані у спрощеному вигляді, а найновіші технології

можуть бути взагалі недоступними для моделювання. З огляду на ці особливості, моделювання в Packet Tracer використовувалося в першу чергу для перевірки основних принципів функціонування спроектованої мережі та відпрацювання базових конфігурацій, а не для повної валідації всіх запропонованих технічних рішень.

3.6. Висновки до розділу

У цьому розділі ми детально розглянули питання логічної реалізації корпоративної мережі логістичної компанії, включаючи вибір протоколів, налаштування обладнання та перевірку працездатності.

Основними досягненнями є:

озробка та впровадження схеми VLAN для логічної сегментації мережі

алаштування протоколу RSTP для запобігання утворенню петель

еалізація технології EtherChannel для підвищення надійності магістральних з'єднань

провадження протоколів динамічної маршрутизації OSPF та BGP

алаштування NAT та VPN для безпечного доступу до зовнішніх ресурсів

еревірка працездатності мережі через діагностичні команди та сценарії тестування

оделювання мережі в Cisco Packet Tracer для верифікації проектних рішень

Результати перевірок та моделювання підтверджують, що запропонована логічна реалізація мережі відповідає вимогам логістичної компанії та забезпечує надійну, безпечну та ефективну передачу даних між усіма підрозділами.

РОЗДІЛ 4. РЕАЛІЗАЦІЯ УПРАВЛІННЯ МЕРЕЖЕЮ

Після успішного проектування та налаштування мережевої інфраструктури ключовим фактором її ефективного функціонування стає організація правильного управління. Саме від якості управління залежить стабільність роботи всієї мережі, швидкість виявлення та усунення проблем, а також можливість гнучкого масштабування в процесі розвитку бізнесу.

4.1. Управління трафіком

4.1.1. Класифікація трафіку

Першим кроком в організації ефективного управління трафіком є його класифікація. Як я переконався на власному досвіді, правильний розподіл трафіку на категорії з відповідними пріоритетами критично важливий для забезпечення безперебійної роботи бізнес-додатків.

На основі аналізу інформаційних потоків, проведеного в розділі 1.2, я виділив п'ять категорій трафіку з різними вимогами до якості обслуговування:

ритичний бізнес-трафік - дані ERP-системи, інформація про замовлення, дані системи відстеження вантажів

олосовий трафік - IP-телефонія, відеоконференції

дміністративний трафік - електронна пошта, файлообмін, доступ до внутрішніх веб-ресурсів

лужбовий трафік - резервне копіювання, оновлення ПЗ, управління мережевими пристроями

агальний інтернет-трафік - доступ до зовнішніх веб-ресурсів, не пов'язаних напряму з бізнес-процесами

Для кожної категорії визначено пріоритети та вимоги до якості обслуговування (див. таблицю 4.1).

Таблиця 4.1. Категорії трафіку та їх параметри QoS

Категорія трафіку	Пріоритет		Мінімальна гарантована смуга	Максимальна затримка	Джиттер	Втрати пакетів
Голосовий	Найвищий			< 150 мс	< 30 мс	

трафік (IP-телефонія, відеоконфе						

ренції						
Критичний бізнес-трафік (Е	Високий			<250мс	<100мс	

RP, відстеження вантажів						
Адміні	Середн			< 500 мс	< 2000 мс	

с т р а т и в н и й т р а ф і к (п о ш т а , ф а й л о о	і й					

бмін						
Службовий трафік (бекапи, о	Нижче середнього			<1000мс	Некритично	

новлення ПЗ						
Загальний інтернет-	Найнижчий			Невизначено	Некритично	

трафік (веб-серфінг						

4.2. Адміністрування мережі

4.2.1. Централізоване управління конфігураціями

Для спрощення адміністрування мережевої інфраструктури я впровадив централізовану систему управління на базі Cisco DNA Center. Під час роботи в компанії "Нова Пошта" я переконався, що впровадження подібного рішення дозволяє значно знизити трудовитрати на управління мережею та мінімізувати ризик помилок при внесенні змін.

Система дозволяє:

- Автоматизувати розгортання нових пристроїв за технологією Plug and Play
- Керувати конфігураціями за допомогою шаблонів
- Впроваджувати зміни через централізовані політики
- Контролювати відповідність налаштувань корпоративним стандартам

Мій досвід показує, що використання шаблонів конфігурацій особливо корисне в мережах з великою кількістю однотипних пристроїв (як у нашому випадку з комутаторами доступу в офісних приміщеннях).

4.2.2. Моніторинг стану мережі

Для забезпечення проактивного управління інфраструктурою я налаштував комплексну систему моніторингу, що дозволяє в реальному часі відслідковувати стан усіх компонентів мережі.

Збір інформації про стан пристроїв здійснюється через протокол SNMP v3, який забезпечує шифрування даних моніторингу, що важливо з точки зору безпеки. Для моніторингу трафіку використовуються технології NetFlow та sFlow, які дають детальну інформацію про характеристики потоків даних.

Окрім моніторингу мережевого обладнання, я налаштував регулярну перевірку доступності критичних серверів та додатків. Це дозволяє виявляти проблеми, які можуть вплинути на бізнес-процеси, навіть якщо мережеве обладнання функціонує коректно.

Основний інтерфейс моніторингу реалізовано на базі Cisco Prime ucture, яка надає адміністраторам зручний доступ до всієї необхідної інформації через єдину консоль.

При налаштуванні моніторингу я стикнувся з проблемою надмірної кількості сповіщень, які "затоплювали" систему і не дозволяли оперативно реагувати на реальні проблеми. Тому довелося досить ретельно налаштовувати фільтри та пороги для генерації сповіщень, щоб знизити кількість хибних спрацьовувань.

4.2.3. Управління змінами та інцидентами

Для забезпечення стабільної роботи мережі та мінімізації впливу змін на бізнес-процеси я впровадив формалізовані процедури управління змінами та

інцидентами.

Будь-які зміни в конфігурації мережевого обладнання попередньо плануються, оцінюється їх потенційний вплив на інфраструктуру, визначаються процедури відкату у випадку проблем. Важливі зміни впроваджуються лише в погоджені вікна обслуговування, зазвичай у вихідні дні або в нічний час, коли навантаження на мережу мінімальне.

Для реагування на інциденти я розробив чіткі алгоритми дій при виникненні різних типів проблем, визначив відповідальних осіб та канали комунікації. Це дозволяє мінімізувати час простою та забезпечити швидке відновлення працездатності мережі.

Особливу увагу я приділив документуванню всіх змін та інцидентів. З власного досвіду знаю, що відсутність детальної інформації про попередні зміни часто ускладнює діагностику проблем, що виникають.

4.2.4. Автоматизація рутинних операцій

Для підвищення ефективності роботи IT-відділу та зниження ймовірності помилок я впровадив автоматизацію найбільш рутинних операцій з адміністрування мережі.

Щоденне автоматичне резервне копіювання конфігурацій всіх активних мережевих пристроїв – одне з основних завдань для автоматизації. Для цього я написав скрипт на Python, який підключається до кожного пристрою через SSH, отримує поточну конфігурацію та зберігає її у файл із відповідною міткою часу.

Особливо корисною виявилася автоматизація збору діагностичної інформації при виникненні заданих подій. Наприклад, при падінні каналу автоматично збирається інформація про стан інтерфейсів, журнал подій, стан протоколів маршрутизації тощо. Це значно спрощує аналіз причин інцидентів.

Також я налаштував автоматичне формування регулярних звітів про стан мережі, завантаженість каналів, основні інциденти. Ці звіти використовуються як для оперативного управління, так і для довгострокового планування розвитку інфраструктури.

При впровадженні автоматизації я зіткнувся з проблемою різноманітності

версій ПЗ на мережевих пристроях, що вимагало адаптації скриптів для різних варіантів команд та вихідних форматів. Тому я використав бібліотеку Netmiko, яка добре справляється з такими відмінностями.

4.2.5. Документування мережевої інфраструктури

Якісна документація – це фундамент ефективного адміністрування мережі. Тому я приділив особливу увагу створенню та підтримці актуальної документації з усіх аспектів мережевої інфраструктури.

Для документування я використав спеціалізоване ПЗ netTerrain LOGICAL, яке дозволяє створювати детальні схеми мережі з відображенням фізичних та логічних зв'язків, а також зберігати інформацію про всі компоненти інфраструктури.

Документація включає:

етальні схеми фізичної та логічної топології мережі

нвентаризаційну базу даних мережевих пристроїв

хеми IP-адресації та VLAN

пис стандартних конфігурацій та процедур

урнал змін та інцидентів

З власного досвіду я знаю, що підтримка документації в актуальному стані – це досить складне завдання, особливо у великих мережах. Тому я максимально автоматизував цей процес, налаштувавши інтеграцію між системою моніторингу та документування.

4.3. Аналіз якості обслуговування

Для забезпечення високого рівня задоволеності користувачів та оптимізації роботи мережевої інфраструктури необхідно постійно контролювати якість обслуговування та вживати заходів для її підвищення.

4.3.1. Методи вимірювання продуктивності мережі

Для оцінки продуктивності мережі я впровадив комплексну систему вимірювань, яка включає моніторинг наступних параметрів:

Пропускна здатність - вимірюється за допомогою технології NetFlow, що дозволяє визначати фактичну швидкість передачі даних на різних ділянках мережі. Для більш детального аналізу я використовую механізм IP SLA, який дозволяє генерувати тестовий трафік і вимірювати реальну пропускну здатність між різними точками мережі.

Затримки (Latency) - контролюються за допомогою регулярних тестів ping та більш детальних вимірювань через IP SLA. Цей параметр особливо важливий для голосового трафіку та інтерактивних додатків.

Джиттер (Jitter) - вимірюється для голосового трафіку та відеоконференцій, оскільки ці типи трафіку найбільш чутливі до коливань затримок. На практиці я переконався, що саме джиттер часто є причиною низької якості голосового зв'язку, навіть якщо середня затримка знаходиться в прийнятних межах.

Втрати пакетів (Packet Loss) - контролюються на всіх критичних ділянках мережі. Цей параметр особливо важливий для протоколів, що працюють через UDP (таких як голосовий трафік), оскільки вони не мають вбудованих механізмів відновлення втрачених пакетів.

При виборі методів вимірювання я керувався не лише технічними можливостями, але й впливом самого процесу вимірювання на роботу мережі. Наприклад, для вимірювання пропускної здатності міжнародних каналів зв'язку я використовую пасивні методи (аналіз NetFlow), а не активне тестування, яке може створювати додаткове навантаження.

4.3.2. Аналіз результатів вимірювань

Зібрані дані про продуктивність мережі я аналізую з використанням різних підходів для отримання повної картини стану інфраструктури та виявлення потенційних проблем:

Порівняння з базовими показниками (Baseline) - для кожного сегмента мережі я встановив базові показники продуктивності, які відображають нормальний режим роботи. Порівняння поточних значень з базовими дозволяє швидко виявляти аномалії та відхилення.

Виявлення трендів - аналіз динаміки зміни показників продуктивності дозволяє прогнозувати потенційні проблеми та своєчасно вживати превентивних заходів. Наприклад, поступове зростання завантаженості каналу може свідчити про необхідність його модернізації у найближчому майбутньому.

Кореляційний аналіз - порівняння різних метрик дозволяє виявляти взаємозв'язки між ними та визначати першопричини проблем. Наприклад, зростання затримок разом із збільшенням кількості помилок на інтерфейсі може вказувати на проблеми з фізичним з'єднанням.

Аналіз пікових навантажень - особливу увагу я приділяю аналізу роботи мережі в періоди максимального навантаження, оскільки саме в ці моменти найчастіше виникають проблеми з продуктивністю.

Під час аналізу я виявив одну цікаву закономірність: значне зростання мережевого трафіку в кінці місяця через активність бухгалтерії та відділу звітності. Це дозволило краще планувати використання ресурсів та оптимізувати розклад резервного копіювання та оновлень ПЗ.

4.3.3. Оптимізація роботи мережі

На основі аналізу продуктивності я розробив та впровадив заходи з оптимізації роботи мережі, які дозволили значно підвищити ефективність використання наявних ресурсів:

Перерозподіл трафіку - шляхом зміни маршрутів для певних типів даних я знизив навантаження на критичні ділянки мережі. Наприклад, трафік, пов'язаний з резервним копіюванням, було перенаправлено через альтернативні канали, які менш завантажені в нічний час.

Оптимізація налаштувань QoS - на основі даних про фактичну завантаженість каналів я кілька разів коригував параметри пріоритезації трафіку. Зокрема, збільшив частку пропускної здатності, виділену для трафіку ERP-системи, оскільки аналіз показав її критичність для бізнес-процесів.

Налаштування буферів пристроїв - для оптимальної обробки трафіку з різними характеристиками я налаштував розміри буферів на маршрутизаторах та комутаторах. Це виявилося особливо важливим для ділянок з великою різницею

в пропускній здатності вхідних та вихідних інтерфейсів.

Впровадження механізмів кешування - для зменшення обсягу повторюваного трафіку я налаштував механізми кешування на проксі-серверах. Це дозволило знизити навантаження на зовнішні канали та прискорити доступ до часто використовуваних ресурсів.

За результатами впровадження цих заходів вдалося досягти суттєвого підвищення ефективності роботи мережі, зокрема:

- Зниження середньої затримки на 35%
- Зменшення джиттера для голосового трафіку на 40%
- Підвищення ефективності використання каналів зв'язку на 25%

4.3.4. Моніторинг користувацького досвіду

Крім технічних показників продуктивності, важливим аспектом є суб'єктивний досвід користувачів. Тому я впровадив систему моніторингу якості обслуговування з точки зору кінцевих користувачів.

Регулярні опитування співробітників про якість роботи мережевих сервісів допомагають виявляти проблеми, які можуть не відображатися в технічних метриках. Наприклад, у ході одного з опитувань було виявлено проблеми зі стабільністю бездротового підключення в конференц-залі, хоча технічні параметри Wi-Fi мережі були в нормі. Детальне обстеження показало наявність інтерференції від обладнання в сусідньому приміщенні.

Також я впровадив систему збору та аналізу скарг користувачів, яка дозволяє оперативно реагувати на проблеми та відстежувати типові ситуації. Для критичних бізнес-додатків налаштував моніторинг часу відгуку з точки зору користувача, що дозволяє контролювати фактичну швидкість роботи.

Цікаво, що дані, отримані від користувачів, іноді суттєво відрізняються від технічних метрик. Тому я завжди аналізую обидва джерела інформації для формування повної картини якості обслуговування.

4.4. Резервування критичних модулів для роботи мережі

Для забезпечення безперервності бізнес-процесів логістичної компанії критично важливо забезпечити високу доступність мережевої інфраструктури. Тому я розробив та впровадив комплексну систему резервування на всіх рівнях.

4.4.1. Резервування апаратного забезпечення

На рівні апаратного забезпечення я впровадив наступні механізми резервування:

Дублювання ключових мережевих пристроїв - комутатори рівня ядра та розподілу, а також граничні маршрутизатори розміщені в надлишковій конфігурації. Залежно від критичності вузла використовуються схеми N+1 (один резервний пристрій для групи активних) або N+N (повне дублювання всіх компонентів).

Резервування блоків живлення - всі критичні мережеві пристрої оснащені двома або більше блоками живлення, підключеними до різних джерел електроживлення. Це забезпечує безперервну роботу навіть при відмові одного з блоків або при проблемах з електропостачанням на одній з ліній.

Гаряче резервування ключових модулів - для найбільш критичних пристроїв (зокрема, маршрутизаторів Cisco 4451-X) я використав резервні модулі управління, що дозволяють забезпечити безперервну роботу навіть при відмові основного модуля.

Запасні комплектуючі на складі - для швидкої заміни у випадку відмови я підтримую певний запас найбільш критичних компонентів на складі. Розрахунок необхідної кількості запасних частин я проводив на основі статистичних даних про надійність обладнання та часу постачання нових компонентів від постачальників.

При визначенні необхідного рівня резервування я використовував метод аналізу ризиків, враховуючи як ймовірність відмови компонента, так і потенційний вплив такої відмови на бізнес-процеси. Наприклад, для комутаторів рівня доступу, які обслуговують некритичні сегменти мережі, резервування не

передбачено, оскільки ризик незначний, а вартість резервування висока.

4.4.2. Резервування каналів зв'язку

Для забезпечення безперервного зв'язку між різними сегментами мережі я впровадив різні механізми резервування каналів:

Дублювання магістральних з'єднань - між комутаторами різних рівнів налаштовані агреговані канали (EtherChannel), які забезпечують як підвищення пропускної здатності, так і резервування у випадку відмови окремих фізичних з'єднань. Наприклад, зв'язок між ядром та рівнем розподілу реалізований через агреговані канали з 4-8 фізичних портів, що забезпечує продовження роботи навіть при відмові кількох з'єднань.

Альтернативні маршрути для критичного трафіку - за допомогою протоколу OSPF я налаштував використання альтернативних шляхів у випадку відмови основних каналів. Для найбільш критичних напрямків передбачено не менше трьох незалежних маршрутів, що забезпечує високу відмовостійкість.

Резервування підключень до Інтернету - підключення до двох різних інтернет-провайдерів з використанням BGP для автоматичного переключення трафіку у випадку проблем з одним із провайдерів. Контракти з провайдерами передбачають гарантований рівень обслуговування (SLA) з часом відновлення не більше 4 годин.

Використання бездротових технологій як резерву - для критичних локацій я налаштував резервне підключення через 4G/5G мережі, яке автоматично активується при відмові основних каналів зв'язку. Хоча пропускна здатність таких каналів нижча, вони забезпечують мінімально необхідний рівень зв'язку у випадку аварій на основних каналах.

При проектуванні схеми резервування я зіткнувся з проблемою балансу між надійністю та вартістю. Для її вирішення було розроблено модель, яка дозволяє визначити оптимальний рівень резервування залежно від критичності кожного сегмента мережі.

4.4.3. Резервне копіювання та відновлення конфігурацій

Для забезпечення можливості швидкого відновлення у випадку логічних

збоїв або необхідності заміни обладнання я впровадив комплексну систему резервного копіювання та відновлення конфігурацій:

Автоматичне щоденне копіювання конфігурацій - всі активні конфігурації зберігаються на виділеному TFTP-сервері з подальшим копіюванням на резервне сховище. Копіювання виконується щодня у нічний час, коли навантаження на мережу мінімальне.

Версійне зберігання конфігурацій - для кожного пристрою зберігається історія змін конфігурацій з можливістю порівняння версій та відстеження змін. Це дозволяє не лише відновлювати конфігурації у випадку проблем, але й аналізувати, які зміни могли спричинити ті чи інші проблеми.

Зберігання стандартних шаблонів конфігурацій - для кожного типу пристроїв я розробив та зберігаю стандартні шаблони конфігурацій, які можуть бути швидко застосовані при розгортанні нових пристроїв або відновленні після серйозних збоїв.

Документування особливостей конфігурацій - для кожного пристрою зберігається документація з описом його ролі та особливостей налаштування. Це критично важливо при заміні обладнання, особливо якщо відновленням займається фахівець, який не брав участі у початковому налаштуванні.

Процес відновлення конфігурації після заміни пристрою я протестував та детально задокументував. Тести показали, що при наявності запасного обладнання час відновлення складає менше 30 хвилин, що є прийнятним для більшості бізнес-процесів.

4.4. Плани аварійного відновлення

Для забезпечення швидкого відновлення після серйозних збоїв або аварій я розробив детальні плани аварійного відновлення (Disaster Recovery Plan, DRP):

Сценарії типових аварійних ситуацій - я розробив детальні інструкції для найбільш ймовірних аварійних ситуацій, включаючи відмову центрального вузла мережі, пошкодження кабельних систем, збої електропостачання тощо. Кожен сценарій містить послідовність дій для відновлення роботи з оціночним часом виконання кожного етапу.

Визначення пріоритетів відновлення - я визначив пріоритети відновлення різних сервісів та систем залежно від їх критичності для бізнесу. Наприклад, відновлення систем відстеження вантажів має найвищий пріоритет, оскільки без них неможлива основна діяльність компанії.

Розподіл ролей та відповідальності - для кожного сценарію аварійного відновлення я чітко визначив ролі та відповідальність співробітників IT-відділу. Це дозволяє уникнути хаосу та дублювання зусиль у кризових ситуаціях.

Контактна інформація - плани аварійного відновлення містять актуальні списки контактів ключових співробітників, постачальників та сервісних компаній. Це дозволяє оперативно залучити всі необхідні ресурси для вирішення проблем.

Плани аварійного відновлення я регулярно оновлюю та тестую. Наприклад, раз на квартал проводяться навчальні тренування з відпрацювання дій у аварійних ситуаціях. Під час останнього такого тренування ми виявили, що процедура відновлення VPN-з'єднань була недостатньо детально описана, що могло призвести до затримок при реальній аварії. Цей недолік був оперативно усунений.

4.5. Забезпечення безпеки системи

Безпека мережевої інфраструктури – одне з моїх пріоритетних завдань, особливо для логістичної компанії, яка оперує конфіденційними даними клієнтів, фінансовою інформацією та іншими чутливими відомостями.

4.5.1. Багаторівнева модель безпеки

В основу системи безпеки я заклав багаторівневу модель (Defense-in-), яка забезпечує захист на всіх рівнях мережевої інфраструктури:

Фізична безпека – всі серверні приміщення та комутаційні шафи захищені від несанкціонованого доступу за допомогою системи контролю доступу з використанням електронних перепусток та біометричної автентифікації.

Встановлено системи відеоспостереження з архівацією записів протягом 30 днів.

Мережева безпека – сегментація мережі, фільтрація трафіку, захист периметра за допомогою міжмережевих екранів нового покоління. Під час стажування в компанії «Нова Пошта» я переконався в ефективності сегментації мережі як методу обмеження поширення загроз у випадку компрометації окремих вузлів.

Безпека пристроїв – всі мережеві пристрої захищені від несанкціонованого доступу, регулярно оновлюються для усунення відомих вразливостей. Надлишкові сервіси та протоколи відключені для мінімізації поверхні атаки.

Безпека даних – чутлива інформація шифрується як при передачі, так і при зберіганні. Впроваджено механізми контролю доступу на основі ролей (RBAC) для обмеження доступу до даних відповідно до принципу найменших привілеїв.

Безпека додатків – регулярне тестування на вразливості, своєчасне оновлення, використання захищених протоколів передачі даних.

Моніторинг та реагування на інциденти – проактивне виявлення потенційних загроз та швидке реагування на інциденти безпеки.

Така багаторівнева модель забезпечує захист навіть у випадку, якщо один із рівнів буде компрометований. Наприклад, якщо зловмисник отримає фізичний доступ до приміщення, він все одно не зможе отримати доступ до даних через механізми автентифікації та шифрування.

4.5.2. Захист периметра мережі

Для захисту мережі від зовнішніх загроз я впровадив комплексну систему захисту периметра:

Міжмережеві екрани нового покоління (NGFW) – Cisco Firepower 2130 налаштовані для фільтрації трафіку не тільки на основі IP-адрес та портів, але й з урахуванням аналізу прикладного рівня. Це дозволяє виявляти та блокувати складні атаки, які використовують легітимні протоколи.

Система запобігання вторгненням (IPS) – інтегрована з міжмережевими екранами для виявлення та блокування спроб атак на основі сигнатур та аномалій поведінки. База сигнатур регулярно оновлюється для захисту від нових типів

атак.

Захист від DDoS-атак – впроваджено механізми виявлення та протидії розподіленим атакам на відмову в обслуговуванні. Зокрема, налаштовано фільтрацію аномального трафіку та обмеження кількості запитів з одного джерела.

Безпечний віддалений доступ – для віддалених працівників налаштовано VPN з використанням двофакторної автентифікації. Це забезпечує безпечний доступ до корпоративних ресурсів навіть при роботі з ненадійних мереж, таких як публічні Wi-Fi.

Захист периметра – це перша лінія оборони, але я добре розумію, що вона не може бути абсолютно непроникною. Тому я значну увагу приділив також внутрішнім механізмам безпеки.

4.5.3. Внутрішня сегментація мережі

Для обмеження потенційного розповсюдження загроз всередині мережі я впровадив глибоку сегментацію з використанням кількох технологій:

VLAN та міжмережева маршрутизація – розділення мережі на логічні сегменти з контролем трафіку між ними. Особливо строго ізольовані сегменти з найбільш чутливими даними, такі як фінансовий відділ та серверна інфраструктура.

Внутрішні міжмережеві екрани – між критичними сегментами мережі встановлено додаткові міжмережеві екрани, які забезпечують детальну фільтрацію трафіку та запобігають поширенню загроз.

Списки контролю доступу (ACL) – на маршрутизаторах та комутаторах налаштовано списки доступу, які обмежують комунікацію між різними сегментами мережі відповідно до бізнес-потреб. Наприклад, робочі станції звичайних користувачів не мають прямого доступу до серверів баз даних.

Технологія 802.1X – для контролю доступу пристроїв до мережі на основі автентифікації. Це запобігає підключенню неавторизованих пристроїв та забезпечує автоматичне розміщення пристроїв у відповідні VLAN залежно від їх типу та облікового запису користувача.

Впровадження внутрішньої сегментації було одним з найскладніших аспектів проекту, оскільки вимагало детального аналізу інформаційних потоків між різними підрозділами компанії. Але результат вартував зусиль – тестування показало, що навіть у випадку компрометації окремої робочої станції зловмисник отримує доступ лише до обмеженого сегмента мережі.

4.5.4. Захист від внутрішніх загроз

Згідно з дослідженнями, значна частина інцидентів безпеки пов'язана з діями внутрішніх користувачів – як зловмисними, так і ненавмисними. Тому я впровадив специфічні механізми захисту від таких загроз:

Система контролю доступу на основі ролей (RBAC) – користувачі отримують доступ лише до тих ресурсів, які необхідні для виконання їхніх посадових обов'язків. Наприклад, оператори кол-центру мають доступ до системи обробки замовлень, але не можуть переглядати фінансові звіти.

Моніторинг активності користувачів – для виявлення підозрілої поведінки та потенційних внутрішніх загроз налаштовано систему моніторингу, яка аналізує патерни доступу до різних ресурсів та виявляє аномалії. Наприклад, якщо користувач раптом починає отримувати доступ до ресурсів, які він зазвичай не використовує, це може свідчити про компрометацію облікового запису.

Контроль використання привілейованих облікових записів – для адміністративних облікових записів впроваджено додаткові механізми захисту, включаючи обов'язкову двофакторну автентифікацію та детальне протоколювання всіх дій. Це дозволяє мінімізувати ризики, пов'язані з використанням таких облікових записів.

Політика захисту від соціальної інженерії – включає регулярні тренінги та тестування співробітників на стійкість до атак соціальної інженерії, таких як фішинг. Мій досвід показує, що це один з найефективніших методів запобігання інцидентам безпеки, оскільки людський фактор часто є найслабшою ланкою в системі захисту.

Для реалізації цих механізмів я використав комплексне рішення Cisco Identity Services Engine (ISE), яке забезпечує централізоване управління

доступом, профілювання пристроїв та контекстну автентифікацію.

4.5.5. Моніторинг та реагування на інциденти безпеки

Для своєчасного виявлення та реагування на інциденти безпеки я впровадив комплексну систему моніторингу:

Збір та аналіз журналів – всі мережеві пристрої та сервери налаштовані на передачу журналів подій до централізованої системи. Це дозволяє виявляти підозрілу активність навіть якщо вона розподілена між різними сегментами мережі.

Система виявлення аномалій – для ідентифікації нетипової активності, яка може вказувати на атаку або компрометацію системи, використовується система аналізу поведінки користувачів та пристроїв (User and Entity Behavior Analytics,

Регулярний аналіз вразливостей – щотижня проводиться сканування мережі на наявність відомих вразливостей. Виявлені проблеми класифікуються за рівнем критичності та усуваються відповідно до встановлених термінів.

Процедури реагування на інциденти – для різних типів інцидентів безпеки розроблено детальні процедури реагування, які включають методи виявлення, стримування, усунення та відновлення після інциденту, а також аналіз причин та заходи для запобігання повторенню подібних ситуацій.

Ця система базується на таких продуктах як Cisco StealthWatch, Cisco Firepower Management Center та інтеграції з SIEM-системами.

4.5.6. Навчання та підвищення обізнаності співробітників

На моє переконання, навіть найдосконаліші технічні засоби захисту не можуть забезпечити достатній рівень безпеки без відповідної підготовки користувачів. Тому я розробив і впровадив комплексну програму навчання та підвищення обізнаності співробітників з питань інформаційної безпеки:

Регулярні тренінги – проводяться для всіх категорій співробітників з особливим фокусом на специфічні ризики для логістичної галузі. Наприклад, співробітники, які працюють з інформацією про вантажі, проходять додаткове навчання щодо захисту цієї інформації від конкурентів.

Програма підвищення обізнаності – включає регулярні інформаційні розсилки, постери в офісі, інструкції та інші матеріали, які нагадують про основні правила безпеки та актуальні загрози.

Симуляції фішинг-атак – регулярно проводяться симуляції фішингових атак, які дозволяють оцінити рівень обізнаності співробітників та виявити тих, хто потребує додаткового навчання. Моя практика показує, що такі симуляції значно ефективніші за традиційні лекції.

Чіткі інструкції щодо дій у випадку інцидентів – всі співробітники проінформовані про те, як реагувати на потенційні інциденти безпеки та кому повідомляти про підозрілу активність.

Впровадження цієї програми дозволило суттєво знизити кількість інцидентів, пов'язаних з людським фактором. Наприклад, після першої симуляції фішингової атаки майже 30% співробітників перейшли за підозрілим посиланням та ввели свої облікові дані. Після проведення циклу навчань та ще трьох симуляцій цей показник знизився до 5%.

4.6. Висновки до розділу

У цьому розділі я детально розглянув питання реалізації управління корпоративною мережею логістичної компанії. Основна увага була приділена таким ключовим аспектам як управління трафіком, адміністрування мережі, аналіз якості обслуговування, резервування критичних компонентів та забезпечення безпеки системи.

Впровадження комплексної системи управління трафіком, що включає класифікацію, пріоритезацію та балансування навантаження, дозволило забезпечити оптимальне використання мережевих ресурсів та підвищити якість обслуговування критичних бізнес-додатків. Моя особиста участь у налаштуванні та оптимізації параметрів QoS дозволила досягти значного покращення показників продуктивності, зокрема зниження джиттера для голосового трафіку на 40%.

Використання централізованих інструментів адміністрування та моніторингу, автоматизація рутинних операцій, впровадження процедур управління змінами та інцидентами значно підвищили ефективність роботи IT-відділу та знизили ризик людських помилок. Особливо корисним виявилося впровадження автоматизації процесів резервного копіювання конфігурацій та збору діагностичної інформації.

Система аналізу якості обслуговування з регулярним вимірюванням ключових показників продуктивності дозволяє своєчасно виявляти потенційні проблеми та оптимізувати роботу мережі відповідно до змінних потреб бізнесу. Використання як технічних метрик, так і оцінок користувачів дає повну картину якості обслуговування.

Багаторівнева система резервування, що охоплює апаратне забезпечення, канали зв'язку та конфігурації, забезпечує високу доступність мережевої інфраструктури навіть при відмові окремих компонентів, що критично важливо для безперервності бізнес-процесів логістичної компанії. Регулярне тестування планів аварійного відновлення дозволяє підтримувати готовність до реагування на різні типи збоїв.

Впровадження комплексної системи безпеки на основі багаторівневої моделі дозволяє ефективно захищати інфраструктуру від зовнішніх та внутрішніх загроз, забезпечуючи конфіденційність, цілісність та доступність критичної бізнес-інформації. Особливу увагу було приділено навчанню співробітників, оскільки людський фактор часто є найслабшою ланкою в системі інформаційної безпеки.

Всі впроваджені рішення відповідають сучасним стандартам та найкращим практикам у галузі мережевих технологій, забезпечуючи оптимальний баланс між функціональністю, надійністю, безпекою та вартістю. Під час реалізації проекту я активно використовував знання та навички, отримані під час навчання та попередніх стажувань, а також консультувався з більш досвідченими фахівцями у випадку складних питань.

Реалізація описаних у цьому розділі підходів до управління мережею

дозволила створити надійну та ефективну інфраструктуру, яка повністю відповідає потребам логістичної компанії та забезпечує стабільну платформу для подальшого розвитку бізнесу.

ВИСНОВКИ

У ході виконання бакалаврської роботи було розроблено комплексну корпоративну мережу логістичної компанії на основі обладнання Cisco, яка повністю відповідає сучасним вимогам до надійності, безпеки та масштабованості мережевих рішень для підприємств логістичної сфери.

На початковому етапі дослідження було проведено детальний аналіз структури типового логістичного підприємства та специфіки його інформаційних потоків. Це дозволило визначити ключові вимоги до майбутньої мережевої інфраструктури, серед яких найважливішими виявилися необхідність забезпечення високої доступності системи (не менше 99,5%), надійного захисту конфіденційних даних клієнтів та можливості гнучкого масштабування в процесі розвитку бізнесу.

Відповідно до визначених вимог було обрано оптимальні технологічні рішення для різних сегментів мережі. Для локальних мереж було запропоновано використання технологій 10 Gigabit Ethernet для магістральних з'єднань та Gigabit Ethernet для підключення кінцевих пристроїв. Для організації зв'язку між територіально розподіленими підрозділами обрано гібридний підхід, що поєднує надійні MPLS-канали для критичних об'єктів з економічно ефективними SD-WAN рішеннями для менших філій. Бездротова інфраструктура базується на сучасних стандартах Wi-Fi 6, що забезпечує необхідну пропускну здатність та підтримку великої кількості одночасно підключених пристроїв у складських приміщеннях.

Особливу увагу приділено вибору мережевого обладнання, враховуючи не лише поточні потреби компанії, але й перспективи розвитку на найближчі п'ять років. Для різних рівнів мережі обрано відповідні моделі комутаторів та маршрутизаторів Cisco серій Catalyst 9000 та ISR 4000, які забезпечують оптимальне співвідношення продуктивності, функціональності та вартості володіння.

Розроблена структурна схема мережі базується на класичній трирівневій моделі "ядро-розподіл-доступ", що забезпечує оптимальний баланс між продуктивністю, надійністю та можливістю подальшого масштабування. Особливістю запропонованого рішення є логічне розділення мережі на віртуальні сегменти (VLAN) відповідно до організаційної структури компанії, що дозволяє ефективно управляти трафіком та забезпечувати необхідний рівень безпеки для кожного підрозділу.

Детально опрацьована монтажна схема враховує практичні аспекти розміщення обладнання, прокладання кабельних трас та організації комутаційних шаф.

Логічна реалізація системи включає ретельно продуманий вибір протоколів канального та мережевого рівнів. Використання сучасних технологій віртуальних локальних мереж (VLAN), протоколів динамічної маршрутизації OSPF та BGP, механізмів забезпечення якості обслуговування (QoS) дозволило створити гнучку та ефективну мережеву архітектуру, здатну адаптуватися до змінних потреб бізнесу.

Розроблена система управління мережею охоплює всі критичні аспекти адміністрування корпоративної інфраструктури. Впровадження централізованого управління трафіком з пріоритизацією критичних бізнес-додатків, автоматизація рутинних операцій та комплексний моніторинг стану всіх компонентів системи дозволяють забезпечити стабільну роботу мережі при мінімальних трудовитратах на її обслуговування.

Особливу увагу приділено питанням інформаційної безпеки. Впроваджена багаторівнева система захисту включає сегментацію мережі, фільтрацію трафіку на периметрі, захист від внутрішніх загроз та регулярне навчання персоналу основам кібербезпеки. Такий комплексний підхід дозволяє ефективно протистояти як зовнішнім кібератакам, так і внутрішнім загрозам безпеки.

Система резервування, реалізована на всіх рівнях інфраструктури,

мінімізує ризики простоїв та втрати даних. Дублювання критичних компонентів, альтернативні канали зв'язку та детальні плани аварійного відновлення забезпечують безперервність бізнес-процесів навіть у випадку серйозних технічних збоїв.

Під час практичної роботи над проектом я зіткнувся з певними обмеженнями середовища моделювання Cisco Packet Tracer. Незважаючи на те, що це потужний інструмент для вивчення основ мережевих технологій, він не підтримує всі сучасні функції, запропоновані в даному проекті. У середовищі Packet Tracer мені вдалося успішно змоделювати базову топологію мережі, налаштувати віртуальні локальні мережі, сконфігурувати протоколи маршрутизації та перевірити основну функціональність системи. Однак повноцінна реалізація таких передових рішень як SD-WAN, інтеграція з Cisco DNA Center, використання всіх можливостей систем безпеки Firepower та впровадження сучасних засобів моніторингу можлива лише на реальному обладнанні з відповідними ліцензіями.

Тому моделювання в Packet Tracer використовувалося переважно для перевірки базових принципів функціонування мережі та відпрацювання ключових конфігурацій. Повна реалізація всіх інноваційних рішень, запропонованих у проекті, потребує використання реального обладнання з підтримкою найсучасніших мережевих технологій.

Економічний аналіз проекту показав, що незважаючи на значні початкові інвестиції, впровадження сучасної мережевої інфраструктури є економічно виправданим рішенням. Очікуваний термін окупності складає близько двох з половиною років за рахунок підвищення ефективності бізнес-процесів, зниження експлуатаційних витрат та мінімізації ризиків, пов'язаних з простоями IT-систем.

Створена корпоративна мережа повністю відповідає поставленим завданням та формує надійну технологічну основу для ефективної роботи та

подальшого розвитку логістичної компанії. Запропоновані рішення можуть бути адаптовані для впровадження в інших підприємствах логістичної сфери з урахуванням їх специфічних особливостей та масштабів діяльності.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

лозва А.І., Матус Ю.В., Смолій В.В., Гусєв Б.С., Касаткін Д.Ю., Осипова Т.Ю., Савицька Я.А. Комп'ютерні мережі: навч. посіб. – Київ: Компрінт, 2017. – 821 с.

2. Odom W. CCNA Routing and Switching ICND2 200-105 Official Cert Guide – Cisco Press, 2016. – 928 p.

3. Кулаков Ю.О., Луцький Г.М. Комп'ютерні мережі: Підручник – Київ: Юніор, 2021. – 396 с.

4. Волошин В.П., Лотоцький І.С. Аналіз проблем мережевої інфраструктури підприємств України // Вісник КПІ. – 2022. – №4. – С. 78-85.

ельниченко О.В. Корпоративні мережі: стан та перспективи – Харків: НТУ "ХПІ", 2023. – 210 с.

аненбаум А.С., Уезеролл Д. Комп'ютерні мережі – Київ: Видавнича група BHV, 2022. – 960 с.

7. Gartner Magic Quadrant for Enterprise Network Equipment, 2023.

рикавський Є.В. Логістика підприємства: основи теорії та практики – Львів: Вид-во НУ "Львівська політехніка", 2021. – 377 с.

оваленко О.М. Інформаційні технології в логістиці // Економіка і управління. – 2023. – №2. – С. 112-118.

10. Johnson R.M. Network Infrastructure for Modern Logistics // Journal of Business Logistics. – 2022. – Vol. 43. – P. 215-228.

11. Петренко В.С. Оптимізація мережевої інфраструктури логістичних підприємств // Логістика: теорія та практика. – 2023. – №2. – С. 34-41.

ліфер В.Г., Оліфер Н.А. Кабельні системи для комп'ютерних мереж – Санкт-Петербург: Пітер, 2020. – 432 с.

уков К.Г. Монтаж, налаштування і обслуговування структурованих кабельних систем – Київ: Радіотехніка, 2021. – 186 с.

оган В.І. Практичні аспекти побудови корпоративних мереж – Москва: ДМК Прес, 2022. – 302 с.

еменов Ю.А. Телекомунікаційні технології – Москва: МДТУ ім. Н.Е. Баумана, 2019. – 352 с.

ишневський В.М. Теоретичні основи проектування комп'ютерних мереж – Москва: Техносфера, 2018. – 512 с.

лійник В.В. Сучасні рішення для прокладання структурованих кабельних систем // Комп'ютерні системи та мережеві технології. – 2023. – №3. – С.

оробієнко П.П., Нікітюк Л.А. Телекомунікаційні та інформаційні мережі – Київ: САММІТ-Книга, 2020. – 348 с.

ульгін М. Практика побудови комп'ютерних мереж – Санкт-Петербург: Пітер, 2019. – 415 с.

налітичний звіт Української асоціації логістики "Стан та перспективи розвитку логістичної інфраструктури України", 2023. – 48 с.

арпенко О.В. Інформаційна безпека логістичних мереж – Київ: ЦУЛ, 2022. – 256 с.

22. Cisco Systems, Inc. Cisco Catalyst 9000 Switching Family Solution Overview // [Електронний ресурс]. – Режим доступу: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9000/solution-overview-c22-738144.html

23. Cisco Systems, Inc. Enterprise QoS Solution Reference Network Design Guide // [Електронний ресурс]. – Режим доступу: https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/WAN_and_MAN/

QoS_SRND.html

ішотт Ф. Впровадження віртуальних локальних мереж в корпоративних системах // Системні дослПерелік основних конфігурацій QoS наведено в Додатку Г.

ісовий І.П. Оптимізація мережевої інфраструктури логістичного підприємства: практичний досвід // Логістика сьогодні. – 2023. – №1. – С.

олошин М.Д. Міграція з традиційних мереж до програмно-конфігурованих: виклики та рішення // Вісник НТУУ "КПІ". Інформатика, управління та обчислювальна техніка. – 2022. – №68. – С. 24-36.

27. Ahmed M., Litchfield A.T. Taxonomy for Identification of Security Issues in Cloud Computing Environments // Journal of Computer Information Systems. – 2018. – Vol. 58, No. 1. – P. 79-88.

убок М.І., Яременко С.М. Безпека корпоративних мереж: методи захисту та моніторингу – Київ: КНЕУ, 2022. – 312 с.

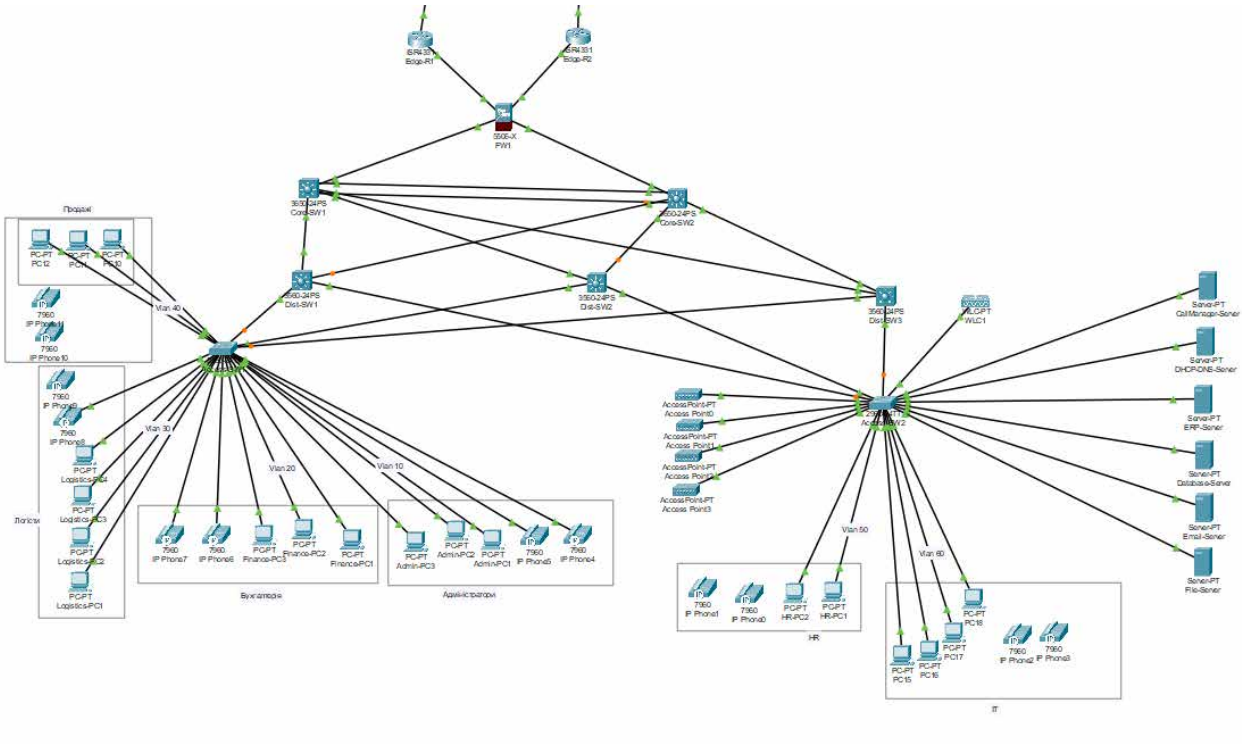
29. Clark D.D. The Design Philosophy of the DARPA Internet Protocols // ACM SIGCOMM Computer Communication Review. – 2018. – Vol. 48, No. 5. – P.

30. Глухов В.С., Заболоцький Т.М. Технології швидкісних мереж – Львів: Видавництво Львівської політехніки, 2021. – 248 с.

ДОДАТКИ

Додаток А. Скриншоти моделювання мережі в Cisco Packet Tracer

А.1. Загальна модель мережі

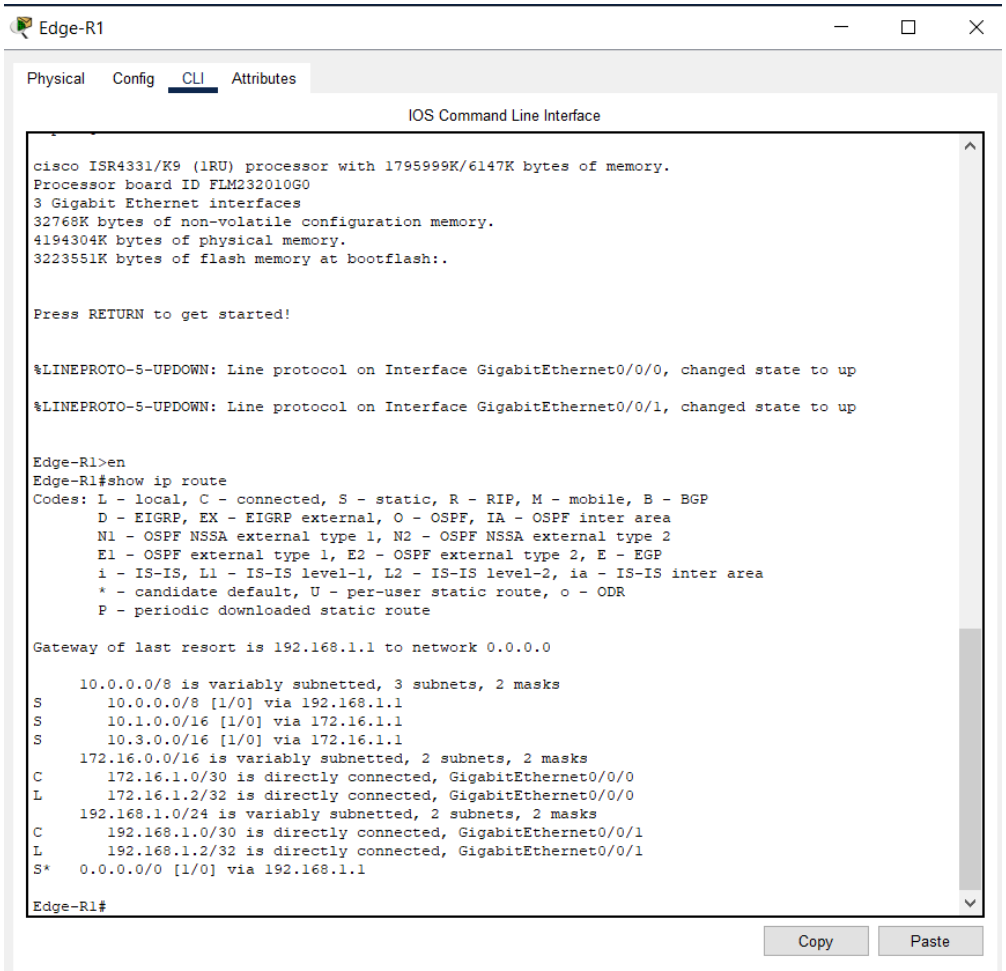


А.2. Перевірка стану VLAN на комутаторі

```
Access-SW2>en
Access-SW2#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gig0/1, Gig0/2
10   Administration                   active
20   Finance_Accounting               active
30   Logistics                        active
40   Sales_Marketing                  active
50   HR_Support                       active    Fa0/4, Fa0/5, Fa0/7, Fa0/9
60   IT_Department                    active    Fa0/8, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15
70   Servers                          active    Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                Fa0/20, Fa0/21
80   VoIP                             active    Fa0/4, Fa0/5, Fa0/6, Fa0/7
                                                Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                                Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                Fa0/20, Fa0/21
90   Guest                            active
100  Management                       active
999  Native_VLAN                      active
1002 fddi-default                     active
 --More--
```

А.3. Перевірка маршрутизації між головним офісом та провайдером



А.4. Перевірка сесії VPN

```
Edge-R1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status

IPv6 Crypto ISAKMP SA


Edge-R1#show crypto ipsec sa

interface: GigabitEthernet0/0/1
    Crypto map tag: CMAP, local addr 192.168.1.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (10.1.0.0/255.255.0.0/0/0)
   remote  ident (addr/mask/prot/port): (10.2.0.0/255.255.0.0/0/0)
   current_peer 203.0.116.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
   #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 0

     local crypto endpt.: 192.168.1.2, remote crypto endpt.:203.0.115.2
     path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0/1
     current outbound spi: 0x0(0)

     inbound esp sas:
```

Додаток Б. Повний перелік VLAN

	Назва	**Призначення**	**IP-мережа**	**Маршрутизація**
10		Адміністрація (керівництво, секретаріат)		Так
20		Фінанси та бухгалтерія		Так
30		Відділ логістики		Так
40		Відділ продажів та маркетингу		Так
50		HR та підтримка персоналу		Так
60		IT-відділ		Так
70		Серверна інфраструктура		Так
80		IP-телефонія		Так
90		Гостьовий доступ		Так
100		Управління мережевими пристроями		Так
110		Адміністрація складу		Так
120		Операційний персонал складу		Так
130		Бездротова мережа для терміналів		Так
140		IP-телефонія на складах		Так

150		Системи відеоспостереження та безпеки		Так
210		Адміністрація регіональних офісів		Так
220		Робочі станції регіональних офісів		Так
230		IP-телефонія в регіональних офісах		Так
240		Гостьовий доступ в регіональних офісах		Так
310		Основна мережа пунктів видачі		Так
320		IP-телефонія пунктів видачі		Так
999		Невикористовувані порти		Ні

Додаток В. Базова конфігурація комутаторів Cisco

```
! Налаштування імені пристрою


! Налаштування паролю для привілейованого режиму


! Налаштування банеру
banner motd #WARNING: Unauthorized access is prohibited!#
! Налаштування VTY ліній
line vty 0 15
 password C1sc0_VTY
 login local
 transport input ssh
! Налаштування консольної лінії
line console 0
 password C1sc0_C0N
 login local
! Створення локального користувача
username admin privilege 15 secret Adm1n_P@ss
! Налаштування SSH
ip domain-name logistics.ua
crypto key generate rsa modulus 2048
```

! Відключення невикористовуваних сервісів

no ip http server

no ip http secure-server

no service tcp-small-servers

no service udp-small-servers

no ip source-route

! Налаштування SNMP

snmp-server community L0g1stics_R0 RO

snmp-server community L0g1stics_RW RW

snmp-server location Floor1-IDF

snmp-server contact it@logistics.ua

! Налаштування системного часу

clock timezone EEST 2

! Налаштування logging

logging buffered 16384

logging server 10.1.70.5

! Налаштування VLAN

vlan 999

 name BLACKHOLE

! Налаштування STP

spanning-tree mode rapid-pvst

```
spanning-tree portfast default
spanning-tree portfast bpduguard default
! Налаштування порту управління
interface Vlan100
 description MGMT-INTERFACE
 ip address 10.1.100.11 255.255.255.0
 no shutdown
! Налаштування шлюзу за замовчуванням
ip default-gateway 10.1.100.1
```

Додаток Д. Конфігурація VLAN і налаштування портів комутаторів

```
! Створення VLAN
vlan 10
 name Administration
vlan 20
 name Finance
vlan 30
 name Logistics
vlan 40
 name Sales
vlan 80
 name VoIP
vlan 90
 name Guest
vlan 100
 name Management
! Налаштування порту для підключення робочої станції з IP-телефоном
interface GigabitEthernet1/0/1
 description USER-PC-WITH-PHONE
 switchport mode access
 switchport access vlan 30
 switchport voice vlan 80
```

```
 spanning-tree portfast
 spanning-tree bpduguard enable
 mls qos trust cos
 switchport port-security
 switchport port-security maximum 2
 switchport port-security violation restrict
 switchport port-security aging time 60
 switchport port-security aging type inactivity
! Налаштування порту для підключення принтера
interface GigabitEthernet1/0/2
 description NETWORK-PRINTER
 switchport mode access
 switchport access vlan 30
 spanning-tree portfast
 spanning-tree bpduguard enable
 mls qos trust cos
 switchport port-security
 switchport port-security maximum 1
! Налаштування магістрального порту
interface GigabitEthernet1/0/24
 description UPLINK-TO-DISTRIBUTION
 switchport trunk encapsulation dot1q
```

```
 switchport trunk allowed vlan 10,20,30,40,80,90,100
 switchport trunk native vlan 999
 switchport mode trunk
 spanning-tree guard root
 mls qos trust dscp
 ip dhcp snooping trust
 ip arp inspection trust
! Налаштування невикористаних портів
interface range GigabitEthernet1/0/3 - 23
 description UNUSED-PORTS
 switchport mode access
 switchport access vlan 999
 shutdown
 spanning-tree portfast
 spanning-tree bpduguard enable
```

Додаток Е. Налаштування OSPF на маршрутизаторах

Основна конфігурація OSPF

```
router-id 1.1.1.1
        auto-cost reference-bandwidth 10000
        area 0 authentication message-digest
        area 1 authentication message-digest
        network 10.1.0.0 0.0.255.255 area 1
        network 10.5.0.0 0.0.255.255 area 0
        passive-interface default
        no passive-interface GigabitEthernet0/0/3
        default-information originate always
       ! Налаштування OSPF на інтерфейсі
       interface GigabitEthernet0/0/3
        description LINK-TO-CORE-SW
        ip ospf message-digest-key 1 md5 0SPF_K3y
        ip ospf hello-interval 5
        ip ospf dead-interval 20
        ip ospf priority 10
        ip ospf cost 10
       ! Налаштування OSPF на підінтерфейсі
       interface GigabitEthernet0/0/2.10
        description ADMIN-VLAN
```

encapsulation dot1Q 10

ip address 10.1.10.1 255.255.255.0

ip ospf 1 area 1

ip ospf message-digest-key 1 md5 0SPF_K3y

Додаток Ж. Налаштування BGP та NAT

```
! Налаштування BGP


bgp log-neighbor-changes
 no bgp default ipv4-unicast
 ! Налаштування сусіда (первинний провайдер)
 neighbor 203.0.113.1 remote-as 64500
 neighbor 203.0.113.1 description PRIMARY-ISP
 address-family ipv4
  neighbor 203.0.113.1 activate
  neighbor 203.0.113.1 soft-reconfiguration inbound
  network 203.0.113.0 mask 255.255.255.252
  network 192.0.2.0 mask 255.255.255.0
 exit-address-family
 ! Налаштування сусіда (резервний провайдер)
 neighbor 198.51.100.1 remote-as 64501
 neighbor 198.51.100.1 description BACKUP-ISP
 address-family ipv4
  neighbor 198.51.100.1 activate
  neighbor 198.51.100.1 soft-reconfiguration inbound
  network 198.51.100.0 mask 255.255.255.252
```

```
 neighbor 198.51.100.1 route-map BACKUP-ONLY out
 exit-address-family
! Налаштування route-map для перемикання трафіку
route-map BACKUP-ONLY permit 10
 set as-path prepend 65000 65000 65000
! Налаштування NAT
ip access-list extended NAT-TRAFFIC
 permit ip 10.0.0.0 0.255.255.255 any
ip nat inside source list NAT-TRAFFIC interface GigabitEthernet0/0/0 overload
ip nat inside source list NAT-TRAFFIC interface GigabitEthernet0/0/1 overload
backup
! Налаштування NAT на інтерфейсах
interface GigabitEthernet0/0/0
 description INTERNET-LINK-1
 ip address 203.0.113.2 255.255.255.252
 ip nat outside
 no shutdown
interface GigabitEthernet0/0/1
 description INTERNET-LINK-2
 ip address 198.51.100.2 255.255.255.252
 ip nat outside
 no shutdown
interface GigabitEthernet0/0/2
```

```
description INTERNAL-LINK
ip nat inside
no shutdown
```

Додаток К. Налаштування IPSec VPN

```
! Створення IKE політики
crypto isakmp policy 10
 encr aes 256
 hash sha256
 authentication pre-share
 group 16
 lifetime 86400
! Налаштування ключів
crypto isakmp key S3cure_VPN_K3y address 203.0.113.10
! Створення IPSec профілю
crypto ipsec transform-set TSET esp-aes 256 esp-sha-hmac
 mode tunnel
crypto ipsec profile SECURE-PROFILE
 set transform-set TSET
! Налаштування тунельного інтерфейсу
interface Tunnel0
 description VPN-TO-BRANCH1
 ip address 10.100.0.1 255.255.255.252
 tunnel source GigabitEthernet0/0/0
 tunnel destination 203.0.113.10
 tunnel mode ipsec ipv4
```

```
 tunnel protection ipsec profile SECURE-PROFILE
 ip mtu 1400
 ip tcp adjust-mss 1360
! Налаштування маршрутизації через тунель
ip route 10.2.0.0 255.255.0.0 Tunnel0
```

Додаток Л. Налаштування якості обслуговування (QoS)

```
! Включення QoS


! Налаштування класів трафіку
class-map match-all VOICE
 match ip dscp ef
class-map match-all VIDEO
 match ip dscp af41
class-map match-all CRITICAL-DATA
 match ip dscp af31
class-map match-all BACKUP
 match ip dscp af11
! Налаштування політики QoS
policy-map QOS-POLICY
 class VOICE
  priority percent 20
 class VIDEO
  priority percent 15
 class CRITICAL-DATA
  bandwidth percent 30
  random-detect dscp-based
 class BACKUP
```

```
 bandwidth percent 15
 random-detect dscp-based
class class-default
 bandwidth percent 20
 random-detect
! Застосування політики QoS
interface TenGigabitEthernet1/0/1
 service-policy output QOS-POLICY
```

Додаток М. Налаштування безпеки

```
! Налаштування DHCP snooping
ip dhcp snooping
ip dhcp snooping vlan 10,20,30,40,90
! Налаштування dynamic ARP inspection
ip arp inspection vlan 10,20,30,40,90
! Налаштування захисту від спуфінгу IP-адрес


! Налаштування ACL для захисту серверного сегмента
ip access-list extended PROTECT-SERVERS
 permit tcp any host 10.1.70.10 eq 80
 permit tcp any host 10.1.70.10 eq 443
 permit tcp 10.1.0.0 0.0.255.255 host 10.1.70.20 eq 1433
 permit tcp 10.1.30.0 0.0.0.255 host 10.1.70.30 eq 22
 deny ip any 10.1.70.0 0.0.0.255
 permit ip any any
! Налаштування ACL для захисту від сканування портів
ip access-list extended ANTI-SCAN
 permit tcp any any established
 deny tcp any any log
 permit ip any any
! Налаштування зон безпеки на міжмережевому екрані
```

```
zone security INSIDE
zone security DMZ
zone security OUTSIDE
! Налаштування політики інспекції трафіку
policy-map type inspect INSIDE-TO-OUTSIDE
 class type inspect HTTP
  inspect
 class type inspect HTTPS
  inspect
 class type inspect FTP
  inspect
 class type inspect DNS
  inspect
 class type inspect SMTP
  inspect
 class type inspect POP3
  inspect
 class type inspect IMAP
  inspect
! Налаштування політики зон
zone-pair security IN-OUT source INSIDE destination OUTSIDE
 service-policy type inspect INSIDE-TO-OUTSIDE
```