ДВНЗ «Донецький національний технічний університет»
Навчально-науковий інститут комп'ютерно-інформаційних технологій та автоматизації
(повне найменування інституту, назва факультету)
Кафедра автоматики та телекомунікацій
(повна назва кафедри)

«До захисту допущено»
Завідувач кафедри автоматики та телекомунікацій
_____ Валерій ПОЦЕПАЄВ
(підпис) (ім'я та прізвище)
«___» _____ 2025 р.

Випускна кваліфікаційна робота

бакалавра
(освітньо-кваліфікаційний рівень)

на тему «Модернізація телекомунікаційної інфраструктури для мережі магазинів взуття «Лідер взуття»

Виконав студент 4 курсу, групи ТКР-21
(шифр групи)

спеціальності 172 Телекомунікації та радіотехніка
(шифр і назва спеціальності)

Манич Сергій Вадимович
(Прізвище, Ім'я та По-батькові) (підпис)

Керівник ст. викладач каф. АТ _____ Гліб СТУПАК
(посада, науковий ступінь, вчене звання, прізвище та ім'я) (підпис)

Рецензент зав. каф.ЕЛІН, к.т.н., доц. _____ Олександр КОЛЛАРОВ
(посада, науковий ступінь, вчене звання, прізвище та ім'я) (підпис)

Нормоконтроль:
Дар'я ЖУКОВСЬКА
18.06.2025 р.

Засвідчую, що у цій випускній кваліфікаційній роботі немає запозичень з праць інших авторів без відповідних посилань.

Студент _____
(підпис)

Дрогобич – 2025 р.

ДВНЗ «Донецький національний технічний університет»
Навчально-науковий інститут комп'ютерно-інформаційних технологій та автоматизації
(повне найменування інституту, назва факультету)
Кафедра автоматики та телекомунікацій
(повна назва кафедри)

Захист відбувся _____
(дата)
з оцінкою_____
Секретар ЕК _____
(підпис)

Випускна кваліфікаційна робота

бакалавра

Тема: «Модернізація телекомунікаційної інфраструктури для мережі магазинів взуття «Лідер взуття»

Виконавець, студент
гр. ТКР-21 _____ Сергій МАНИЧ
(підпис, дата, Ім'я ПРІЗВИЩЕ)
Керівник _____ Гліб СТУПАК
(підпис, дата, Ім'я ПРІЗВИЩЕ)
Консультанти: _____ Анна ВОРОПАЄВА
(підпис, дата, Ім'я ПРІЗВИЩЕ)
_____ Дар'я ЖУКОВСЬКА
(підпис, дата, Ім'я ПРІЗВИЩЕ)
_____ Олександр СЕРГІЄНКО
(підпис, дата, Ім'я ПРІЗВИЩЕ)

Нормоконтроль _____ Дар'я ЖУКОВСЬКА
(підпис, дата, Ім'я ПРІЗВИЩЕ)

Дрогобич – 2025 р.

Державний вищий навчальний заклад

"Донецький національний технічний університет"

Навчально-науковий інститут комп'ютерно-інформаційних технологій та автоматизації

Кафедра Автоматика та телекомунікації

Освітньо-кваліфікаційний рівень бакалавр

Галузі знань 17 Електроніка та телекомунікації
(шифр і назва)

Спеціальність 172 Телекомунікації та радіотехніка
(шифр і назва)

ЗАТВЕРДЖУЮ
Завідувач кафедри АТ
Валерій ПОЦЕПАЄВ
«____» _____2025 року

З А В Д А Н Н Я

НА ВИПУСКНУ КВАЛІФІКАЦІЙНУ РОБОТУ БАКАЛАВРА

Маничу Сергію Вадимовичу
(прізвище, ім'я, по батькові)

1. Тема проекту (роботи) «Модернізація телекомунікаційної інфраструктури для мережі магазинів взуття «Лідер взуття»
керівник проекту (роботи) Ступак Гліб Володимирович
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом вищого навчального закладу від 11.04.2025 року № 115.

2. Строк подання студентом проекту (роботи)_____

3. Вихідні дані до проекту (роботи)_____
Технічна документація та матеріали з переддипломної практики, характеристика об'єкту та вимоги до проєктування мереж

4.Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити): характеристика об'єкту, структура мережі та інформаційних потоків, розрахунок величини додаткового навантаження, загальний алгоритм проведення модернізації, вибір технології модернізації транспортної мережі, імітаційне моделювання

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)
мапа, структурна схема мережі, графіки затримки, графіки втрат, імітаційні моделі

6. Консультанти розділів проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
1	Ступак Г.В., ст. викл. каф. АТ		
2	Воропаєва А.О., доц. каф. АТ		
3	Жуковська Д.О., старший викладач		
Додаток А	Сергієнко О. І. к.т.н., доц. каф. УГВіОП		
Нормо-контроль	Жуковська Д.О., старший викладач	-	18.06.2025 р.

7. Дата видачі завдання_____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1	Характеристика об’єкту	01.05.2025	
2	Модернізація мережі	15.05.2025	
3	Моделювання роботи мережі	05.06.2025	
4	Охорона праці та безпека під час надзвичайних ситуаціях на підприємстві	08.06.2025	

Студент _____ **Сергій МАНИЧ**
(підпис) (прізвище та ініціали)

Керівник роботи _____ **Гліб СТУПАК**
(підпис) (прізвище та ініціали)

ЛИСТ ЗАУВАЖЕНЬ

Посада, Ім’я та ПРІЗВИЩЕ	Суть зауваження, оцінка та підпис

АНОТАЦІЯ

Манич С.В.. «Модернізація телекомунікаційної інфраструктури для мережі магазинів взуття «Лідер взуття» / Випускна кваліфікаційна робота на здобуття освітнього ступеня «бакалавр» зі спеціальності 172 Телекомунікації та радіотехніка. – ДВНЗ «ДонНТУ», Дрогобич, 2025.

Пояснювальна записка: 89 стор., 14 рис., 18 табл., 20 посиланнь.

Кваліфікаційна робота бакалавра присвячена модернізації телекомунікаційної інфраструктури транспортного сегменту телекомунікаційної мережі з метою покращення якості обслуговування і підвищення надійності.

У роботі проведено аналіз поточної ієрархічної мережевої архітектури, виявлено недоліки та «вузькі місця», зокрема залежність від центрального вузла та недостатню якість передачі даних для сервісів реального часу.

Запропоновано використання технології Dynamic Multipoint VPN (DMVPN) Фази 3 у поєднанні з механізмом DiffServ Code Point (DSCP), що забезпечить логічну повнозв'язну топологію з динамічними тунелями. Це значно скорочує затримку та підвищує відмовостійкість.

Проведено імітаційне моделювання існуючої та модернізованої мережі в Cisco Packet Tracer. Результати моделювання підтвердили покращення характеристик мережі і зниження рівня втрат.

Ключові слова: ТЕЛЕКОМУНІКАЦІЙНА МЕРЕЖА, МОДЕРНІЗАЦІЯ, VPN, DMVPN, QOS, DSCP, IP-ТЕЛЕФОНІЯ, НАДІЙНІСТЬ, ДОСТАВКА, ЗАТРИМКА, CISCO PACKET TRACER.

ЗМІСТ

ВСТУП

Актуальність роботи. У сучасному світі, де динамічний розвиток бізнесу нерозривно пов'язаний з ефективністю інформаційних технологій, телекомунікаційна інфраструктура відіграє ключову роль у забезпеченні безперебійної та продуктивної діяльності підприємств. Зростання обсягів інформації, впровадження хмарних технологій, систем відеоспостереження, а також поширення IP-телефонії як основного засобу комунікації, вимагають від мережевої інфраструктури не тільки високої пропускної здатності, а й здатності гарантування якості обслуговування для застосунків. Існуючі традиційні архітектури, часто побудовані за принципом «зірки» з централізованим транзитом всього трафіку, виявляються недостатньо гнучкими, масштабованими та відмовостійкими для задоволення цих потреб. Вони створюють «вузькі місця», збільшують затримку та знижують надійність зв'язку між філіями, що може призвести до збоїв у бізнес-процесах та фінансових втрат. Компанія «Лідер Взуття», що має розгалужену мережу магазинів, стикається з аналогічними викликами.

Мета роботи підвищення надійності, масштабованості та забезпечення якості обслуговування критично важливих бізнес-додатків, за рахунок модернізації транспортного сегменту телекомунікаційної мережі компанії «Лідер Взуття»

Завдання:

1. Провести аналіз телекомунікаційної інфраструктури транспортного сегменту мережі магазинів «Лідер Взуття»;
2. Виконати експериментальне дослідження завантаженості каналів зв'язку;
3. Розрахувати додаткове навантаження від впровадження IP-телефонії;
4. Провести аналіз та порівняння існуючих технологічних рішень для побудови захищених та ефективних корпоративних мереж, обґрунтувати вибір;
5. Запропонувати варіант модернізації або реконфігурації мережі;

6. Провести імітаційне моделювання роботи існуючої структури і запропонованого рішення, проаналізувати отримані результати.

Об’єктом в роботі є телекомунікаційна інфраструктура транспортного сегменту корпоративної мережі магазинів взуття «Лідер Взуття».

Предметом в роботі є методи та технології модернізації транспортного сегменту телекомунікаційної мережі з використанням VPN-рішень та механізмів якості обслуговування (QoS)

Методи дослідження:

- Системний аналіз – використаний для вивчення поточної архітектури мережі, її компонентів, взаємозв'язків та функціональних можливостей.
- Експериментальний метод – застосований для збору реальних даних про завантаженість каналів зв'язку та склад трафіку існуючої мережі за допомогою інструментів моніторингу (Port Mirroring, MRTG, Wireshark).
- Метод розрахунків – використаний для кількісної оцінки додаткового навантаження, що виникне при впровадженні нових сервісів, зокрема IP-телефонії.
- Порівняльний аналіз – застосований для оцінки різних VPN-топологій та механізмів QoS з метою вибору оптимальних технологічних рішень.
- Імітаційне моделювання – проведено за допомогою програмного пакету Cisco Packet Tracer для візуалізації, відтворення та порівняльного дослідження поведінки існуючої та модернізованої мереж, а також для кількісної оцінки таких показників, як надійність доставки та затримка.
- Аналіз отриманих даних – використаний для інтерпретації результатів моделювання та формулювання висновків щодо ефективності запропонованих рішень.

Структура та загальний обсяг випускної кваліфікаційної роботи.

Робота складається зі вступу, 3 основних розділів, висновків, переліку посилань на 20 джерел та 2 додатків. Загальний обсяг роботи становить 88 сторінок, 14 рисунків та 18 таблиць.

1 ХАРАКТЕРИСТИКА ОБ’ЄКТУ

1.1 Характеристика об’єкту модернізації

В якості об’єкту у випускній кваліфікаційній роботі бакалавра виступає мережа магазинів «Лідер взуття», що спеціалізується на продажі взуття для всіх вікових категорій [1]. В рамках роботи необхідно виконати модернізацію телекомунікаційної мережі.

На сьогоднішній день мережа складається з центрального офісу, що вже знаходиться в Києві, 6 великих магазинів з складськими і логістичними потужностями, та кількох дрібних філій. Причина проведення модернізації – збільшення обороту, перенос головного офісу з Дніпра до Києва і як наслідок зростання обсягів трафіку. Інфраструктура мережі магазинів стисло можна охарактеризувати так:

- мережа є корпоративною структурою з чітко визначеною організаційною схемою;
- існуюча інфраструктура перебуває на етапі, що вимагає модернізації для досягнення сучасних стандартів;
- мережа має потенціал для реструктуризації та оптимізації розподілу трафіку.

Аналіз та основні проєктні рішення будуть зосереджені на ключових компонентах телекомунікаційної структури мережі «Лідер взуття». Дрібні роздрібні точки продажу, а також віддалені склади не будуть включені до детального розгляду. Робота спрямована на покращення інфраструктури транспортного сегменту мережі, який забезпечує зв’язок між центральним офісом і ключовими магазинами, що мають найбільше навантаження, також весь трафік між філіями проходить через центральний офіс.

В табл. 1.1 наведена класифікація філій.

Таблиця 1.1 – Класифікація філій

№		Тип
1	Київ №1	Головний офіс
2	Київ №2	Регіональне представництво
3	Бровари	Регіональне представництво
4	Житомир	Регіональне представництво
5	Дніпро	Регіональне представництво
6	Харків	Регіональне представництво
7	Херсон	Регіональне представництво

Серед мережних сервісів, що функціонують завдяки наявної телекомунікаційної інфраструктури переважно є програмні рішення для забезпечення відеоспостереження, корпоративного зв'язку та ведення бухгалтерського і складського обліку.

Щодо топологічної схеми об'єкту, то на сьогоднішній день це зірка (рис.1.1).

Рисунок 1.1 – Топологічна схема

Телекомунікаційна інфраструктура транспортного сегменту мережі магазинів взуття «Лідер взуття» побудована на базі топології зірка, де

центральним вузлом виступає головний офіс у Києві. Для з'єднання територіально розподілених магазинів із центральним офісом використовуються віртуальні приватні мережі (VPN), які працюють через публічну мережу Інтернет. Такий спосіб організації транспортних сегментів забезпечує високу гнучкість і економічну доцільність, що робить його популярним рішенням як для великих корпорацій, так і для середніх та малих підприємств. В табл. 1.2 наведена характеристика пропускної здатності каналів транспортного сегменту мережі.

Таблиця 1.2 – Характеристика каналів зв'язку транспортного сегменту мережі

Канал	Тип каналу	Пропускна здатність каналу, Мбіт/с
Київ 1 - Київ 2	VPN	35
Київ 1 - Бровари	VPN	35
Київ 1 - Житомир	VPN	40
Київ 1 - Дніпро	VPN	45
Київ 1 - Харків	VPN	50
Київ 1 - Херсон	VPN	35

Загальна пропускна здатність основного каналу Інтернет-зв'язку в головному офісі становить 300 Мбіт/с. Для забезпечення стабільності та безперервності роботи мережі окрім основних каналів передбачено резервні. Їх пропускна здатність для кожного магазину становить 2 Мбіт/с, а для центрального офісу — 12 Мбіт/с.

1.2 Структура існуючі мережі та характеристика інформаційних потоків

Поточна архітектура телекомунікаційної мережі «Лідер Взуття» детально представлена на рис.1.2.

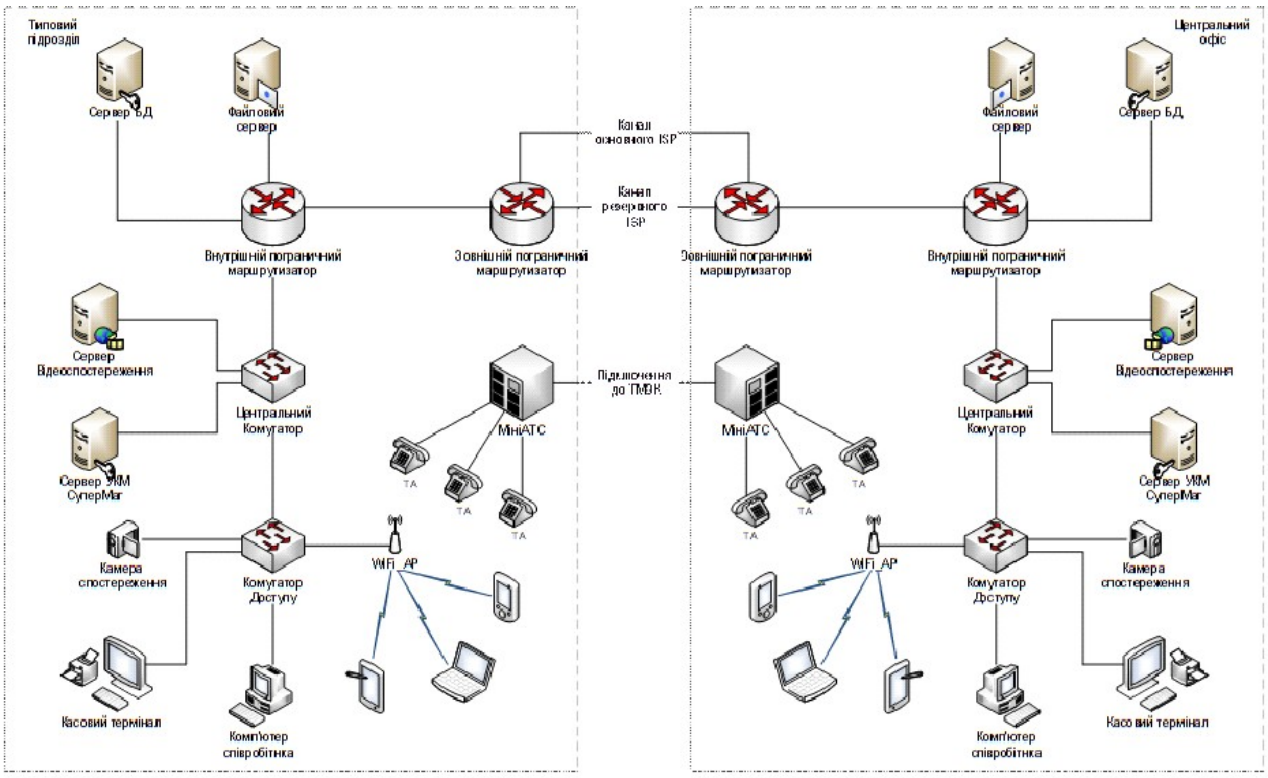

Рисунок 1.2 – Структура мережі «Лідер взуття»

Як виходить з наведеного рис. 1.2, структура є доволі уніфікованою, і поширюється як на центральний офіс, так і на всі філії та магазини. У складі мережі застосовується низка ключових компонентів, що включає маршрутизатори, комутатори, точки бездротового доступу (Wi-Fi), серверне забезпечення, а також спеціалізоване обладнання, яке використовується для роботи касових терміналів. Побудова мережі базується на ієрархічній топології типу «зірка», що охоплює рівні доступу, розподілу та ядра.

Відповідно до ієрархічної моделі архітектури, у структурі мережі реалізовано такі технології:

- рівень ядра – Gigabit Ethernet;
- рівень розподілу: Gigabit Ethernet;
- рівень доступу: Fast Ethernet та Wi-Fi.

Ядро мережі реалізовано з використанням двох окремих маршрутизаторів: внутрішнього та зовнішнього. Внутрішній маршрутизатор відповідає за управління локальним сегментом мережі. Серед його основних

функцій слід виокремити: автоматичний розподіл IP-адрес клієнтським пристроям за допомогою протоколу DHCP, впровадження правил доступу до локальних ресурсів, створення віртуальних підмереж (VLAN) для сегментації мережевого трафіку, обмеження доступу до сервісних серверів (включаючи бази даних і FTP-сервери) для користувачів як із внутрішнього, так і із зовнішнього сегмента мережі, а також організацію доступу до Інтернету та корпоративної мережі з урахуванням контексту користувача. Зовнішній маршрутизатор виконує завдання міжмережевого екрану (firewall), забезпечує маршрутизацію трафіку між основним і резервним каналами Інтернет-провайдерів (ISP), організовує віртуальні приватні мережі (VPN) для зв’язку між офісами, надає підключення до Інтернету та захищає локальну інфраструктуру від потенційних загроз. Важливо зазначити, що у загальній конфігурації мережі маршрутизатор центрального офісу функціонує як VPN-сервер, тоді як маршрутизатори філій виконують роль VPN-клієнтів, встановлюючи безпечні канали зв'язку між окремими вузлами системи.

Рівень розподілу у мережі базується на центральному комутаторі, до якого підключено комутатори доступу та критично важливі сервери, зокрема сервер УКМ «СуперМаг», що відповідає за управління касовими операціями, та сервер відеоспостереження. Зв’язок між цими пристроями та внутрішнім прикордонним маршрутизатором реалізовано за допомогою технології Gigabit Ethernet. Центральний комутатор виконує функцію агрегації мережевого трафіку, передаючи його зведеним потоком на пристрої ядра.

Рівень доступу відповідає за підключення кінцевих термінальних пристроїв до мережі. Сюди входять персональні комп’ютери, платіжні та касові термінали, камери спостереження, а також бездротові термінальні пристрої, такі як сканери та мобільні гаджети. Точки бездротового доступу (Wi-Fi) підключаються до комутаторів доступу через Fast Ethernet, тоді як з’єднання між комутаторами доступу та пристроями рівня розподілу реалізується за технологією Gigabit Ethernet.

Телефонна мережа кожного магазину чи філії функціонує як автономна

система з топологією «зірка». Вона базується на цифровій МініАТС, яка підтримує як аналогові, так і цифрові телефонні апарати. Підключення до телефонної мережі загального користування (ТМЗК) здійснюється через виділені лінії до місцевих АТС. З огляду на сучасні потреби бізнесу, у межах модернізації слід передбачити можливість інтеграції та передачі голосового трафіку корпоративної IP-телефонії між філіями через основну телекомунікаційну мережу.

Програмне забезпечення, що використовується для забезпечення роботи мережі «Лідер Взуття» та надання послуг, включає:

- Система Управління Бізнесом (СУБ) – спеціалізований програмний комплекс для управління підприємством, бухгалтерським обліком, складськими запасами та продажами. Платформа призначена для комплексного управління діяльністю як окремих магазинів, так і всієї мережі;
- УКМ «СуперМаг» – програмне рішення для управління касовими апаратами та платіжними терміналами, що забезпечує процес продажів. УКМ інтегрується із СУБ і функціонує в єдиному інформаційному середовищі;
- «Відео-7Е» – програмний комплекс для адміністрування системи відеоспостереження.

В якості термінальних пристроїв в мережі використовуються:

- персональні комп’ютери для забезпечення доступу до СУБ, УКМ «СуперМаг», Інтернет та електронної пошти;
- POS-термінали для роботи з програмним забезпеченням УКМ «СуперМаг»;
- камери спостереження;
- бездротові клієнтські пристрої – використання гостьового доступу до Інтернету;
- дистанційні сканери QR-кодів та штрихкодів для організації обліку товарів з доступом до СУБ.

Окрім цього, між філіями постійно взаємодіють СУБ і УКМ «СуперМаг». Основний міжфілійний трафік зараз складається із синхронізації даних серверів СУБ та обміну електронною поштою. В рамках модернізації очікується розширення трафіку за рахунок додавання даних корпоративної IP-телефонії.

На основі проведеного аналізу інформаційної інфраструктури створено інформаційну модель взаємодії мережевих ресурсів (рис. 1.3).

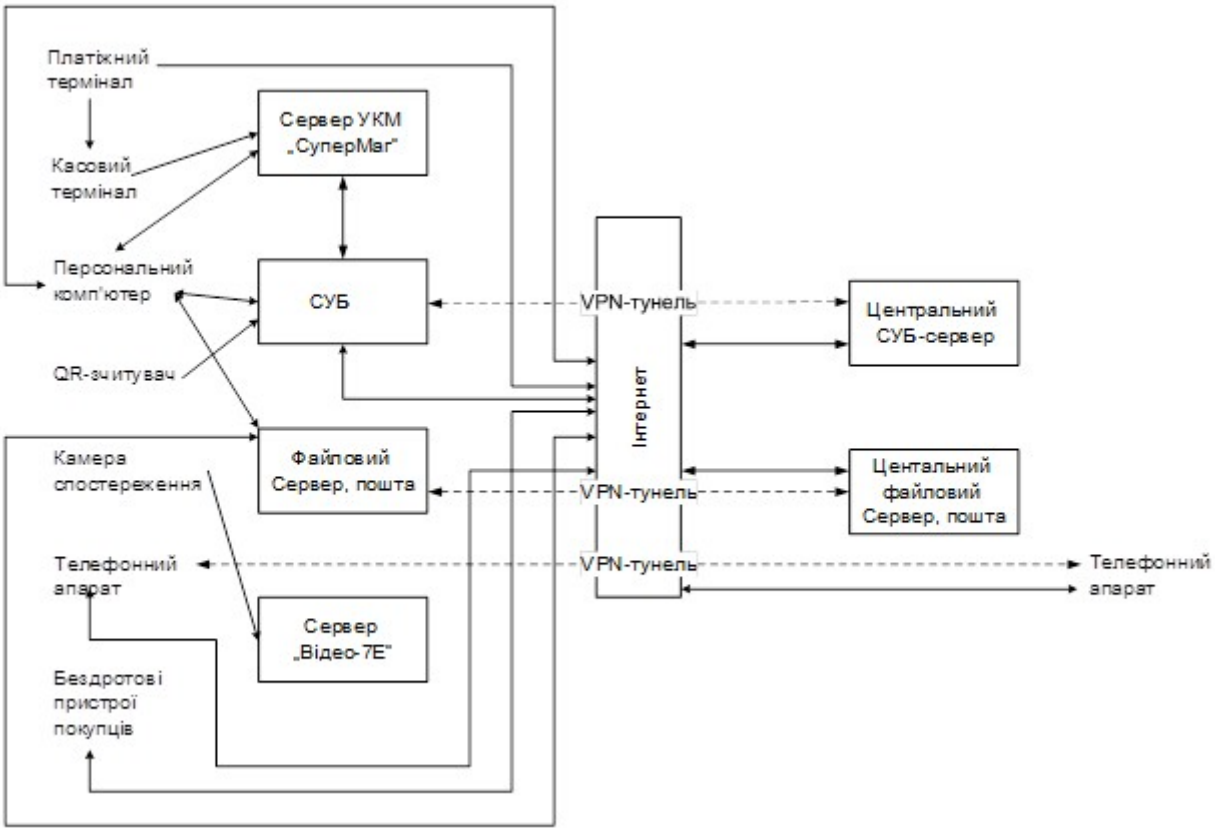

Рисунок 1.3 – Інформаційна модель мережі

Логічні канали зв’язку позначені пунктирними лініями, тоді як суцільними лініями відображені фізичні з'єднання. Таке графічне подання сприяє візуалізації маршрутизації трафіку основних бізнес-додатків, зокрема Системи Управління Бізнесом (СУБ), файлового сервера, корпоративної пошти, а також перспективної IP-телефонії через логічні VPN-тунелі.

З метою комплексного аналізу та оцінки ефективності функціонування наявних каналів зв’язку для кожного сегмента транспортної мережі було проведено експериментальне дослідження. Схема експериментального

дослідження приведена рис. 1.4.

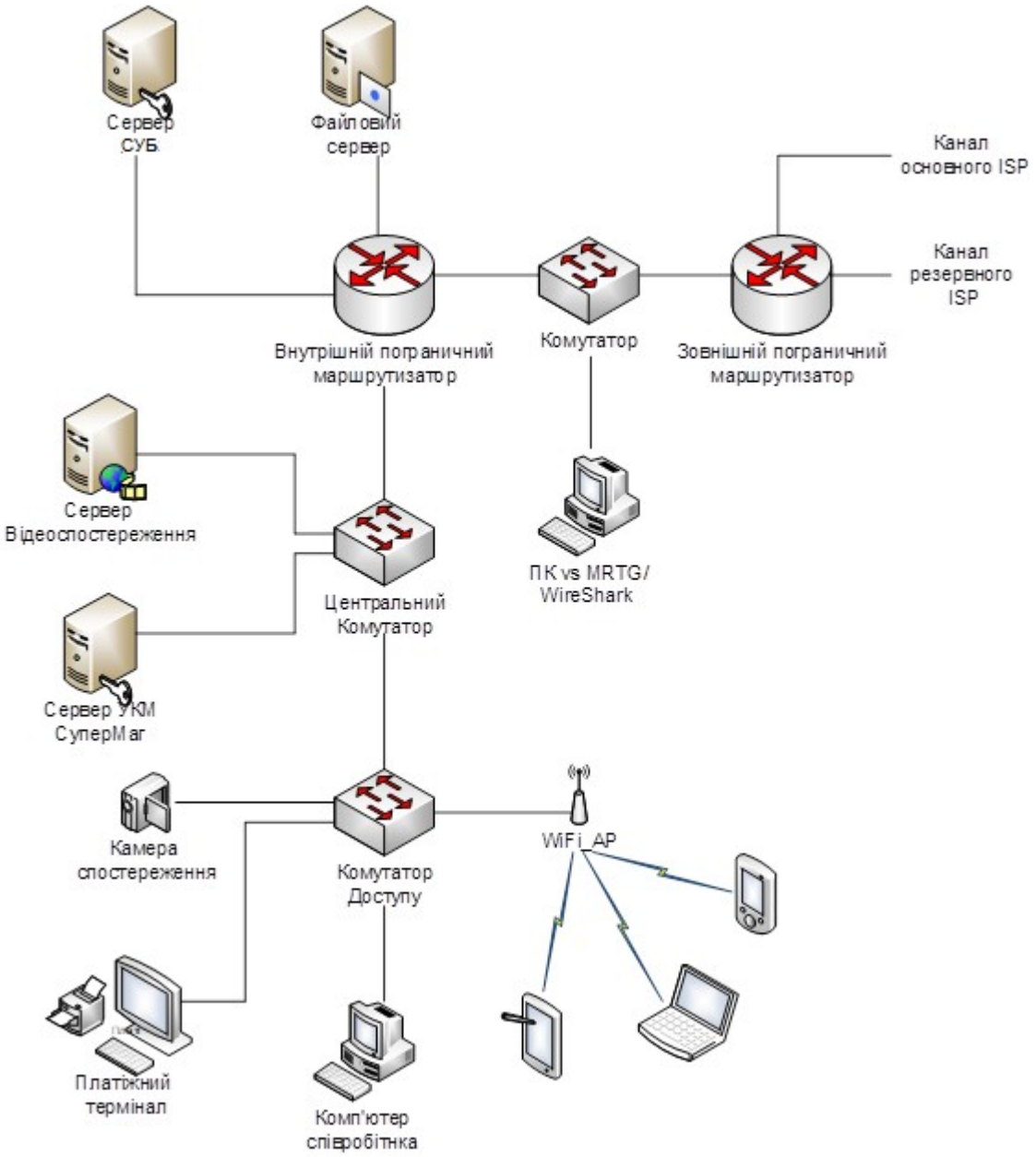

Рисунок 1.4 – Схема проведення експериментального дослідження каналів зв’язку

Для забезпечення високої ефективності аналізу параметрів функціонування транспортного сегмента мережі «Лідер Взуття» були використані спеціалізовані програмні утиліти:

– MRTG (Multi Router Traffic Grapher) – інструмент для моніторингу завантаженості каналів зв’язку в режимі реального часу. Ця

програма дозволяє збирати статистичні дані, генерувати графічну візуалізацію завантаження та створювати звіти на основі отриманих показників трафіку. Завдяки цьому стало можливим оцінити динаміку використання пропускної здатності мережі;

– Wireshark – потужний аналізатор мережевих протоколів, застосовувався для детального аналізу складу мережевого трафіку. Ця утиліта надала можливість ідентифікувати трафік за протоколами моделі OSI, портам та адресам призначення, що є критично важливими для розуміння типів інформації, що циркулює в мережі, а також їхнього потенційного впливу на загальну продуктивність системи.

Склад апаратних засобів для проведення вимірювань:

1. Персональний комп’ютер налаштований на базі операційної системи FreeBSD, обладнаний мережевою картою Gigabit Ethernet, що забезпечує необхідну пропускну здатність для роботи з мережевим трафіком.
2. Керований комутатор Mikrotik RB-250GS, який має можливість використання функції Port Mirroring (дзеркалювання портів), що дозволило перехоплювати та аналізувати трафік у реальному часі без порушення його передачі.
3. Набір комунікаційних кабелів для фізичного підключення обладнання у тестовій конфігурації.

Це обладнання та підхід забезпечили інструментальну базу для реалізації дослідження продуктивності каналів зв’язку.

Під час дослідження дотримувалися ключової умови – використання виключно основного каналу інтернет-провайдера (ISP). Такий підхід забезпечив чистоту отриманих результатів, виключаючи вплив резервних каналів на аналіз продуктивності.

Методологія збору даних була побудована відповідно до схеми, представленої на рис. 1.4. Усі мережеві дані, що передавалися між

маршрутизаторами (тобто весь міжфілійний трафік), дублювалися за допомогою функції Port Mirroring комутатора Mikrotik на спеціально виділений порт. До цього порту підключався персональний комп'ютер з встановленими програмними засобами MRTG та Wireshark, що забезпечило пасивний і ненастирливий збір даних для подальшого аналізу.

Експериментальне дослідження завантаженості каналів зв'язку між центральним офісом у Києві та регіональними представництвами (магазинами) «Лідер Взуття» дало змогу отримати низку важливих результатів. У табл. 1.3 наведено відсотковий розподіл інформаційних потоків та визначено пропускну здатність для кожної категорії мережевих сервісів. Крім того, таблиця містить фактичні показники завантаження каналів зв'язку в Мбіт/с.

Таблиця 1.3 – Характеристика розподілу інформаційних потоків

	Інтернет, Мбіт/с	СУБ, Мбіт/с	FTP, Мбіт/с	Mail, Мбіт/с	Загальне завантаження, Мбіт/с	Відсоток утилізації каналу
Київ 1 - Інтернет	59	37,6	21	2,23	119,83	40
Київ 1 - Київ 2	11,2	5,6	2,7	0,32	19,82	57
Київ 1 - Бровари	13,7	5,7	2,1	0,33	21,83	63
Київ 1 - Житомир	15,7	6,2	4,1	0,36	26,36	66
Київ 1 - Дніпро	16	7,1	5,2	0,43	28,73	64
Київ 1 - Харків	19	7,8	4,6	0,47	31,87	64
Київ 1 - Херсон	13,5	5,2	2,2	0,32	21,22	61

Для наочного зображення динаміки мережевого навантаження були представлені характеристики добового і тижневого розподілу навантаження каналів зв'язку. Ця інформація детально наведена на рис. Б.1–Б.8 у Додатку Б. Там же містяться додаткові статистичні дані та графічні інтерпретації.

Узагальнені результати експериментального дослідження рівня завантаженості каналів візуалізовано на рис. 1.5, що відображає основні тенденції та особливості використання пропускної здатності транспортного сегмента мережі.

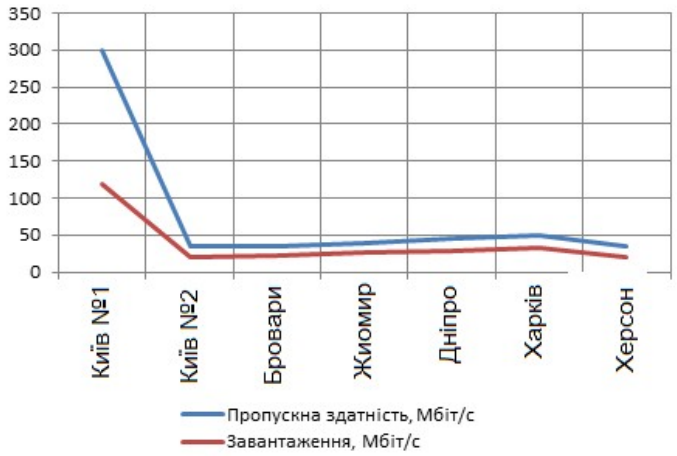

Рисунок 1.3 – Результати дослідження каналів зв’язку

1.3 Розрахунок величини додаткового навантаження від впровадження нових послуг

Дослідження завантаженості каналів зв’язку транспортного сегмента мережі «Лідер Взуття» проводилося протягом календарного тижня. На основі даних цього моніторингу було визначено день із найвищим піковим навантаженням – середа. Це співвідноситься з бізнес-процесами компанії, зокрема впровадженням оновлень цінової політики та акційних пропозицій, які, зазвичай, запускаються з четверга. Для цього необхідна інтенсивна синхронізація даних і оновлення інформації в мережі магазинів.

Загальний аналіз показав, що середній рівень використання смуги каналу зв'язку до Інтернет-провайдерів (ISP) становить близько 60%. Це свідчить про наявність певного запасу пропускної здатності. Проте при плануванні модернізації слід враховувати можливе зростання потреб та інтеграцію нових сервісів у майбутньому.

Також було виявлено, що пікове навантаження спостерігається в унісон для всіх підрозділів (магазинів) мережі в період між 10:00 і 20:00 годинами. Така закономірність зумовлена характером роботи мережі магазинів та функціональними обов'язками персоналу, які включають активні продажі,

взаємодію з СУБ, обробку платежів та виконання інших операцій у цей період інтенсивності.

На даний момент вплив корпоративної IP-телефонії не було враховано в дослідженні, оскільки її впровадження лише планується в межах модернізації. Для об'єктивної оцінки її впливу на існуючу інфраструктуру, а також необхідної пропускної здатності, потрібно провести окремі розрахунки додаткового навантаження, що буде створюватись новою послугою.

Основною інформацією для розрахунку параметрів IP-телефонії слугують такі показники:

- кількість кінцевих користувачів IP-телефонії;
- частота використання телефонного зв’язку (кількість та тривалість дзвінків);
- тип голосового кодеку, що визначатиме обсяг трафіку одного розмовного каналу;
- протоколи передачі даних, які будуть застосовуватись (наприклад, SIP, RTP).

Для проведення точного розрахунку додаткового навантаження на транспортний сегмент мережі, яке генеруватиме послуга корпоративної IP-телефонії, були визначені наступні ключові параметри:

- кількість користувачів – n=5 осіб;
- загальне значення навантаження в (ГНН) для групи послуг телефонії становить y=0,1 Ерл (очікувана інтенсивність використання голосового зв'язку);
- тип голосового кодеку – G.711, що забезпечує якість мовлення, порівнянну з телефонною мережею загального користування, і генерує відносно вищий обсяг трафіку порівняно з більш стиснутими кодеками;
- тривалість семпла) для кодека G.711 встановлена на рівні 10 мс, що впливає на розмір пакетів та частоту їх відправлення;
- для організації передачі даних на канальному рівні буде

використано Etherne;.

- на мережевому рівні застосовуватиметься протокол IP;
- транспортний протокол UDP (User Datagram Protocol), що є типовим для IP-телефонії завдяки його швидкості та низькій затримці, незважаючи на відсутність гарантій доставки;
- протоколом для передачі мультимедійних даних у реальному часі – RTP (Real-time Transport Protocol).

Ці вихідні дані дозволять провести необхідні інженерні розрахунки для визначення оптимальної пропускної здатності каналів та конфігурації мережевого обладнання для успішного впровадження послуги корпоративної IP-телефонії у мережі «Лідер Взуття».

Розрахунок буде проведено для випадку примітивного потоку, враховуючи відносно невелику загальну кількість абонентів, яка становить

Загальна величина абонентського навантаження (Y) розраховується за формулою:

$$Y = n*y \tag{1.1}$$

Де:

n – кількість користувачів групи корпоративної телефонії ;

y – питоме значення навантаження в ГНН для групи послуг телефонії.

Підставивши вихідні дані, отримаємо:

$Y = 5*0,1 = 0,5$ Ерл

Таким чином, загальне абонентське навантаження становить 0,5 Ерл.

Далі необхідно розрахувати параметри семпла. Семпл це елементарна одиниця оцифрованої фонограми, яка записується, перетворюється, кодується та передається як одиниця корисної інформації. Тривалість семпла є параметром налаштування обладнання; її можна встановлювати за власним

розсудом, проте слід враховувати, що більший семпл дає менший показник швидкості, але може призводити до збільшення затримки.

Обсяг даних у одному семплі (V_{sample}) є ключовим показником, що залежить від типу голосового кодека, який використовується IP-телефонним апаратом, та тривалості семпла. Він визначається за формулою:

$$V_{sample} = R*t_s/8 \quad (1.2)$$

Де:

R – бітова швидкість кодека (bit rate). Згідно з обраним типом кодека G.711, його бітова швидкість становить 64 Кбіт/с;

t_s – тривалість семпла;

Знаменник 8 використовується для переведення біт у байти.

Отже, обсяг корисної інформації в одному семплі становитиме:

V_{sample} = 0,01*64000/8=80 байт

Обсяг корисної інформації в одному семплі становить 80 байт.

Необхідна пропускна здатність у каналі зв'язку для однієї розмови (B_{call}) залежить не лише від обсягу корисної інформації, але й від кількості службової інформації (заголовків протоколів), яка додається до даних фонограми. Вона розраховується за формулою:

$$B_{call} = (V_{sample} + H_2 + H_3 + H_4 + H_5) * 8 / t_S \quad (1.3)$$

Для визначення обсягу службової інформації враховуються розміри заголовків, які додаються до кожного пакета з корисною інформацією семпла:

- H_2 – розмір заголовка канальної технології Ethernet, який дорівнює 18 байтам.

- H_3 – розмір заголовка мережевої технології IP, який дорівнює 20 байтам.
- H_4 – розмір заголовка транспортної технології UDP, який дорівнює 8 байтам.
- H_5 – розмір заголовка потокової технології RTP, який дорівнює 12 байтам.

Таким чином, пропускна здатність у каналі зв'язку для однієї розмови становитиме:

B_{call} = (80 + 18 + 20 + 8 + 12) * 8 /0,01 = 110,4 Кбіт/с

Пропускна здатність для однієї розмови становить 110,4 Кбіт/с.

Для розрахунку кількості еквівалентних каналів ($N_{channels}$), необхідних для пропускання голосового трафіку, використовується перша формула Ерланга. Числові значення цієї формули часто представлені у вигляді таблиць, таких як таблиця Кендалла-Башаріна.

Вхідними даними для таблиці Ерланга є загальне навантаження (Y) та прийнятна норма втрат телефонного сполучення (P). Норма втрат приймається P = 0,001, виходячи з того, що ділянка мережі виконує функції «групового шукання».

Проведемо розрахунок кількості еквівалентних каналів, що задіяні при проведенні розмов у мережі, з урахуванням загального навантаження (враховуючи локальний зв'язок і зв'язок з ТМЗК). Виходячи з вихідних даних Y=0,5 Ерл (розраховано раніше) та P = 0,001, за таблицею Ерланга (або відповідним розрахунком) загальна кількість каналів становить 4 лінії.

Остаточна необхідна пропускна здатність у каналі зв'язку (B_{total}) визначається як сумарна пропускна здатність для потрібної кількості еквівалентних «шнурових комплектів» (каналів) за формулою:

$$B_{total} = N_{channels} * B_{call} \quad (1.4)$$

Таким чином, сумарна пропускна здатність, необхідна для забезпечення корпоративної IP-телефонії, становитиме:

$B_{total} = 4 * 110,4 = 441,6$ Кбіт/с

Таким чином додаткове навантаження на IP-мережу від впровадження послуги корпоративної IP-телефонії становитиме приблизно 0,44 Мбіт/с. Це значення є важливим для планування модернізації, оскільки його необхідно врахувати при визначенні загальної необхідної пропускної здатності каналів зв'язку для центрального офісу та філій.

1.4 Передумови модернізації

Існуюча корпоративна транспортна мережа компанії «Лідер Взуття» потребує реструктуризації та значних покращень. Ця необхідність зумовлена кількома ключовими факторами: неоптимальним використанням існуючих пропускних здатностей каналів зв'язку, критичною потребою у впровадженні послуг реального часу (зокрема, корпоративного голосового зв'язку IP-телефонії), а також необхідністю підвищення загального рівня безпеки обміну даними.

Наявна мережа, попри свою функціональність, має низку суттєвих недоліків, які перешкоджають ефективній та стабільній роботі, особливо з огляду на майбутні вимоги.

До основних проблем можна сміливо віднести такі:

відсутність гарантії доставки даних, що може призвести до втрати важливої інформації або необхідності повторної передачі, знижуючи ефективність бізнес-процесів;

- нестабільний показник затримки в мережі (latency) – висока та непередбачувана затримка негативно впливає на роботу критично важливих бізнес-додатків, таких як СУБ та УКМ «СуперМаг», а також унеможливлює якісну передачу голосового трафіку;
- джиттер (jitter) – коливання затримки доставки пакетів є особливо критичним для послуг реального часу (наприклад, IP-телефонії), викликаючи перебої та погіршення якості зв'язку;
- неоптимальне використання смуги пропускання каналів зв’язку, що призводить до простоїв під час низького навантаження та можливих перевантажень у пікові періоди.

Для успішної реструктуризації мережі та усунення цих недоліків, ключовим завданням є досягнення оптимального балансу між показниками продуктивності, надійності та економічності. Досягти поставленої мети можна за рахунок комплексного підходу, що включає:

- перерозподіл інформаційних потоків за рахунок оптимізації процесу маршрутизації та пріоритезації трафіку;
- зміна топології корпоративної мережі для підвищення відмовостійкості та ефективності;
- пріоритезація трафіку за допомогою політики Class of Service (CoS) / Quality of Service (QoS) для забезпечення пріоритетного переважного обслуговування критичних для бізнесу сервісів;
- оптимізація параметрів мережі з точки зору QoS, а саме впровадження механізмів, що гарантують якість обслуговування для різних типів трафіку, зокрема зменшення затримки та джиттера.

Ці заходи дозволять побудувати більш адаптивну, надійну та високопродуктивну телекомунікаційну інфраструктуру.

Висновки до розділу 1

У першому розділі випускної кваліфікаційної роботи було проведено аналіз поточної телекомунікаційної інфраструктури транспортного сегменту мережі магазинів взуття «Лідер Взуття», до складу якої входить сім магазинів.

Було встановлено, що мережа побудована за ієрархічною топологією «зірка», де центральним вузлом є головний офіс у Києві, а для міжфілійного зв'язку активно використовуються VPN-тунелі через публічну мережу Інтернет. Розглянуто архітектуру на рівнях ядра, розподілу та доступу, а також описано функціонал ключових мережевих пристроїв.

Для об'єктивної оцінки поточного стану та виявлення потенційних вузьких місць, було проведено експериментальне дослідження завантаженості каналів зв'язку транспортного сегменту. Застосовані інструментальні засоби на базі комутатора L3 Mikrotik з функцією Port Mirroring та утилітами MRTG і Wireshark, дозволили отримати дані про утилізацію каналів і якісний склад трафіку. Визначено що пікові навантаження припадають на середу в межах 10:00-20:00, що пов'язано з бізнес-процесами оновлення даних та продажів.

Виконано розрахунок додаткового навантаження, яке виникне при впровадженні корпоративної IP-телефонії. На основі заданих параметрів (кількість користувачів, інтенсивність, кодек G.711) було визначено, що додатково потрібно приблизно 0,44 Мбіт/с.

Розглянуті та обґрунтовані передумови проведення модернізації. Аналіз виявив, що, незважаючи на загальну функціональність існуючої інфраструктури, її модернізація є актуальною та необхідною. Це дозволить не лише врахувати додаткове навантаження від майбутніх сервісів, таких як IP-телефонія, а й потенційно підвищити загальну надійність, ефективність та масштабованість мережі «Лідер Взуття» відповідно до зростаючих потреб сучасного бізнесу.

2 МОДЕРНІЗАЦІЯ МЕРЕЖІ

2.1 Загальний алгоритм проведення модернізації

Для успішної модернізації та реструктуризації телекомунікаційної інфраструктури транспортного сегменту мережі магазинів «Лідер Взуття» необхідно здійснити комплекс ключових заходів, що включають:

1. Розробку нової топології, що передбачає перегляд поточної архітектури мережі з акцентом на підвищення її надійності, масштабованості та загальної ефективності. Роботи охоплюватимуть оптимізацію як фізичної, так і логічної структури зв'язків між центральним офісом і філіями.
2. Впровадження сучасних технологій для транспортного сегмента мережі. Це дозволить поліпшити якість передачі даних, забезпечити гарантовану пропускну здатність для критично важливих сервісів та підвищити загальну стабільність каналів зв'язку. Особливу увагу слід приділити підтримці послуг реального часу, таких як IP-телефонія.
3. Розробку та реалізацію політики Class of Service (CoS) і Quality of Service (QoS). Цей крок передбачає впровадження механізмів управління трафіком, що дозволять пріоритезувати критично важливі дані й сервіси (наприклад, голосовий та бази даних) над менш чутливим трафіком, гарантуючи необхідну якість обслуговування.

Детальний аналіз існуючої мережі та запропонованого комплексу заходів виявляє дві задачі, які потребують вирішення:

– оптимізація мережевої топології з вибором відповідних технологій побудови. Це включає вивчення обмежень нинішньої системи та визначення технічних рішень для їх усунення;

– розробка політики CoS/QoS. Завдяки цьому буде забезпечено належну якість роботи всіх сервісів, особливо тих, що є критично важливими для бізнесу чи залежать від реального часу.

Цей структурований підхід дозволить поетапно впроваджувати необхідні зміни та досягти поставлених цілей у рамках модернізації телекомунікаційної інфраструктури мережі «Лідер Взуття».

2.2 Вибір відповідних технологій побудови та рішень

Для забезпечення ефективної модернізації інфраструктуру магазинів «Лідер Взуття» доцільно поділити на локальні мережі (LAN) всередині кожного магазину/офісу та транспортну мережа (WAN), яка об'єднує всі локальні мережі в єдину корпоративну структуру. Усі локальні мережі повинні бути надійно з'єднані між собою за допомогою оптимізованої транспортної мережі.

Ключовим етапом вибору технологій для побудови оновленої транспортної мережі є формулювання чітких вимог до пропускної здатності каналів зв'язку (табл. 2.1). Ці вимоги ґрунтуються на аналізі поточного трафіку (розділі 1), і розрахунках додаткової пропускної здатності для IP-телефонії.

Таблиця 2.1 – Вимоги до пропускних здатностей каналів зв'язку (Мбіт/с)

	Інтернет, Мбіт/с	Передача даних, Мбіт/с	IP-телефонія, Мбіт/с	Всього, Мбіт/с
Київ 1 - Київ 2	11,2	8,62	0,44	20,26
Київ 1 - Бровари	13,7	8,13	0,44	22,27
Київ 1 - Житомир	15,7	10,66	0,44	26,8
Київ 1 - Дніпро	16	12,73	0,44	29,17
Київ 1 - Харків	19	12,87	0,44	32,31
Київ 1 - Херсон	13,5	7,72	0,44	21,66

Модернізована мережа повинна забезпечувати високоякісне надання наступного переліку основних послуг:

1. Високошвидкісний доступ до мережі Інтернет для забезпечення стабільного та швидкого зв'язку для всіх підрозділів.
2. Впровадження корпоративної IP-телефонії для оптимізації комунікацій та зниження витрат.
3. Швидкий та надійний доступу до централізованих баз даних для всіх операцій.
4. Забезпечення безперебійного обміну файлами та документами між підрозділами.

Для забезпечення оптимальних характеристик, особливо з огляду на вимоги послуг реального часу (які мають дуже жорсткі вимоги до затримки, джиттера та втрат пакетів), ідеальною була б повнозв'язна топологія. Проте її реалізація для географічно розподіленої мережі є майже нереальною і економічно невиправданою.

При виборі способу організації транспортної мережі варто розглядати два основні підходи:

1. Виділені канали. Цей спосіб передбачає використання фізично окремих, орендованих або прокладених каналів зв'язку (наприклад, оптоволоконних ліній). Незважаючи на високу надійність та продуктивність, побудова мережі на основі виділених каналів є надзвичайно дорогим рішенням, що вимагає значних капітальних вкладень у прокладання або довгострокову оренду інфраструктури. З економічної точки зору, цей варіант майже ніколи не застосовується для мереж такого масштабу.
2. Віртуальні канали. Цей підхід дозволяє створювати логічні канали зв'язку поверх існуючої публічної інфраструктури, таких як Інтернет. Віртуальні канали можуть надавати якість, порівнянну з виділеними, але при цьому не потребують оренди окремих фізичних каналів або прокладання власної транспортної мережі. Це робить їх значно більш економічно ефективним та гнучким рішенням.

Враховуючи, що у мережі «Лідер Взуття» на сьогодні вже успішно застосовується підхід з віртуальними каналами (через VPN), відмовлятися від нього не є доцільним. Навпаки, слід зосередитися на його вдосконаленні. Організувати віртуальні канали можна декількома способами:

- організація мережі на базі технологій (Frame Relay, ATM), що забезпечують високу якість сервісу, але є дорожчими у впровадженні та підтримці для сучасної IT-інфраструктури порівняно з IP-орієнтованими рішеннями;
- організація мережі на базі технології VPN поверх публічної мережі Інтернет, що більш найпоширеним і економічно вигідним на сьогодні. VPN дозволяє створювати безпечні та надійні логічні канали через загальнодоступний Інтернет, що є хорошим рішенням для географічно розподіленої мережі магазинів.

Нижче опишемо конкретні технології, за допомогою яких можливо побудувати та оптимізувати транспортну мережу.

Frame Relay (ретрансляція кадрів) – це протокол канального рівня моделі OSI, який свого часу був широко поширеною службою комутації пакетів. Він дозволяє створювати безліч незалежних постійних віртуальних каналів (PVC) в одній фізичній лінії зв'язку, що ідентифікуються за допомогою ідентифікаторів підключення до з'єднання (DLCI).

Переваги мереж Frame Relay полягають у їхній низькій протокольній надмірності та дейтаграмному режимі роботи, що забезпечувало відносно високу пропускну здатність і невеликі затримки кадрів для свого часу. Однак, ключовим недоліком Frame Relay є відсутність вбудованих механізмів корекції та відновлення помилок, а також відсутність гарантій щодо величини затримок. Саме цей фактор є основною перешкодою для ефективного застосування цієї технології для передачі чутливих до затримок послуг, таких як голосовий зв'язок (VoIP).

MPLS (Multiprotocol Label Switching – багатопротокольна комутація за мітками) є сучасним та потужним механізмом передачі даних, що поєднує

переваги мереж з комутацією каналів та комутацією пакетів. Цей протокол функціонує на рівні, який часто називають «рівнем 2,5» (між канальним та мережевим рівнями моделі OSI).

Основна ідея MPLS полягає в тому, що замість традиційної IP-маршрутизації, де кожен маршрутизатор на шляху проходження пакета виконує детальний аналіз заголовка пакета для визначення наступного переходу, в MPLS управління переадресацією здійснюється виключно на основі коротких міток. Ці мітки додаються до пакетів на вході в MPLS-мережу. Маршрутизатори (Label Switch Routers, LSR) в MPLS-мережі просто зчитують ці мітки та використовують їх для швидкого пересилання пакетів за визначеними шляхами (Label Switched Paths, LSPs) без необхідності повторного аналізу IP-заголовка.

Такий підхід надає численні переваги над традиційною маршрутизацією на мережевому рівні:

- висока швидкість обробки пакетів завдяки комутації за мітками, яка є швидшою за традиційну маршрутизацію;
- підтримка різних типів трафіку бо MPLS є багатопротокольним і може ефективно передавати IP-пакети, а також емулювати властивості ATM, Frame Relay, SONET та кадри Ethernet, що робить його універсальним рішенням;
- можливість реалізації QoS та Traffic Engineering, що дозволяє більш тонко управляти якістю обслуговування (QoS) та інженерією трафіку, забезпечуючи пріоритезацію чутливого до затримок трафіку (наприклад, VoIP та відео), що є критичним для мережі «Лідер Взуття».
- спрощення створення VPN.

В табл. 2.2 проведено порівняльний аналіз технологій за основними і важливими в контексті даної роботи параметрами.

Таблиця 2.2 – Порівняння технологій побудови мережі

Технологія	MPLS	Frame Relay	VPN
Пропускна здатність	Будь-яка	До 35 Мбіт/с	Будь-яка
Захищеність мережі	Висока	Висока	Низька
Необхідність покупки послуги від одного провайдера	Так	Так	Ні

В будь-якому з обраних механізмів і підходів до побудови слід знати та пам’ятати, що використання віртуальних каналів для побудови корпоративної мережі має спільний недолік, бо при великій кількості точок доступу та складному характері зв'язків може вимагатися значна кількість окремих віртуальних каналів, і кожен з яких має оплачуватися окремо.

Аналіз чинних та перспективних технологій для реалізації транспортної інфраструктури мережі "Лідер Взуття" свідчить про неефективність застосування технології Frame Relay у сучасних умовах. Основними обмеженнями цієї технології є відсутність гарантій якості обслуговування (QoS) для додатків реального часу, а також технічна неспроможність розширити швидкість передачі даних понад 34.368 Мбіт/с. Отже, з огляду на зростаючі потреби в масштабованості та продуктивності, Frame Relay не відповідає вимогам сучасної бізнес-мережі. Мережа "Лідер Взуття" потребує сучасного технологічного рішення, здатного забезпечити надійну підтримку голосового трафіку та інших додатків, чутливих до затримок.

Оцінюючи альтернативні варіанти, технологія MPLS (Multiprotocol Label Switching) виступає як найбільш перспективна для модернізації транспортного сегмента. Використання MPLS гарантує підвищену ефективність у керуванні трафіком, високу продуктивність та можливості забезпечення QoS. Ці характеристики є особливо важливими для інтеграції сервісів реального часу.

Таким чином, визначаються два ключові підходи до організації транспортної мережі з використанням підключення до Інтернету:

1. Побудова віртуальних приватних мереж (VPN) поверх публічного Інтернету.
2. Використання послуг MPLS VPN, що надаються оператором

зв’язку.

Головна різниця між цими підходами полягає у рівні гарантій пропускної здатності та якості обслуговування (QoS).

У разі використання VPN на базі публічного Інтернету відсутні будь-які гарантії щодо QoS. Через негарантований характер публічної мережі Інтернет можуть виникати значні коливання затримки, джитеру і втрати пакетів, що здатне негативно вплинути на працездатність критично важливих бізнес-додатків й якість голосових сервісів. Проте цей підхід характеризується нижчими витратами на впровадження та експлуатацію, а також широкою доступністю Інтернет-з’єднань. Завдяки цьому забезпечується охоплення філій у різних регіонах незалежно від наявності локальних операторів MPLS.

Натомість MPLS VPN, що пропонується оператором зв’язку, гарантує пропускну здатність і QoS на визначеному рівні. Відповідальність за забезпечення зазначених параметрів покладається на провайдера послуг, що є істотним плюсом для сервісів реального часу. Проте такий варіант зазвичай коштує дорожче і може бути недоступним у певних регіонах через інфраструктурні обмеження.

На даний момент транспортний сегмент мережі «Лідер Взуття» реалізовано шляхом побудови статичних VPN-тунелів, що відповідає першій із зазначених опцій. Однак використання виключно статичних VPN-тунелів має очевидні недоліки для великої кількості філій та під час росту обсягів трафіку.

Серед можливих архітектур VPN-мереж найчастіше застосовуються такі топології:

- Hub-and-spoke. У цьому варіанті всі філії підключаються до центрального вузла. Ця архітектура проста у впровадженні, але має обмеження через централізовану точку відмови і можливе перевантаження головного вузла.
- Full mesh. Кожен вузол мережі має пряме з’єднання з усіма іншими вузлами. Такий підхід забезпечує високу надійність і мінімальні затримки, однак відзначається значною складністю впровадження

та високими витратами при масштабуванні великої кількості вузлів.

– Partial mesh. Є поєднанням різних мережевих топологій, де окремі вузли мають прямі з'єднання, в той час як інші - ні. Такий підхід дозволяє досягти оптимального балансу між надійністю мережі, її продуктивністю та витратами на впровадження й підтримку.

Нижче розглянемо переваги та недоліки кожної з типових топологій у контексті мережі магазинів «Лідер Взуття».

На рис. 2.1 представлена топологія «зірка» (Hub-and-Spoke).

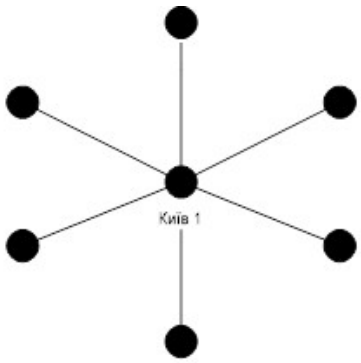

Рисунок 2.1 – Топологія «зірка»

Як зображено на рис. 2.1, топологія зірки передбачає, що всі периферійні вузли (тобто філії чи окремі магазини) взаємодіють між собою виключно через центральний вузол — у випадку мережі «Лідер Взуття» таким є головний офіс, розташований у Києві.

Перевагами такого рішення є простота впровадження та адміністрування і значне зменшення. Ця топологія вирізняється простотою реалізації і забезпечує централізоване управління мережею, спрощуючи її обслуговування та модернізацію інфраструктури. Також така архітектура потребує меншої кількості VPN-з'єднань, порівняно з іншими варіантами, витрати на обслуговування мережі суттєво знижуються.

Недоліками є:

– перевантаження центрального вузла;

– зниження показників якості послуг (QoS);

– обмежена надійність.

Центральний маршрутизатор (hub) має виконувати обробку всього трафіку мережі, що створює підвищені вимоги до його продуктивності та ширини каналу зв’язку. Таке навантаження формує ризик виникнення вузького місця у системі й відповідає концепції єдиної точки відмови (single point of failure). Оскільки весь мережевий трафік проходить через центральний вузол, це збільшує часові затримки (latency) та нерівномірність доставки пакетів (джиттер). Така проблема є особливо критичною для послуг, що залежать від передачі даних у реальному часі, наприклад, IP-телефонії. Важливим є також, що вихід зі строю центрального вузла або його каналів зв’язку спричиняє збій у роботі всієї мережі. Попри наявність рішення у вигляді резервування центрального вузла (створення додаткового резервного вузла), це значно ускладнює мережеву архітектуру та підвищує вартість її реалізації.

Наступна топологія – повнозв'язна (рис. 2.2)

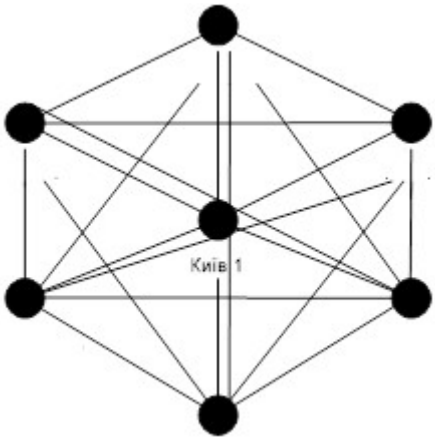

Рисунок 2.2 – Повнозв'язна топологія

На відміну від топології «зірка», повнозв'язна топологія забезпечує пряме з'єднання між усіма вузлами в мережі. До її переваг можна віднести:

– високий рівень QoS;

– відмовостійкість;

– розподіл та балансування навантаження.

Уникнення транзиту через центральний вузол дозволяє зменшити затримки та джиттер, що є критично важливим для додатків із потребою в реальному часі. Трафік рівномірно розподіляється між усіма вузлами, допомагаючи уникнути перевантаження окремих точок. Навіть при збої декількох вузлів чи каналів мережа продовжує працювати завдяки наявності альтернативних маршрутів.

Ключовим недоліком є складність управління та велика вартість. Із збільшенням кількості вузлів кількість необхідних VPN-з'єднань різко зростає за формулою $N \cdot (N-1)/2$, де N — кількість вузлів. Для великих мереж це може створити значні труднощі в управлінні. Також необхідність підтримки численних одночасних VPN-з'єднань значно підвищує вимоги до апаратури маршрутизаторів та їх обчислювальної потужності.

Компроміс між топологією «зірка» та повнозв'язною структурою представлений у вигляді часткової зв'язності (partial mesh), що зображено на рис. 2.3.

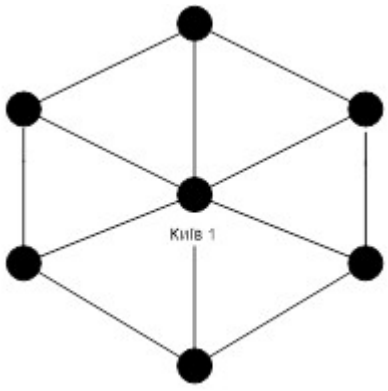

Рисунок 2.3 – Топологія partial mesh

У межах такої топології з'єднання встановлюються не за жорстко визначеними правилами, а з урахуванням актуальних потреб мережі. Це забезпечує пріоритетне створення резервних зв'язків для критично важливих вузлів, гарантуючи їхню максимальну доступність. У той же час вузли з меншою важливістю можуть мати лише одне або кілька з'єднань із мережею, зазвичай через центральний вузол або найближчий локальний центр.

Переваги:

- оптимальний баланс між витратами та надійністю дозволяє досягти необхідного рівня відмовостійкості для ключових вузлів без значного ресурсоємного навантаження на мережу;
- гнучкість дає змогу адаптовувати мережу відповідно до специфічних бізнес-потреб та поточного трафіку;
- поліпшення якості обслуговування (QoS) у порівнянні із топологією «зірка» завдяки можливості створювати прямі канали зв'язку між важливими вузлами.

Недоліки:

- висока складність проектування через те що на початковому етапі інтеграції потрібен детальний аналіз трафіку та важливості вузлів для правильної побудови структури.
- ризик виникнення вузьких місць через неналежне планування і створення нових зон перевантаження.

Проаналізовані топологічні моделі вказують на те, що жодна з них у чистому вигляді не здатна цілком задовольнити специфічні потреби мережі «Лідер Взуття». Ключовими недоліками є низька надійність та проблеми з QoS у «зірковій» топології; надмірна складність і високі витрати на обслуговування в повнозв'язній структурі; вимоги до ретельного проектування у випадку часткової зв'язності.

З огляду на це, виникає необхідність пошуку оптимального підходу. Він повинен забезпечувати підтримку великої кількості VPN-тунелів, гарантувати відмовостійкість через резервні підключення та зберігати простоту обслуговування мережі. Це свідчить про доцільність застосування гібридної топології або запровадження сучасних інтелектуальних рішень, які здатні динамічно керувати VPN-з'єднаннями.

Для розв’язання цієї складної задачі пропонується інтеграція технології динамічних VPN-тунелів, відомих як DMVPN (Dynamic Multipoint VPN).

Основна концепція роботи DMVPN полягає в тому, що тунелі

створюються й функціонують тільки у разі реальної необхідності, а не підтримуються постійно. Цей підхід дозволяє об’єднати переваги топологій типу «зірка» та «повнозв’язна». Початкова конфігурація DMVPN передбачає присутність одного або кількох центральних вузлів (Hub), до яких усі периферійні вузли (Spoke) мають постійне з’єднання, формуючи базову топологію «зірка». Утім, у разі потреби в безпосередньому обміні даними між двома периферійними вузлами, технологія DMVPN може автоматично налаштувати тунель прямого з’єднання між ними («Spoke-to-Spoke») без залучення центрального вузла.

Ця технологія є ідеальним рішенням для організації транспортної мережі в межах модернізації транспортного сегменту телекомунікаційної мережі магазинів «Лідер взуття», оскільки вона:

- забезпечує логічну повнозв’язну мережу – надає переваги топології full-mesh, такі як зменшені затримки та покращене якісне обслуговування (QoS), водночас уникаючи зайвої складності адміністрування;
- ефективно використовує ресурси – тунелі активуються виключно за необхідністю, що значно знижує навантаження на маршрутизатори та зменшує кількість постійних з’єднань;
- дозволяє легке масштабування – в процесі додавання нових філій достатньо підключити їх до центрального вузла Hub, а надалі нові вузли зможуть динамічно встановлювати прямі з’єднання з іншими Spoke-вузлами за потреби.

Для реалізації VPN-тунелів у рамках DMVPN використовується протокол GRE (Generic Routing Encapsulation).

Для побудови взаємодії між вузлами будуть застосовуватися наявні канали доступу до Інтернету. Надзвичайно важливо зазначити, що різні вузли можуть використовувати різних провайдерів або способи підключення до Інтернету, а DMVPN в свою чергу дозволяє забезпечити стабільну роботу навіть за умов неоднорідної інфраструктури.

Попри відсутність галузевого стандарту для DMVPN, реалізації цієї технології можуть варіюватися залежно від виробника обладнання. Для ілюстрації принципів її роботи найбільш доцільно розглянути рішення від компанії Cisco.

На рис. 2.4 зображена типова мережа DMVPN, що складається з одного центрального вузла (Hub) та декількох периферійних вузлів (Spoke).

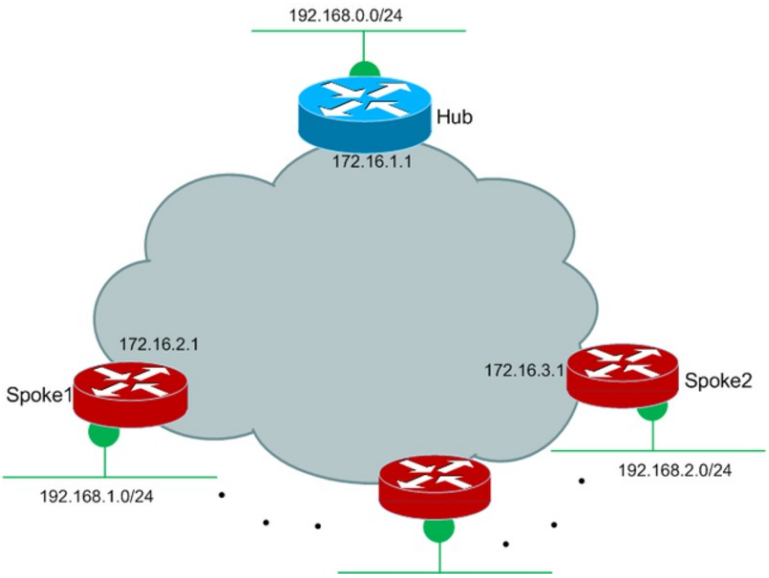

Рисунок 2.4 – Схема DMVPN мережі з Hub та Spoke вузлами

«Лідер Взуття» потребує не лише класичного зв'язку периферійних вузлів із центральним, але й налагодженої комунікації між самими філіями (Spoke-to-Spoke). Така функціональність реалізується за допомогою технології DMVPN, яка базується на використанні протоколу Next-Hop Resolution Protocol (NHRP).

Ключова роль у DMVPN належить саме NHRP, який відповідає за динамічне створення тунелів між всіма вузлами мережі. У цьому процесі маршрутизатори задіюють тунельні інтерфейси типу multipoint GRE (mGRE), що дозволяє одному GRE-інтерфейсу обслуговувати кілька тунельних з'єднань одночасно. Для забезпечення безпеки всі передані дані через ці тунелі шифруються, що гарантує конфіденційність та цілісність інформації.

Принцип роботи NHRP включає такі етапи:

1. Центральний вузол (Hub) в термінології NHRP виконує роль NHS (Next-Hop Server). На початковому етапі NHS не має даних про жоден із периферійних вузлів.
2. Реєстрація вузлів Spoke. Коли периферійні вузли (відомі як NHC — Next-Hop Client) підключаються до мережі, вони надсилають реєстраційні запити до NHS.
3. Формування таблиці відображень. Після завершення реєстрації всіх NHC, NHS створює деталізовану таблицю, яка містить їхні внутрішні IP-адреси та відповідні зовнішні (фізичні) IP-адреси.
4. Динамічний запуск Spoke-to-Spoke тунелів. Коли один NHC, наприклад, філія у місті Житомир, ініціює зв'язок із іншим NHC, наприклад, філією у Дніпрі, він звертається до NHS за даними про цільовий вузол. Отримавши відповідь, обидва NHC самостійно встановлюють прямий VPN-тунель у форматі Spoke-to-Spoke. Після цього вони можуть обмінюватись даними безпосередньо, без залучення NHS для передачі трафіку. Роль NHS обмежується лише ініціалізацією зв'язку та підтримкою таблиці адрес.

Ця архітектура забезпечує DMVPN можливістю створення масштабованої, надійної та безпечної транспортної мережі, яка ідеально відповідає зростаючим потребам компанії «Лідер Взуття». Такий підхід також здатен підтримувати сервіси реального часу, забезпечуючи ефективність та надійність роботи мережі.

Технологія DMVPN характеризується трьома основними режимами функціонування, які називаються фазами. Кожна фаза має унікальні особливості в побудові інфраструктури та маршрутизації трафіку, забезпечуючи різні рівні ефективності та гнучкості.

**DMVPN Фаза 1: **

Фаза 1: DMVPN – Топологія Hub-to-Spoke з динамічними Spoke.

Дана фаза функціонує на основі моделі «hub-to-spoke», де всі з'єднання проходять через центральний вузол (NHS). У цій фазі відсутня можливість

встановлення прямих тунелів між периферійними вузлами (NHC), тобто весь трафік spoke-to-spoke передається через хаб.

На рис. 2.5 показано, як відбувається встановлення сесій і обмін даними між двома пристроями, розташованими в різних периферійних вузлах (NHC).

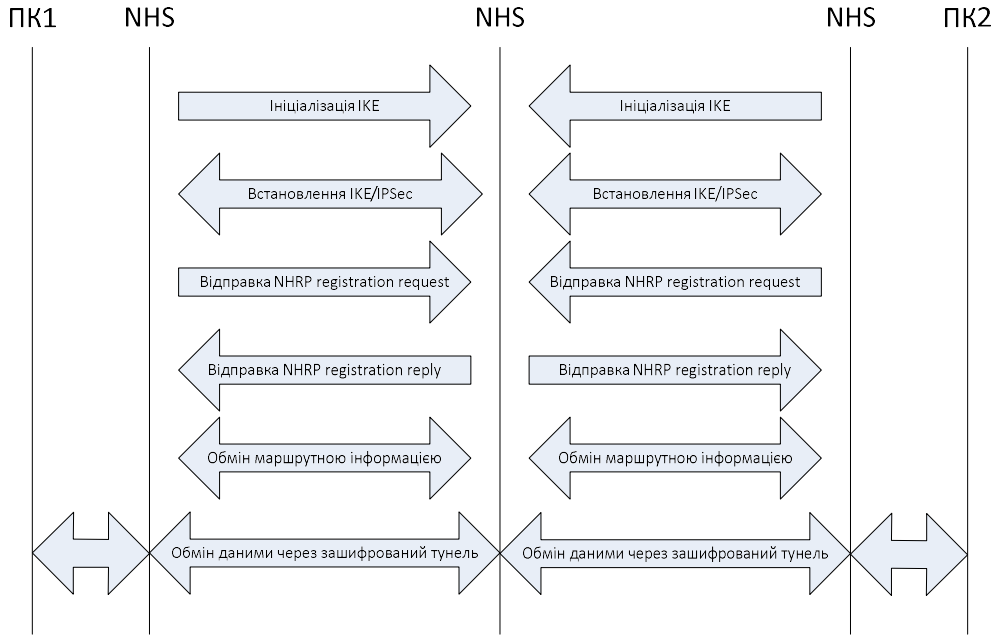

Рисунок 2.5 – Порядок встановлення сесій і обміну даними в рамках DMVPN Фази 1

Процедурний механізм роботи Фази 1 виглядає так.

Спершу відбувається процедура IKE (Internet Key Exchange) з подальшим встановленням основного тунелю IPsec між кожним NHC і центральним NHS. Це гарантує безпечне і зашифроване з'єднання в мережі. Після встановлення IPsec-тунелю кожен NHC відправляє запит реєстрації NHRP Registration Request до NHS. Цей етап дозволяє центральному вузлу отримати інформацію про внутрішні (приватні) IP-адреси NHC і їх відповідні зовнішні (публічні) IP-адреси. NHS підтверджує успішну реєстрацію, надсилаючи повідомлення NHRP Registration Reply. Це забезпечує, щоб центральний вузол мав точну картину доступних периферійних вузлів у мережі. Для того щоб забезпечити передачу трафіку між вузлами, NHC і NHS повинні обмінятися маршрутами своїх локальних мереж. Це може бути реалізовано за допомогою динамічних

протоколів маршрутизації (які краще підходять для масштабованих мереж) або статичних маршрутів (менш гнучкий варіант для великих інфраструктур). Після завершення всіх етапів налаштування периферійні вузли можуть почати обмінюватися даними. Однак характерною рисою Фази 1 є те, що весь трафік spoke-to-spoke проходить через центральний вузол, навіть якщо два периферійні вузли намагаються напряму зв’язатися один з одним.

Фаза 2: Механізм Тунелювання Spoke-to-Spoke.

Перехід до Фази 2 у рамках DMVPN представляє суттєвий еволюційний стрибок у порівнянні з попередньою Фазою 1. Основною перевагою цієї фази є впровадження можливості створення динамічних тунелів між периферійними вузлами (Spoke-to-Spoke). Такий підхід усуває необхідність транспортування всього мережевого трафіку через центральний вузол (Hub). Це, своєю чергою, значно підвищує ефективність мережі, особливо для додатків із підвищеними вимогами до затримок, таких як послуги реального часу.

На представленій діаграмі (рис. 2.6) ілюструється порядок встановлення сесій у мережі DMVPN Фази 2.

Процес встановлення прямого зв’язку у Фазі 2 відбувається за таким чином. На початку кожен периферійний вузол (Next Hop Client – NHC) встановлює постійний захищений IPsec-тунель із центральним вузлом (Next Hop Server – NHS). У процесі цієї взаємодії периферійні вузли реєструють свої приватні та публічні IP-адреси на NHS завдяки повідомленням реєстрації NHRP (NHRP Registration Request/Reply). У випадку, коли одному з периферійних вузлів (наприклад, Spoke «А») потрібно встановити з’єднання з іншим "периферійним вузлом (наприклад, Spoke «Б»), він надсилає запит NHRP Resolution Request до центрального NHS, який містить прохання надати публічну IP-адресу цільового Spoke «Б». Після отримання запиту центральний NHS надає Spoke «А» інформацію про публічну IP-адресу Spoke «Б», використовуючи механізм NHRP Resolution Reply. Отримавши необхідну адресу, Spoke «А» безпосередньо ініціює створення захищеного IPsec-тунелю з Spoke «Б». Після успішного встановлення цього тунелю подальша передача

даних між зазначеними вузлами здійснюється напряму без транзитного проходження через NHS.

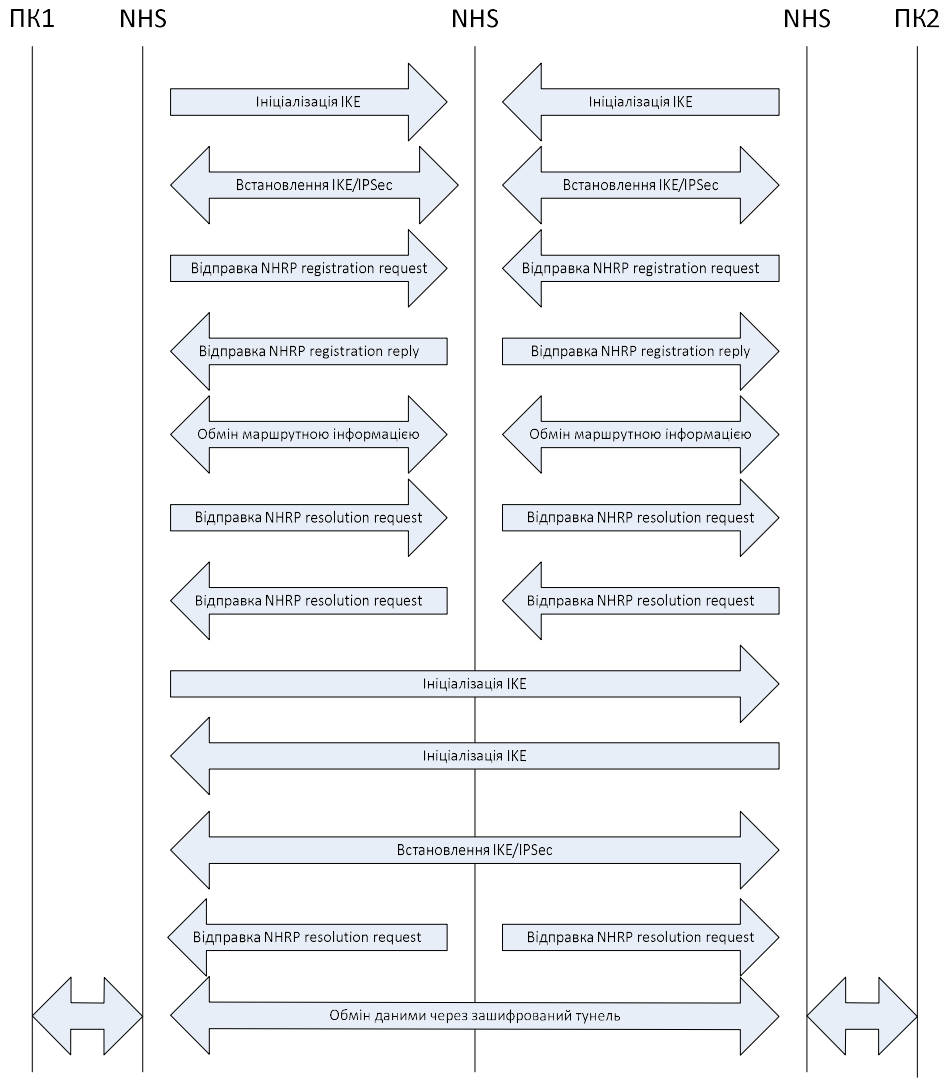

Рисунок 2.6 – Встановлення сесій у мережі DMVPN Фази 2

Третя фаза DMVPN являє собою подальший розвиток концепцій Фази 2, зосереджуючись на оптимізації маршрутизації і вдосконаленні взаємодії Node-to-Node за допомогою механізму NHRP Redirect. Ці дозволяє значно підвищити ефективність роботи мережі, особливо в умовах складних і масштабних інфраструктур.

Ключовою відмінністю між Фазами 3 та 2 є те що у Фазі 3 центральний маршрутизатор (NHS) може відправляти агреговані маршрути для всіх підмереж вузлів типу Spoke. Це значно зменшує розмір таблиць маршрутизації

на Spoke-маршрутизаторах, знижуючи їхню складність і спрощуючи процес конфігурації. Такий підхід також сприяє більш ефективному управлінню маршрутами в мережі.

У Фазі 3 центральний вузол NHS виконує функцію перенаправлення. Отримавши пакет, який не адресовано йому, NHS генерує спеціальне повідомлення — NHRP Redirect Message. Це повідомлення сигналізує відправнику про необхідність зміни адреси наступного вузла (next-hop), вказуючи на публічну IP-адресу кінцевого Spoke.

Принцип роботи механізму Spoke-to-Spoke у Фазі 3 включає три етапи:

1. Ініціалізація через Hub. На початковому етапі трафік між двома вузлами Spoke (NHC) передається через центральний вузол (NHS), за аналогічною схемою до тієї, що використовується у Фазі 1.
2. Генерація NHRP Redirect. Після отримання першого пакета NHS ідентифікує, що він не є кінцевим пунктом призначення для цього трафіку. У відповідь він надсилає відправнику спеціальне повідомлення — NHRP Redirect Message.
3. Динамічне оновлення next-hop і створення прямого з'єднання. Після отримання NHRP Redirect Message відправник оновлює адресу next-hop на публічну IP-адресу цільового Spoke. Далі відбувається автоматичне налаштування прямого IPsec-тунелю між кінцевими Spoke. Після цього увесь подальший обмін даними здійснюється через пряме Spoke-to-Spoke з'єднання, минаючи центральний вузол.

На рис. 2.7 представлена загальна схема організації мережі DMVPN, яка демонструє постійні тунелі типу Hub-to-Spoke та можливість динамічного встановлення з'єднань між Spoke-вузлами.

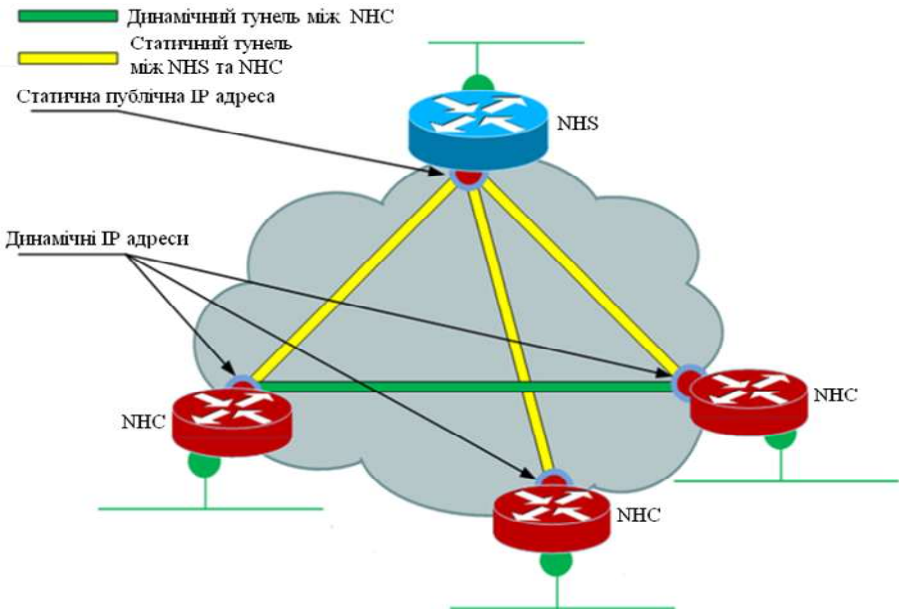

Рисунок 2.7 – Схема організації мережі DMVPN

Постійні з'єднання встановлюються лише між NHS (Network Hub Server) та NHC (Network Hub Client). При цьому NHS необхідно мати статичну публічну IP-адресу. Значною перевагою DMVPN є здатність NHC використовувати динамічні публічні IP-адреси, або навіть приватні IP-адреси (за умови знаходження за NAT). Це не перешкоджає створенню динамічних тунелів безпосередньо між вузлами Spoke. Така гнучкість суттєво полегшує розгортання в регіональних офісах, де часто застосовуються динамічні IP-адреси, видані провайдером.

Основна перевага DMVPN Фази 1 у порівнянні зі статичними VPN-тунелями полягає в тому, що вона дозволяє використовувати динамічні приватні IP-адреси на NHC. Це значно спрощує адміністрування та процес впровадження мережі – змінювати конфігурацію тунелів вручну більше не потрібно при зміні публічної IP-адреси філії, як це було б у разі статичних VPN.

Втім, основний недолік полягає в тому, що весь трафік spoke-to-spoke транзитом проходить через хаб, що призводить до збільшення затримок, створення потенційного вузького місця в центральному вузлі та збільшення навантаження на його ресурси. Ці проблеми стають особливо критичними для

додатків реального часу, таких як IP-телефонія чи відеозв’язок.

Головною перевагою запровадженої архітектури DMVPN Фази 2 є можливість оптимізації маршрутизації даних між периферійними вузлами. Це дозволяє суттєво зменшити затримки передачі, мінімізувати джиттер та розвантажити центральний маршрутизатор. У результаті така архітектура є більш ефективною для сучасних мереж із високими вимогами до якості обслуговування.

Таким чином, Фаза 3 забезпечує всі переваги прямої взаємодії між вузлами Spoke, які були представлені у Фазі 2, досягнувши при цьому більш ефективного управління маршрутами та швидшої установи тунелів. Ці вдосконалення мають особливе значення при впровадженні DMVPN у великих і складних мережах із великою кількістю вузлів і складною топологією.

2.3 Політика CoS/QoS

Однією з головних проблем сучасних IP-мереж є забезпечення ефективного контролю та управління трафіком. Для подолання цієї проблеми застосовуються спеціалізовані політики, спрямовані на оптимальний розподіл інформаційних потоків і пріоритизацію обробки критичних даних. Протокол IP, який автивно застосовується в мережах передачі даних спочатку створений для передачі даних в Інтернеті, не передбачав жорстких гарантій доставки інформації. Аналогічно, Ethernet у локальних мережах функціонує за принципом «best effort service», що також не гарантує надійності доставки. У традиційних сценаріях передачі даних, таких як електронна пошта або обмін файлами, невеликі затримки чи втрати пакетів зазвичай залишаються непомітними або лише мінімально впливають на користувачів. Проте ситуація змінюється при роботі застосунків із високими вимогами до стабільності та швидкості передачі даних. Це стосується корпоративної IP-телефонії, відеоконференцій та систем управління базами даних, чутливих до затримок. У

таких випадках навіть просте збільшення пропускної здатності каналу не вирішує проблему перевантаження мережі. Для забезпечення стабільної роботи всіх додатків у мережах зі змішаним трафіком необхідно змінити підхід до управління даними. Сьогодні розроблено низку схем для впровадження QoS/CoS у локальних і розподілених мережах, що дозволяють суттєво підвищити ефективність їх використання.

Одним із найпростіших і найбільш поширених підходів у рамках забезпечення якості обслуговування (QoS) та класу обслуговування (CoS) є пріоритизація мережевого трафіку.

У стандарті IEEE 802.1p передбачено вісім рівнів пріоритетності (від 0 до 7), які записуються в спеціальні біти тегу VLAN. Організація IETF застосовує подібний підхід, використовуючи спеціальні біти в IP-заголовку (DiffServ Code Point - DSCP).

У середовищах де потрібна мала затримка передачі даних і гарантована пропускна здатність, застосовуються складніші схеми QoS. Ці механізми дозволяють здійснювати детальний контроль за управлінням пропускною здатністю, мінімізувати затримки та суворо регулювати дотримання пріоритетів, включно з визначенням пакетів, які слід відкинути в разі переповнення черги.

Протокол RSVP забезпечує розподіл і резервування пропускної здатності для певного типу трафіку. Однак його складність у реалізації та підтримці обмежує широке застосування в корпоративних мережах. Альтернативою є більш сучасний і гнучкий механізм забезпечення QoS в IP-мережах – MPLS.

Ефективним і значно економічнішим підходом до управління трафіком, порівняно з впровадженням повноцінної політики QoS із резервуванням ресурсів, може бути розподіл смуги пропускання на логічні сегменти для окремих потреб. Функції пріоритезації використовуються в багатопротокольних маршрутизаторах і комутаторах. Класифікація може базуватися на різних параметрах, наприклад, типі протоколу. Для прикладу, дані SNMP-протоколу, що використовуються для керування мережею, зазвичай

належать до найвищого класу пріоритету.

Існують різноманітні схеми маркування CoS і QoS:

- пріоритезація на основі MAC-адреси – дає змогу визначати пріоритет для трафіку від певних пристроїв;
- VLAN-мітки та 802.1p – у межах стандарту IEEE 802.1Q (для VLAN) три біти з P-bit (Priority Code Point, PCP) VLAN-мітки можуть позначати до восьми рівнів пріоритету (0–7). Такі мітки дозволяють мережевому обладнанню ідентифікувати пакети належного класу обслуговування;
- TOS (Type Of Service) / DSCP (DiffServ Code Point) – заголовок IP-пакета містить поле TOS, яке, відповідно до стандартів IETF, використовується в рамках Differentiated Services (Diff-Serv). Diff-Serv класифікує й маркує пакети так, щоб їм призначався певний тип обслуговування чи маршрут у мережі. Політика визначає встановлення бітів TOS/DSCP, які читаються пристроями для виконання певних правил QoS. Завдяки універсальності протоколу IP механізм Diff-Serv забезпечує CoS як у локальних мережах (LAN), так і у розподілених середовищах (intranet чи extranet).

Наразі йде процес поступового відмовлення від використання поля TOS на користь DSCP. Поле DSCP є розширенням IP-пріоритету й використовує 6 із 8 бітів у полі TOS, що дозволяє визначити 64 різні варіанти сервісів.

Схема трансляції заголовка IP-пакета з полями TOS і DSCP представлена на рис. 2.8.

Рисунок 2.8 – Біти типів обслуговування (IP-заголовок)

Класифікація даних пакетів може бути виконана різними методами.

Найефективнішим підходом є реалізація безпосередньо на рівні користувацького додатку або кінцевого пристрою, наприклад, IP-телефону. Проте, враховуючи, що більшість програмного забезпечення зазвичай не підтримують усі доступні схеми класифікації, дану функцію здебільшого здійснюють багаторівневі комутатори (Layer 2/3 Switches) чи маршрутизатори. Ці пристрої дозволяють аналізувати різноманітні поля заголовків пакетів та застосовувати відповідні політики залежно від заданих умов.

2.4 Вибір технології модернізації транспортної мережі

На основі здійсненого аналізу існуючої мережевої інфраструктури та ретельно сформульованого опису запропонованих технологічних рішень, зокрема DMVPN та QoS/CoS, необхідно обрати шлях модернізації мережі. З метою забезпечення об’єктивності й наукової обґрунтованості цього рішення буде застосовано методологію експертних оцінок та системи критеріїв.

Методи експертного оцінювання становлять формалізовані процедури, спрямовані на структурування взаємодії з компетентними фахівцями для отримання їхніх висновків у кількісному чи якісному форматі. Такі дослідження проводяться для підготовки аналітичних матеріалів, які надають основу для ухвалення управлінських рішень відповідальними особами.

Для об’єктивного вибору оптимального рішення з реструктуризації мережі були визначені такі критеріальні показники:

- складність реалізації мережі (оцінюється рівень трудомісткості та обсяг ресурсів, необхідних для впровадження запропонованого рішення);
- величина затримки (прогнозований рівень затримок передачі даних для забезпечення якості сервісів реального часу);
- гарантована пропускна здатність (спроможність забезпечити мінімальну гарантовану пропускну здатність);

- сумісність з існуючим обладнанням (можливість використання поточного активного устаткування без масштабного оновлення);
- надійність передачі (здатність мережевої архітектури протидіяти збоям та забезпечувати стабільну доставку даних).

Для оцінювання застосовано п'ятибальну систему, де 1 бал вказує на найвищу відповідність критерію, а 5 балів − на найнижчу.

Розглянуто такі комбінації технологій, що включають різні етапи розвитку DMVPN у синергії з різноманітними механізмами QoS/CoS: 1 фаза DMVPN + RSVP; 1 фаза DMVPN + MPLS; 1 фаза DMVPN + DSCP; 2 фаза DMVPN + RSVP; 2 фаза DMVPN + MPLS; 2 фаза DMVPN + DSCP; 3 фаза DMVPN + RSVP; 3 фаза DMVPN + MPLS; 3 фаза DMVPN + DSCP.

Для встановлення найоптимальнішого підходу до модернізації корпоративної мережі була побудована експертна матриця (табл. 2.3), що містить індивідуальні оцінки варіантів за визначеними критеріями.

Таблиця 2.3 – Матриця експертних оцінок

	складність реалізації мережі	планується величина затримки	гарантування пропускної здатності	можливість використання існуючого устаткування	надійність доставки
1 фаза DMVPN + RSVP	4	3	3	4	4
1 фаза DMVPN + MPLS	5	2	3	5	2
1 фаза DMVPN + DSCP	3	2	3	1	4
2 фаза DMVPN + RSVP	4	2	2	4	3
2 фаза DMVPN + MPLS	5	3	2	5	2
2 фаза DMVPN + DSCP	3	4	3	1	3
3 фаза DMVPN + RSVP	4	2	2	4	3
3 фаза DMVPN + MPLS	5	2	3	5	3
3 фаза DMVPN + DSCP	2	3	2	1	3

Після отримання експертних оцінок було проведено їхню обробку з

використанням методу середнього арифметичного та методу медіан для визначення оптимального рішення. Результати проведених розрахунків та отримані ранжировки наведені в табл. 2.4.

Таблиця 2.4 – Результати обробки експертної оцінки та ранжировка

	1 фаза DMVPN + RSVP	1 фаза DMVPN + MPLS	1 фаза DMVPN + DSCP	2 фаза DMVPN + RSVP	2 фаза DMVPN + MPLS	2 фаза DMVPN + DSCP	3 фаза DMVPN + RSVP	3 фаза DMVPN + MPLS	3 фаза DMVPN + DSCP
Сума рангів	18	17	13	15	17	14	15	18	11
Середнє арифм. рангів	3,6	3,4	2,6	3	3,4	2,8	3	3,6	2,2
Підс. ранг по серед. арифм.	8,5	6,5	2	4,5	6,5	3	4,5	8,5	1
Медіани рангів	3,7	3,34	2,67	3	3,34	3	3	3,7	2,34
Підс. ранг по медіанах	8,5	6,5	5	3	6,5	3	3	8,5	1

На основі проведеного аналізу експертних оцінок обрано впровадження третьої фази DMVPN у поєднанні з методом DSCP. Ця комбінація забезпечує найвищі результати за більшістю критеріїв, зводячи до мінімуму складність реалізації та гарантуючи оптимальну якість обслуговування. Це особливо важливо для інтеграції IP-телефонії та інших сервісів реального часу в інфраструктурі мережі "Лідер Взуття". Обрання даного рішення сприятиме створенню високопродуктивної, надійної та масштабованої транспортної мережі, яка відповідатиме сучасним стандартам і потребам бізнесу.

2.5 Опис оновленої структури транспортного сегменту мережі

Загальна структура мережі зберігає основні риси, проте її функціонування зазнає значних змін завдяки впровадженню нових, більш прогресивних

механізмів управління трафіком і динамічного встановлення захищених з'єднань.

У процесі модернізації мережі планується впровадження таких ключових технологій:

- IPsec VPN для забезпечення безпечного зв’язку між головним офісом і філіями;
- Cisco DMVPN (Dynamic Multipoint VPN) Фаза 3 для динамічної прямої передачі даних між філіями (spoke-to-spoke) без необхідності транзиту через центральний вузол;
- DSCP (DiffServ Code Point) як механізм забезпечення Quality of Service (QoS) для пріоритетного обслуговування критичного трафіку.

Для реалізації функцій шифрування та захисту на маршрутизаторах використовуватиметься програмне забезпечення Cisco IOS VPN, вбудоване в операційну систему маршрутизаторів Cisco. Це дозволяє створювати віртуальну приватну мережу VPN швидко й ефективно, адаптуючи її для компаній різного масштабу та складності топології.

Технологія Cisco DMVPN, заснована на принципі динамічного з'єднання вузлів мережі, може використовуватись як у поєднанні із системами безпеки (зокрема Cisco IOS Firewall та Cisco IOS IPS), так і з іншими сучасними мережевими механізмами: QoS; IP Multicast; Split Tunneling; routing-based failover.

Використання можливостей Cisco DMVPN сприяє створенню VPN-мереж із функціями балансування навантаження і резервування каналів, що усуває необхідність налаштування кожного з’єднання вручну. З'єднання формуються автоматично відповідно до заданих політик доступу та безпеки. DMVPN підтримує різноманітні протоколи маршрутизації, включаючи Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest Path First (OSPF) та Border Gateway Protocol (BGP).

Мережа «Лідер Взуття» не матиме класичної трирівневої архітектури

через переважно віртуальний характер більшості з'єднань. Практично кожен маршрутизатор у філіях матиме лише один фізичний канал для доступу до Інтернет через провайдера. Всі внутрішньокорпоративні зв’язки реалізуються за допомогою побудови віртуальних тунелів. Такий підхід забезпечує значну економію коштів, а також підвищує конфіденційність переданої інформації завдяки використанню шифрування. Проте необхідно враховувати можливі труднощі, такі як підвищене навантаження на апаратні ресурси маршрутизаторів (зокрема, CPU і RAM) під час процесів шифрування і дешифрування трафіку.

Для динамічної організації з'єднань між вузлами мережі основою DMVPN є протокол NHRP (NBMA Next Hop Resolution Protocol). Цей протокол дозволяє станціям-відправникам ініціювати зв'язок з іншими вузлами у мережах, які не підтримують широкомовний доступ з множинним доступом (NBMA). Він забезпечує динамічне визначення адрес мережевого рівня та NBMA-адрес маршрутизатора, який є наступною точкою у напрямку до станції-одержувача. Усі маршрутизатори в мережі DMVPN використовують NHRP для автоматичного визначення адрес наступного маршруту. У «Лідер Взуття» центральним вузлом (Next-Hop Server, NHS) служить головний офіс у Києві (Київ1).

Дані інкапсулюються за допомогою протоколу GRE (Generic Routing Encapsulation), що дозволяє інкапсулювати пакети мережевого рівня (наприклад, IP або IPX) у IP-пакети. Це тунельний протокол, який ідентифікується в заголовку IP за номером 47. Тунель GRE складається з трьох основних компонентів – інкапсульований протокол, протокол інкапсуляції та транспортний протокол.

Для забезпечення захисту інформації та її шифрування застосовують набір протоколів IPsec. На відміну від SSL/TLS, IPsec функціонує на мережевому рівні (третій рівень моделі OSI), що дозволяє забезпечувати безпеку будь-яких протоколів, побудованих на основі TCP та UDP. Завдяки своїй архітектурній гнучкості, IPsec може застосовуватись для безпечного

обміну даними між IP-вузлами, між шлюзами безпеки, а також між IP-вузлом і шлюзом безпеки. IPsec є доповненням до протоколу IP, опрацьовуючи вже сформовані IP-пакети. Цей набір протоколів забезпечує функції підтримки цілісності даних, конфіденційності, аутентифікації джерела інформації, а також захисту від повторної передачі пакетів.

Для передачі даних через тунелі DMVPN використовують схему GRE over IPsec, у якій GRE-тунелі інкапсулюються в IPsec. Завдяки такому підходу забезпечується як шифрування інформації, так і захист мережевого трафіку в процесі передачі.

Для виконання маршрутизації між вузлами в інфраструктурі DMVPN застосовується протокол маршрутизації EIGRP (Enhanced Interior Gateway Protocol). Це дистанційно-векторний протокол який є ідеальним вибором для топологій типу «зірка». У середовищі DMVPN така топологія ефективно реалізується шляхом створення логічних з'єднань між центральним вузлом і всіма іншими учасниками мережі. EIGRP використовує алгоритм DUAL для визначення найоптимальніших маршрутів і здійснює обмін маршрутною інформацією між пристроями засобами власного протоколу RTP.

Для взаємодії між провайдерами та корпоративною мережею проєкту передбачено використання протоколу BGP (Border Gateway Protocol). BGP є ключовим протоколом маршрутизації в Інтернеті, призначеним для обміну інформацією між автономними системами (AC) про доступність підмереж. Це протокол прикладного рівня, який функціонує на базі TCP з використанням порту 179. Після встановлення TCP-сесії між маршрутизаторами у провайдерів і корпоративної мережі відбувається обмін BGP-даними, що дозволяє формувати таблиці маршрутизації для доступу через глобальні мережі.

Механізм автоматичного призначення IP-адрес у локальних мережах філій реалізовано за допомогою протоколу DHCP (Dynamic Host Configuration Protocol). Цей протокол дає змогу пристроям автоматично отримувати IP-адреси та інші налаштування для роботи у середовищі TCP/IP.

Для забезпечення сегментації мережі та ізоляції різних груп користувачів

застосовуються віртуальні локальні мережі (VLAN), які реалізуються на основі стандарту IEEE 802.1Q (VLAN Tagging). Цей стандарт дозволяє одній фізичній Ethernet-мережі одночасно підтримувати кілька логічно ізольованих мереж. Використовуючи промарковані пакети VLAN, можливо організувати обмін даними між пристроями, підключеними до різних VLAN, через комутатори третього рівня моделі OSI або маршрутизатори. У проєктованій мережі VLAN забезпечують сегментацію для таких служб, як IP-телефонія, обслуговування касових терміналів чи робочих станцій.

Інкапсуляція даних прикладного рівня здійснюється за допомогою транспортних протоколів TCP та UDP. Протокол TCP характеризується високою надійністю: він забезпечує контроль доставки сегментів, нумерацію пакетів, повторну передачу втрачених даних і збір отриманих фрагментів у правильній послідовності на стороні отримувача. UDP, навпаки, є менш складним і працює без попереднього встановлення з'єднання, а також без підтверджень і гарантій передачі. Обидва протоколи — TCP і UDP — інкапсулюються в IP-протокол мережевого рівня (Internet Protocol), який відповідає за адресацію пакетів та їх передачу між мережами. Проте IP не забезпечує функціональності відстеження доставки та встановлення з'єднань.

Для наочності відповідність використаних протоколів до рівнів моделі OSI та до реалізованих послуг відображено у табл.2.5-2.6 відповідно.

Таблиця 2.5 – Протоколи, що використовуються у мережі за рівнями моделі OSI

Рівень моделі OSI	Протоколи
Прикладний	BGP, DHCP, DNS, FTP, HTTP, IMAP, NTP, POP3, RTCP, RTP, SIP, SMTP, SNMP, SSH, STUN, TLS/SSL, EIGRP
Представлення	ASCII
Сеансовий	RTCP, SSH
Транспортний	TCP, UDP
Мережевий	IP, ICMP, IPsec
Канальний	Ethernet
Фізичний	1000BASE-TX, 100BASE-TX

Таблиця 2.6 – Протоколи, що використовуються в реалізації послуг

Послуга	Протоколи
Internet	BGP, DHCP, DNS, FTP, HTTP, IMAP, NTP, POP3, RTCP, RTP, SIP, SMTP, SSH, STUN, TLS/SSL
Доступ до БД	DHCP, ARP, IP, TCP, SQL
Доступ до файлового сервера	DHCP, ARP, FTP, IP, TCP
VoIP	IP, ICMP, IPsec, Ethernet, GRE, DHCP, SIP, RTP, RTCP, UDP, TCP, STUN, NTP, ARP

Для забезпечення логічного поділу мережі доступу, і і підвищення її безпеки та управління трафіком, визначено ряд VLAN (табл. 2.7). Пріоритети DSCP впроваджені шляхом додавання відповідних тегів на абонентському обладнанні. Маршрутизатори та комутатори, будуть налаштовані на розпізнавання цих тегів і застосування відповідних політик управління чергами та пріоритетами. Відповідність типів трафіку заданим тегам DSCP наведено в табл. 2.8.

Таблиця 2.7 – Склад VLAN

№ VLAN	VLAN name	Призначення
101	tel	Пристрої корпоративної IP-телефонії
102	vk	Камери спостереження
103	kassa	Касові термінали
104	terminal	Платіжні термінали
105	pc	Персональні комп’ютери
106	free	Бездротові пристрої покупців

Таблиця 2.8 – Теги DSCP

Тип трафіку	Тег DSCP
Телефонія	5
АБС	4
УКМ "СуперМаг"	3
FTP	2
Mail	2
Інтернет	1

Висновки до розділу 2

У другому розділі випускної кваліфікаційної роботи проведено аналіз поточного стану транспортного сегменту телекомунікаційної мережі компанії «Лідер Взуття». Як виявилось, існуюча архітектури має кілька недоліків, які потребують усунення. Основні з них це недостатня масштабованість, обмежена відмовостійкість та незадовільна якість обслуговування (QoS) для додатків, чутливих до затримок, таких як IP-телефонія. Ці обмеження ускладнювали ефективне функціонування сучасних бізнес-процесів підприємства та становили перепону для його подальшого зростання.

Для усунення виявлених недоліків та побудови високоефективної, надійної й захищеної мережевої інфраструктури було проаналізовано ряд технологій. На підставі порівняльного аналізу був обґрунтований вибір технології Dynamic Multipoint VPN (DMVPN) Фази 3 у поєднанні з механізмом DSCP (DiffServ Code Point) для забезпечення необхідного рівня якості обслуговування. Технологія DMVPN Фази 3 була відібрана завдяки її здатності створювати логічно повнозв’язну мережу з динамічним встановленням тунелів «spoke-to-spoke». Це дозволяє уникнути проблеми маршрутизації міжфіліального трафіку через центральний вузол, скорочує затримки, оптимізує маршрутизацію та зменшує навантаження на центральну інфраструктуру.

Запропонований підхід, заснований на використанні DMVPN Фази 3 та DSCP, дає змогу створити гнучку, захищену, надійну та високопродуктивну транспортну мережу. Вона ефективно підтримуватиме всі корпоративні сервіси компанії «Лідер Взуття» та сприятиме її подальшому розвитку.

3 МОДЕЛЮВАННЯ РОБОТИ МЕРЕЖІ ТА ІМПЛЕМЕНТАЦІЯ ПРИЙНЯТИХ ПРОЄКТНИХ РІШЕНЬ

3.1 Постановка задачі моделювання

Для порівняльної оцінки поточної мережі та запропонованої оптимізованої архітектури необхідно проведести імітаційне моделювання роботи. Для цього розробити дві окремі моделі:

- модель існуючої мережі, яка відображатиме функціональні можливості та обмеження поточної інфраструктури компанії «Лідер Взуття»;
- модель реструктуризованої мережі, яка імплементуватиме всі прийняті проєктні рішення, зокрема технології DMVPN Фази 3 та DSCP для забезпечення якості обслуговування.

Метою моделювання є кількісна та якісна оцінка наступних ключових показників продуктивності мережі:

- надійність доставки;
- затримка.

Отримані результати моделювання мають підтвердити або ж спростувати правильність прийнятих рішень щодо реорганізації мережі.

Виходячи з поставленої мети та необхідності комплексного дослідження зазначених критеріїв, було обрано програмний пакет Cisco Packet Tracer. Використання саме цього продукту обумовлено можливістю повноцінного налаштування активного обладнання. Cisco Packet Tracer емулює широкий спектр активного мережевого обладнання Cisco (маршрутизатори, комутатори, бездротові точки доступу) з можливістю їх детального конфігурування за допомогою командного рядка (CLI), що повністю відповідає реальним пристроям. Це дає змогу точно імітувати поведінку та взаємодію протоколів DMVPN, IPsec, EIGRP, BGP, а також налаштування QoS (DSCP) та VLAN.

3.2 Розробка імітаційних моделей

Реалізація моделей на початковому етапі представляє собою створення структуру мережі на базі доступного обладнання і подальше його налаштування. Структура мережі повторює структурну схему з першого розділу, а налаштування мають відповідати прийнятим рішенням у другому розділі.

Розподіл адресного простору для локальних та глобальних сегментів мережі буде уніфікованим для обох моделей, що дозволить коректно порівнювати результати. Основні принципи розподілу адресного простору представлені в табл. 3.1.

Таблиця 3.1 – Принципи розподілу адресного простору в мережі

№ VLAN	VLAN name	Адресний простір
101	tel	192.168.1x.0/24
102	vk	192.168.2x.0/24
103	kassa	192.168.3x.0/24
104	terminal	192.168.4x.0/24
105	pc	192.168.5x.0/24
106	free	10.0.x.0/24

У відповідності до табл. 3.1, символ "x" у зазначених адресних просторах є унікальним ідентифікатором філії, що забезпечує унікальність адресного простору для всієї корпоративної мережі. Відповідність філії та її порядкового номеру, що підставляється замість "x", наведено в табл. 3.2.

Таблиця 3.2 – Відповідність філій та порядкового номеру

Філія	Порядковий номер
Київ 1	1
Київ 2	2
Бровари	3
Житомир	4
Дніпро	5
Харків	6
Херсон	7

Таким чином, наприклад, VLAN 101 (tel) у філії "Київ 2" (порядковий номер 2) матиме адресний простір 192.168.12.0/24. Цей підхід забезпечує чітке та масштабоване управління IP-адресами в мережі.

Налаштування правил DSCP (DiffServ Code Point) буде виконано у відповідності до політики QoS, визначеної в попередньому розділі, та деталізовано в табл. 3.3. Ці правила будуть застосовані до трафіку на мережевих пристроях, що підтримують QoS, для забезпечення пріоритезації.

Таблиця 3.3 – Правила DSCP

Тип трафіку	Тег DSCP
Телефонія	5
СУБ	4
УКМ "СуперМаг"	3
FTP	2
Mail	2
Інтернет	1

Варто зазначити, що представлені значення тегів DSCP (від 1 до 5) є умовними, спрощеними для цілей моделювання, і в реальних мережах відповідають стандартизованим значенням DiffServ Code Points (наприклад, EF для голосу, AFxx для інших пріоритетних класів). У моделі Packet Tracer ми будемо використовувати ці умовні значення для демонстрації пріоритезації.

В обох моделях (існуючої та реорганізованої) як протокол динамічної маршрутизації буде використано EIGRP. Цей вибір обумовлений його швидкою збіжністю та ефективністю в ієрархічних та частково зв'язних топологіях, що є характерними для VPN-мереж. Крім EIGRP, у моделі існуючої мережі можуть бути присутні статичні записи в таблиці маршрутизації, якщо це відповідає реальному стану мережі. У реорганізованій мережі EIGRP буде повноцінно інтегрований з DMVPN.

На базі визначених критеріїв та принципів, було розроблено дві візуальні моделі в Cisco Packet Tracer.

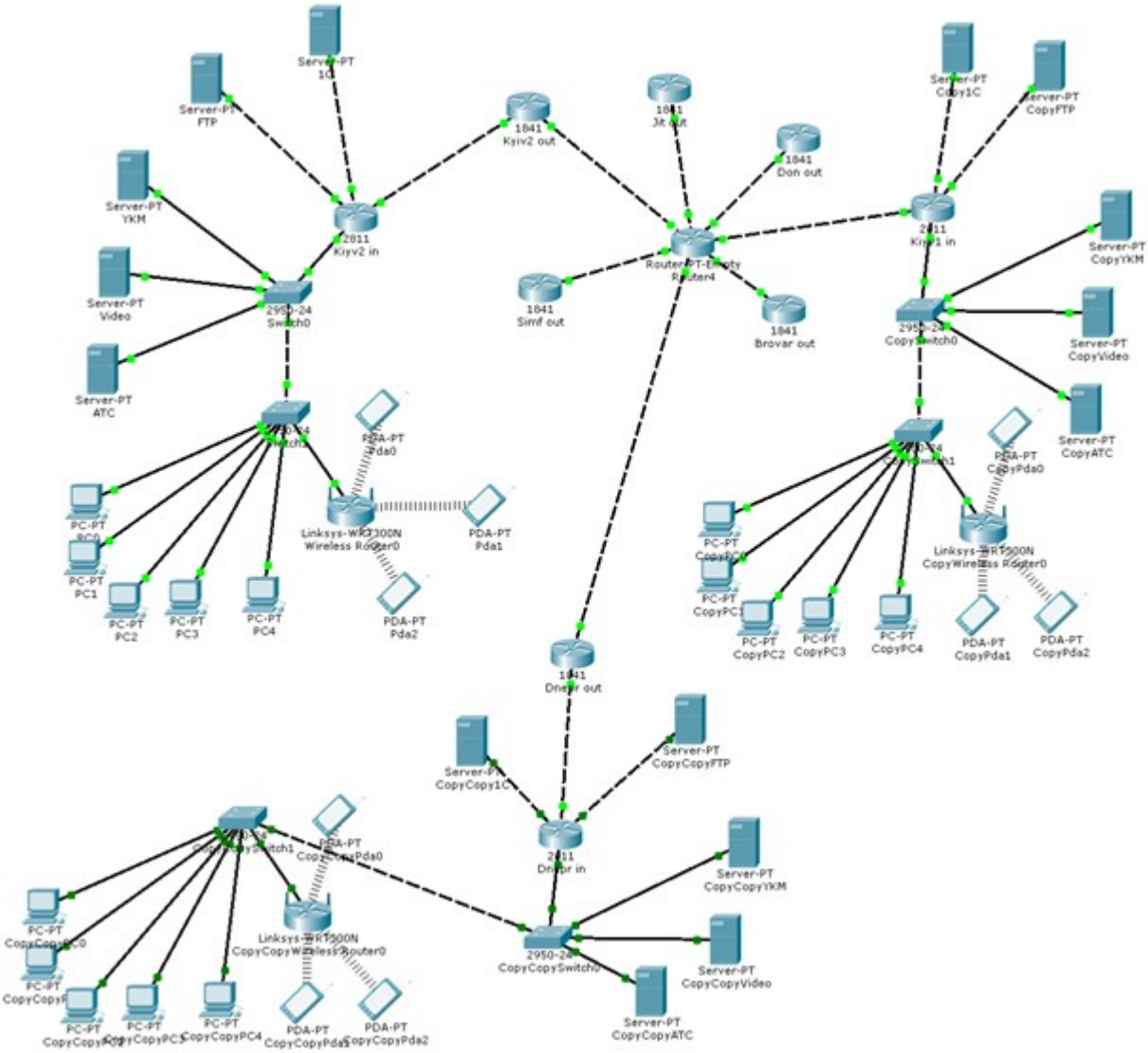

Рисунок 3.1 – Схема моделі існуючої мережі

Схема моделі існуючої мережі (рис. 3.1) відображає поточну топологію Hub-and-Spoke з використанням традиційних VPN-тунелів (IPsec) без динамічних spoke-to-spoke з'єднань. Усі міжфіліальні комунікації проходять через центральний маршрутизатор у Києві.

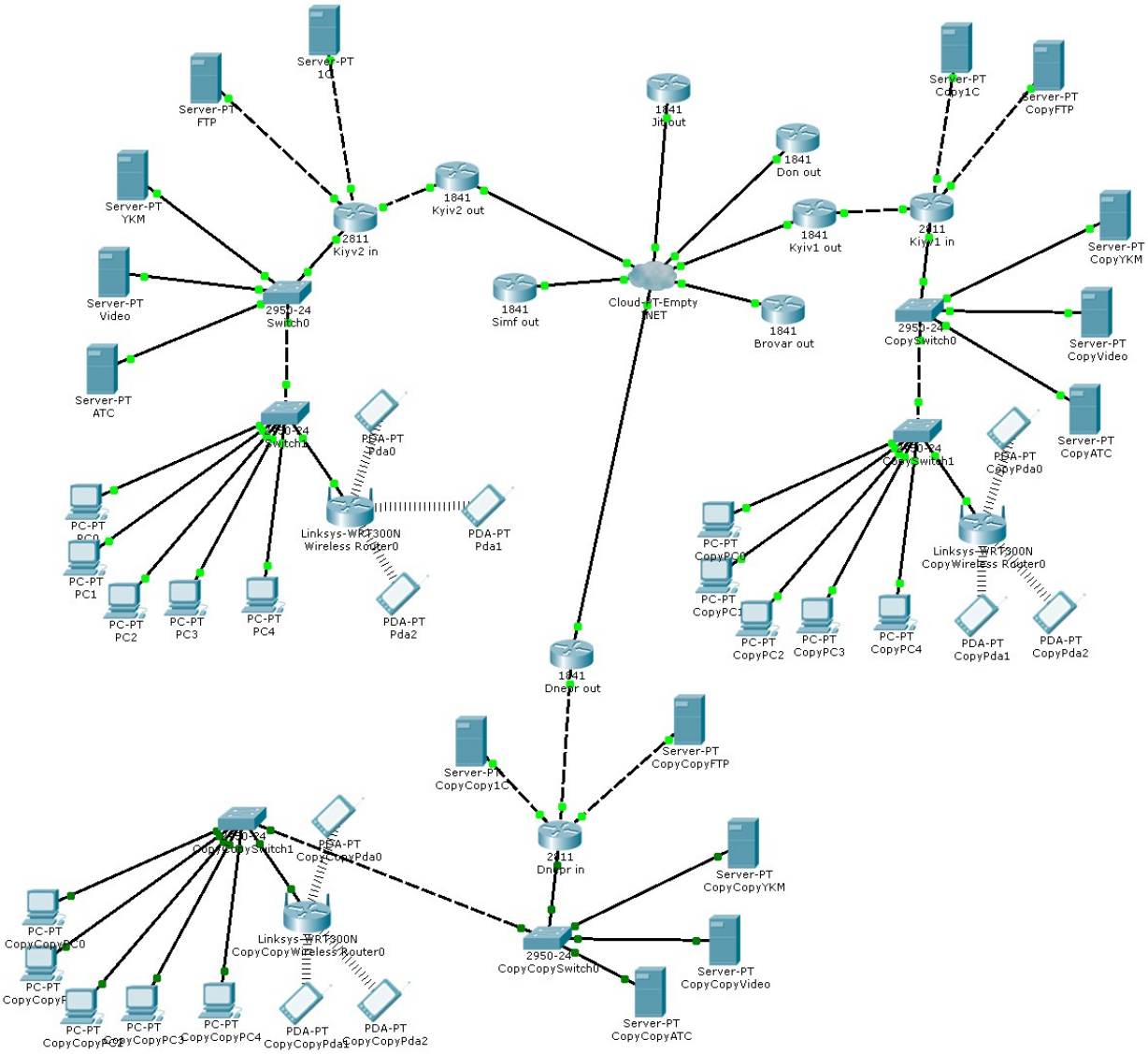

Рисунок 3.2 – Схема моделі реорганізованої мережі

Схема моделі реорганізованої мережі (рис. 3.2) демонструє впровадження DMVPN Фази 3. На цій схемі центральний маршрутизатор (Hub) та маршрутизатори філій (Spoke) налаштовані для підтримки динамічних тунелів, що дозволяє встановлювати прямі зв'язки між філіями без транзиту через Hub. Також на цій моделі будуть реалізовані налаштування QoS з DSCP на всіх ключових маршрутизаторах.

Налаштування центрального маршрутизатора (Hub - Київ1) Hub-маршрутизатор виступає як сервер NHRP та точка агрегації для всіх Spoke-тунелів.

```
! Конфігурація інтерфейсу, підключеного до Інтернету
interface GigabitEthernet0/0
 ip address <Публічна IP-адреса Hub> <Маска підмережі>
 ip nat outside
!
! Конфігурація внутрішнього інтерфейсу
interface GigabitEthernet0/1
 ip address 192.168.1.1 255.255.255.0
 ip nat inside
!
! Налаштування NAT для доступу в Інтернет
ip nat inside source list 1 interface GigabitEthernet0/0 overload
access-list 1 permit 192.168.0.0 0.0.255.255
!
! Налаштування тунельного інтерфейсу mGRE
interface Tunnel0
 ip address 10.0.0.1 255.255.255.0  ! Приватна IP-адреса для тунелю
 no ip redirects
 ip nhrp authentication <Пароль NHRP>
 ip nhrp map multicast dynamic  ! Дозволяє динамічне відображення multicast
 ip nhrp network-id 100         ! Унікальний ідентифікатор DMVPN-мережі
 ip nhrp redirect              ! Увімкнення NHRP Redirect для Фази 3
 tunnel source GigabitEthernet0/0  ! Зовнішній інтерфейс Hub
 tunnel mode gre multipoint      ! Тип тунелю - multipoint GRE
 tunnel protection ipsec profile DMVPN_PROFILE  ! Застосування IPsec профілю
!
! Налаштування IPsec профілю
crypto isakmp policy 10
 encr aes 256                ! Шифрування
 authentication pre-share    ! Тип аутентифікації
 group 5                     ! Група Діффі-Хеллмана
crypto isakmp key <DMVPN_KEY> address 0.0.0.0 0.0.0.0 ! Попередньо узгоджений ключ для всіх Spoke
!
crypto ipsec transform-set TS_DMVPN esp-aes 256 esp-sha256-hmac
 mode tunnel
!
crypto ipsec profile DMVPN_PROFILE
 set transform-set TS_DMVPN
 set isakmp policy 10
!
! Налаштування EIGRP
router eigrp 1
 network 10.0.0.0 0.0.0.255   ! Мережа тунельного інтерфейсу
 network 192.168.1.0 0.0.0.255 ! Мережа внутрішнього інтерфейсу Hub
 no auto-summary
```

Налаштування периферійного маршрутизатора (Spoke - наприклад, Львів1), Spoke-маршрутизатор виступає як клієнт NHRP, який встановлює тунелі з Hub та іншими Spoke.

```
! Конфігурація інтерфейсу, підключеного до Інтернету (може бути DHCP)
interface GigabitEthernet0/0
 ip address dhcp              ! Або статична публічна IP-адреса
 ip nat outside
!
! Конфігурація внутрішнього інтерфейсу (VLANs будуть на ньому)
interface GigabitEthernet0/1
 no ip address
!
! Налаштування NAT (якщо Spoke має приватну публічну IP-адресу)
ip nat inside source list 1 interface GigabitEthernet0/0 overload
access-list 1 permit 10.0.0.0 0.0.0.255  ! Дозвіл для тунельної мережі
access-list 1 permit 192.168.10.0 0.0.0.255 ! Приклад локальної мережі філії
!
! Налаштування тунельного інтерфейсу mGRE
interface Tunnel0
 ip address 10.0.0.10 255.255.255.0  ! Приватна IP-адреса для тунелю (унікальна для кожного Spoke)
```

```
 no ip redirects
 ip nhrp authentication <Пароль NHRP>
 ip nhrp map 10.0.0.1 <Публічна IP-адреса Hub>  ! Статичне відображення Hub
 ip nhrp map multicast <Публічна IP-адреса Hub> ! Multicast через Hub
 ip nhrp network-id 100                         ! Повинен збігатися з Hub
 ip nhrp nhs 10.0.0.1                           ! Вказання IP-адреси NHS (Hub)
 tunnel source GigabitEthernet0/0               ! Зовнішній інтерфейс Spoke
 tunnel mode gre multipoint                     ! Тип тунелю - multipoint GRE
 tunnel protection ipsec profile DMVPN_PROFILE  ! Застосування IPsec профілю
!
! Налаштування IPsec профілю (аналогічно Hub)
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 5
crypto isakmp key <DMVPN_KEY> address <Публічна IP-адреса Hub> ! Ключ для Hub
crypto isakmp key <DMVPN_KEY> 0.0.0.0 0.0.0.0 ! Ключ для Spoke-to-Spoke, якщо не відомі адреси
!
crypto ipsec transform-set TS_DMVPN esp-aes 256 esp-sha256-hmac
 mode tunnel
!
crypto ipsec profile DMVPN_PROFILE
 set transform-set TS_DMVPN
 set isakmp policy 10
!
! Налаштування EIGRP
router eigrp 1
 network 10.0.0.0 0.0.0.255      ! Мережа тунельного інтерфейсу
 network 192.168.10.0 0.0.0.255  ! Приклад локальної мережі філії
 no auto-summary
!
```

Для забезпечення пріоритезації трафіку буде використана модель DiffServ з маркуванням DSCP. Налаштування QoS буде виконуватися на маршрутизаторах Hub та Spoke відповідно до Табл. 2.8.

Налаштування QoS включає наступні етапи:

- створення Class-map – визначення критеріїв для класифікації трафіку (наприклад, по портам, протоколам);
- Створення Policy-map – визначення дій для кожного класу трафіку (наприклад, маркування DSCP, встановлення пріоритету, обмеження смуги);
- застосування Service-policy – прив'язка policy-map до інтерфейсу (зазвичай на вихідному інтерфейсі, де можливе перевантаження).

Приклад конфігурації на Hub/Spoke маршрутизаторах:

```
! Класифікація трафіку
class-map match-all VOICE_TRAFFIC
 match ip dscp ef                  ! Для голосового трафіку
! Або можна класифікувати за портами:
! class-map match-all VOICE_TRAFFIC_NEW
!  match port udp 5060 (SIP)
!  match port udp range 10000 20000 (RTP, приклад)
!
class-map match-all ABS_TRAFFIC
```

```
 match ip dscp af41
!
class-map match-all UKM_TRAFFIC
 match ip dscp af31
!
class-map match-all FTP_MAIL_TRAFFIC
 match ip dscp af11
!
class-map match-all INTERNET_TRAFFIC
 match ip dscp default
!
! Створення policy-map
policy-map QOS_POLICY_OUT
 class VOICE_TRAFFIC
  priority percent 30            ! Виділення 30% смуги для голосового трафіку з пріоритетом
 class ABS_TRAFFIC
  bandwidth percent 20           ! Гарантована смуга 20%
 class UKM_TRAFFIC
  bandwidth percent 15           ! Гарантована смуга 15%
 class FTP_MAIL_TRAFFIC
  bandwidth percent 10           ! Гарантована смуга 10%
 class class-default             ! Весь інший трафік
  fair-queue                     ! Справедливе чергування
!
! Застосування policy-map до тунельного інтерфейсу (вихідний напрямок)
interface Tunnel0
 service-policy output QOS_POLICY_OUT
!
```

Налаштування VLAN на комутаторах доступу проведемо відповідно до табл. 2.7, порти будуть налаштовані в режимі «access» для відповідних VLAN або «trunk» для зв'язку з маршрутизатором.

```
! Приклад налаштування на комутаторі доступу
vlan 101
 name tel
vlan 102
 name vk
! ... та інші VLAN
!
interface GigabitEthernet0/1  ! Порт для IP-телефону та ПК
 switchport mode access
 switchport access vlan 105   ! Призначення VLAN для ПК
 switchport voice vlan 101    ! Призначення VLAN для IP-телефону (Cisco IP Phones)
!
interface GigabitEthernet0/2  ! Порт для касового терміналу
 switchport mode access
 switchport access vlan 103
!
interface GigabitEthernet0/24 ! Порт до маршрутизатора (trunk)
 switchport mode trunk
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 101-106
```

Маршрутизатор буде виконувати функцію DHCP-сервера для локальних мереж філій, проведемо відповідні налаштування:

```
! На Hub-маршрутизаторі
ip dhcp excluded-address 192.168.1.1 192.168.1.10 ! Виключення адрес
!
ip dhcp pool VLAN_101_TEL
 network 192.168.10.0 255.255.255.0 ! Приклад мережі для VLAN 101 у філії
 default-router 192.168.10.1      ! Шлюз за замовчуванням для цієї VLAN
```

```
 dns-server 8.8.8.8 8.8.4.4       ! DNS-сервери
 option 150 ip 192.168.1.1        ! Опція для IP-телефонів (TFTP-сервер для прошивки)
!
! ... аналогічні пули для інших VLAN
!
! На Spoke-маршрутизаторі (якщо DHCP-сервер знаходиться на Hub)
interface GigabitEthernet0/1.101
 ip address 192.168.10.1 255.255.255.0
 ip helper-address 192.168.1.1   ! IP-адреса DHCP-сервера на Hub
!
! ... аналогічні налаштування для інших sub-інтерфейсів VLAN
```

Для ефективної маршрутизації в рамках DMVPN та зв'язку із зовнішнім світом необхідно налаштувати протоколи динамічної маршрутизації.

EIGRP буде використовуватися для обміну маршрутами між Hub та Spoke, а також між самими Spoke після встановлення прямого тунелю.

```
! На Hub та Spoke маршрутизаторах (як було показано в 3.2.1 та 3.2.2)
router eigrp 1
 network 10.0.0.0 0.0.0.255   ! Тунельна мережа
 network <Локальна мережа Hub/Spoke> ! Приклад: 192.168.1.0 0.0.0.255
 no auto-summary
```

BGP буде налаштований на Hub-маршрутизаторі для взаємодії з Інтернет-провайдером.

```
! На Hub-маршрутизаторі (Київ1)
router bgp <Номер Автономної Системи>
 no synchronization
 bgp log-neighbor-changes
 neighbor <IP-адреса маршрутизатора провайдера> remote-as <Номер АС провайдера>
 neighbor <IP-адреса маршрутизатора провайдера> update-source GigabitEthernet0/0
 no auto-summary
!
address-family ipv4
 neighbor <IP-адреса маршрутизатора провайдера> activate
 network <Ваша публічна мережа> mask <Маска>  ! Анонсування вашої публічної мережі в Інтернет
 exit-address-family
```

Моделі налаштовані, можна переодити до дослідів.

3.3 Імітаційне моделювання роботи мережі

Першим критерієм що буде досліджуватись – надійність доставки. Цей параметр критично важливий для всіх мережевих сервісів і особливо для застосунків, які вимагають мінімальних втрат пакетів.

У моделі існуючої мережі (рис. 3.1), де використовується традиційна VPN-архітектура «зірка», надійність обміну даними між філіями повністю залежить від центрального маршрутизатора «Київ1». Цей маршрутизатор виконує функції VPN-сервера, через який йде весь міжфіліальний трафік. У разі виходу з ладу цього пристрою, можливість обміну між філіями стає неможливою, що є безперечним недоліком для безперебійного функціонування мережі. Це створює єдину точку відмови та потенційне "вузьке місце", що негативно впливає на загальну надійність.

На моделі реструктуризованої мережі (рис. 3.2) фізична топологія також візуально виглядає як «зірка», однак на логічному рівні, завдяки використанню технології DMVPN Фази 3, топологія мережі представлена як повнозв'язна (full mesh). Цей архітектурний підхід забезпечує наступні переваги для надійності доставки:

1. Динамічні Spoke-to-Spoke тунелі. Віртуальні канали між філіями створюються динамічно, відповідно до записів у таблицях маршрутизації маршрутизаторів. Це дозволяє організовувати VPN-тунелі які динамічно визначаються протоколом маршрутизації EIGRP.
2. Відмовостійкість. У випадку недоступності центрального вузла або перевантаження, трафік може перенаправлятися безпосередньо між філіями.
3. Оптимізація маршрутизації. EIGRP, в залежності від завантаженості каналів та метрик, може обирати найбільш оптимальний маршрут.
4. Вплив DSCP. Залежно від класу обслуговування, для різних типів пакетів обираються найоптимальніші маршрути та механізми обробки, що мінімізує їх втрати.

Якісним показником надійності доставки інформації є відсоток втрачених пакетів. Цей показник може коливатися залежно від інтенсивності навантаження на мережу. Програмний пакет Packet Tracer надає відповідні інструменти, що дозволяють генерувати пакети різного розміру, за різними

протоколами та напрямками. Крім величини пакету, існує можливість встановлювати такі параметри, як ToS (Type of Service), що відповідає флагу DSCP, TTL (Time To Live) (максимальний час життя), кількість відправлених пакетів або інтенсивність та адресу отримувача.

У табл.і 3.4 наведені результати роботи існуючої мережі при різних величинах навантаження для різних типів трафіку.

Таблиця 3.4 – Характеристики надійності доставки існуючої мережі

Тип пакетів	ToS	Навантаження, Ерл	Кількість відправлених пакетів	Кількість втрачених	%
FTP	0	0,5	7500	750	10
HTTP	0	0,3	4500	1350	30
POP3	0	0,05	750	37	4,94
SMTP	0	0,05	750	48	6,4
RTP	0	0,1	1500	97	6,47
Всього		1	15000	2282	15,22

Аналогічні дослідження проводились для модернізованої мережі при тих самих вихідних параметрах навантаження, але з відповідними DSCP-мітками, згідно з табл. 3.3. Результати моделювання наведені в таб. 3.5.

Таблиця 3.5 – Характеристики надійності доставки модернізованої мережі

Тип пакетів	ToS	Навантаження, Ерл	Кількість відправлених пакетів	Кількість втрачених	%
FTP	4	0,5	7500	12	0,16
HTTP	1	0,3	4500	97	2,16
POP3	2	0,05	750	14	1,87
SMTP	2	0,05	750	12	1,6
RTP	5	0,1	1500	0	0
Всього		1	15000	135	0,9

На рис. 3.3 наведено графічне відображення рівня втрат пакетів для обох моделей мережі, що дозволяє візуально порівняти їхню ефективність щодо надійності доставки.

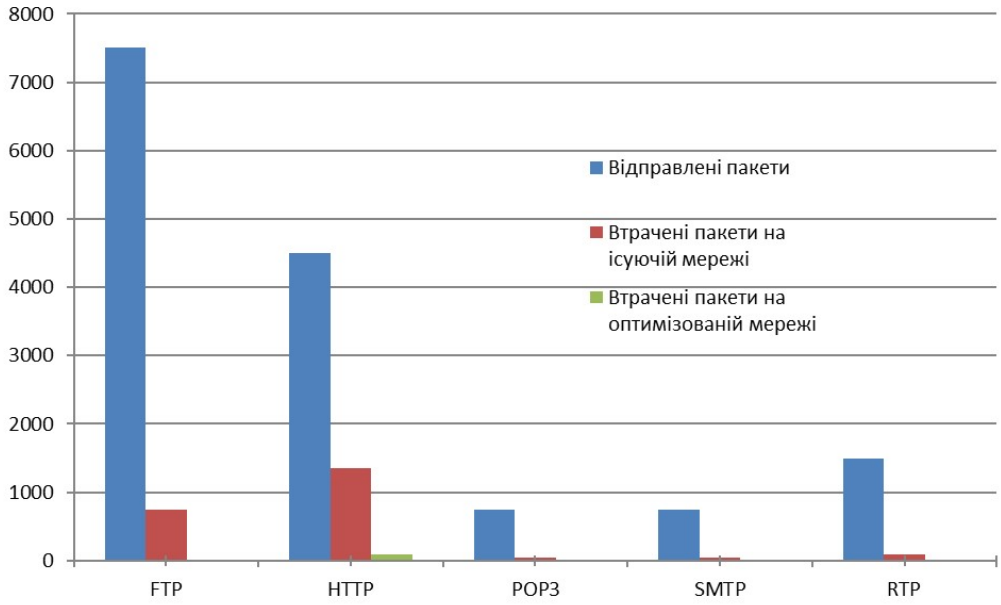

Рисунок 3.3 – Результати дослідження рівня втрат пакетів

Як видно з отриманих експериментальних даних, модернізована мережа демонструє значне покращення показників надійності доставки. Зокрема, для трафіку RTP (який відповідає за IP-телефонію та був відмічений найвищим пріоритетом DSCP 5), втрати пакетів вдалося повністю усунути (0%). Загальний відсоток втрат пакетів у реструктуризованій мережі скоротився з 15.22% до 0.90%, що свідчить про кардинальне підвищення стабільності та якості передачі даних.

Наступним етапом дослідження є вимірювання усередненого значення затримки при доставці пакетів. Генератори пакетів були налаштовані так само, як і в попередній серії досліджень. Для оцінки величини затримки використана спеціальна утиліта в Packet Tracer, що дозволяє за допомогою команди ping відправляти пакети не тільки за протоколом ICMP, а й за будь-яким підтримуваним програмним забезпеченням протоколом, фіксуючи мінімальний, максимальний та середній час відповіді.

Результати дослідження параметрів затримки для існуючої мережі зведені в табл. 3.6.

Таблиця 3.6 – Дослідження затримки на існуючій мережі

Тип пакетів	ToS	Навантаження, Ерл	Кількість відправлених пакетів	Затримка, мс		
				мін	макс	середня
FTP	0	0,5	7500	81	212	146,5
HTTP	0	0,3	4500	32	115	73,5
POP3	0	0,05	750	24	74	49
SMTP	0	0,05	750	18	89	53,5
RTP	0	0,1	1500	59	174	116,5

Аналогічні досліди проводились для модернізованої мережі при тих самих вихідних параметрах навантаження, але з активними механізмами DSCP. Результати дослідження наведені в табл. 3.7.

Таблиця 3.7 – Дослідження затримки на модернізованої мережі

Тип пакетів	ToS	Навантаження, Ерл	Кількість відправлених пакетів	Затримка, мс		
				мін	макс	середня
FTP	4	0,5	7500	5	38	21,5
HTTP	1	0,3	4500	12	84	48
POP3	2	0,05	750	7	44	25,5
SMTP	2	0,05	750	8	58	33
RTP	5	0,1	1500	2	29	15,5

Графічне відображення результатів дослідження величини затримки для обох моделей мережі наведено на рис. 3.4.

Виходячи з результатів, отриманих при дослідженні моделей існуючої та модернізованої мережі, на підставі табличного та графічного їх відображення, можна зробити наступні ключові висновок про покращення надійності доставки завдяки впровадженню DMVPN Фази 3, яка забезпечує логічну повнозв'язність та відмовостійкість, а також використанню DSCP для пріоритезації. Зменшення затримки для всіх типів трафіку.

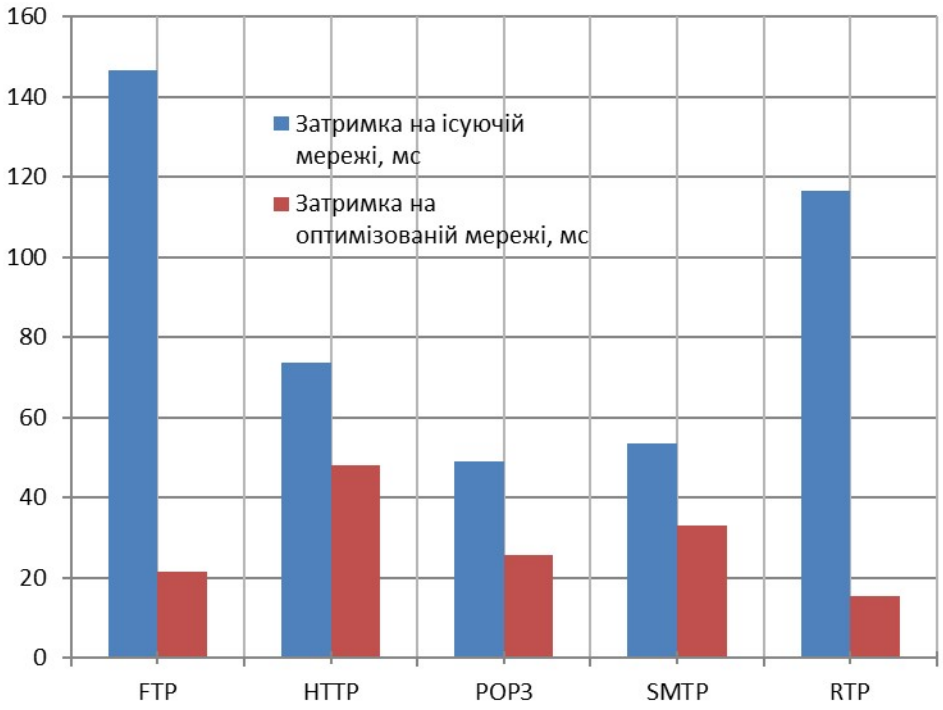

Рисунок 3.4 – Порівняння середньої затримки в існуючій та оптимізованій мережах

Результати імітаційного моделювання в Cisco Packet Tracer однозначно підтверджують правильність та ефективність прийнятих проєктних рішень. Модернізована мережа має значно кращі показники якості обслуговування (QoS), демонструючи менший відсоток втрат пакетів та значно меншу величину затримки при доставці пакетів. Це забезпечить стабільну та високопродуктивну роботу всіх корпоративних сервісів, включаючи IP-телефонію, та відповідатиме сучасним вимогам до мережевої інфраструктури.

Висновки за розділом 3

У третьому розділі випускної кваліфікаційної роботи було проведено імітаційне моделювання транспортного сегменту телекомунікаційної мережі компанії «Лідер Взуття» за двома сценаріями: існуюча мережа та модернізована мережа. Моделювання проводилося в програмному пакеті Cisco Packet Tracer,

який забезпечив необхідну точність емуляції мережевого обладнання та протоколів. Основним завданням було кількісне та якісне порівняння двох архітектур за ключовими показниками продуктивності мережі: надійністю доставки та затримкою.

На етапі підготовки моделювання було чітко визначено принципи розподілу адресного простору для віртуальних підмереж (VLAN), а також деталізовано політику DSCP, що мала застосовуватися в реструктуризованій мережі для пріоритезації трафіку. Для внутрішньої маршрутизації в обох моделях використовувався протокол EIGRP, що забезпечує швидку збіжність маршрутів.

Існуюча мережа продемонструвала недоліки в надійності доставки, обумовлені залежністю від центрального маршрутизатора як єдиної точки транзиту для міжфіліального трафіку. Загальний відсоток втрачених пакетів становив 15.22%, що є високим показником. Також моделювання показало високу затримки для всіх типів трафіку, оскільки весь трафік мусив проходити через центральний вузол. Середня затримка для RTP-трафіку сягала 116.5 мс, що негативно впливає на якість IP-телефонії.

Модернізована мережа, завдяки впровадженню DMVPN Фази 3 та механізмів DSCP, показала набагато кращі результати. Загальний відсоток втрат пакетів знизився до 0.90%. Середня затримка для RTP-трафіку скоротилася до 15.5 мс, що є відмінним показником для послуг реального часу. Це досягнуто завдяки прямим «spoke-to-spoke» з'єднанням DMVPN, які усувають необхідність транзиту через Hub, а також ефективному управлінню чергами та пріоритетами за допомогою DSCP.

Таким чином, результати імітаційного моделювання підтвердили ефективність та доцільність прийнятих проєктних рішень щодо реорганізації мережевої інфраструктури «Лідер Взуття». Впровадження технологій DMVPN Фази 3 та DSCP дозволить не лише підвищити надійність доставки та суттєво зменшити затримки, але й забезпечить необхідну масштабованість, відмовостійкість та якість обслуговування (QoS).

ВИСНОВКИ

Об'єктом дослідження цієї дипломної роботи є телекомунікаційна інфраструктура транспортного сегменту мережі магазинів взуття «Лідер Взуття», яка охоплює сім філій. Метою роботи стало підвищення ефективності, надійності та забезпечення високої якості обслуговування (QoS) для критично важливих бізнес-додатків, зокрема корпоративної IP-телефонії, шляхом модернізації цієї мережі.

У першому розділі, було проведено аналіз поточної телекомунікаційної інфраструктури. Встановлено, що мережа побудована за ієрархічною топологією «зірка», де головний офіс у Києві виступає центральним вузлом, а міжфілійний зв'язок реалізується через VPN-тунелі в публічній мережі Інтернет. Детальне дослідження архітектури та функціоналу ключових мережевих пристроїв дозволило виявити потенційні «вузькі місця». Експериментальний аналіз завантаженості каналів зв'язку, виконаний за допомогою інструментів Mikrotik Port Mirroring, MRTG та Wireshark, виявив пікові навантаження, пов'язані з бізнес-процесами. Розрахунок додаткового навантаження від впровадження корпоративної IP-телефонії (приблизно 0.44 Мбіт/с) підтвердив необхідність модернізації. Було обґрунтовано, що існуюча інфраструктура, попри загальну функціональність, потребує оновлення для врахування майбутніх сервісів та підвищення загальної надійності, ефективності й масштабованості.

У другому розділі було проведено обґрунтування вибору технологічних рішень для усунення виявлених недоліків, таких як обмежена масштабованість, недостатня відмовостійкість та незадовільна якість обслуговування (QoS) для чутливих до затримок додатків. На основі порівняльного аналізу різних VPN-топологій та механізмів QoS, було обґрунтовано вибір технології Dynamic Multipoint VPN (DMVPN) Фази 3 у поєднанні з механізмом DSCP (DiffServ Code Point). DMVPN Фази 3 була обрана за її здатність створювати логічно повнозв'язну мережу з динамічним встановленням прямих «spoke-to-spoke»

тунелів, що дозволяє уникнути транзиту всього міжфіліального трафіку через центральний вузол, значно скорочуючи затримки та оптимізуючи маршрутизацію. Інтеграція DSCP забезпечує необхідний рівень якості обслуговування шляхом пріоритезації критичного трафіку.

Третій розділ присвячений практичній реалізації та імітаційному моделюванню запропонованих рішень за допомогою програмного пакету Cisco Packet Tracer. Було розроблено дві моделі – існуюча та модернізована – для порівняльного аналізу ключових показників продуктивності: надійності доставки (відсоток втрачених пакетів) та затримки. Результати моделювання підтвердили ефективність модернізації:

- надійність доставки в реструктуризованій мережі зросла, загальний відсоток втрачених пакетів знизився з 15.22% до 0.90%;
- затримка зменшилася, середня затримка для RTP-трафіку скоротилася зі 116.5 мс до 15.5 мс.

Отримані результати свідчать, що запропоновані проєктні рішення, засновані на технологіях DMVPN Фази 3 та DSCP, дозволяють створити гнучку, безпечну, відмовостійку та високопродуктивну транспортну мережу. Ця модернізація забезпечить компанії «Лідер Взуття» не лише значне підвищення надійності доставки та зменшення затримок, але й гарантуватиме високу якість обслуговування (QoS) для всіх корпоративних сервісів, підтримуючи подальший розвиток бізнесу та його адаптацію до сучасних телекомунікаційних вимог.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Беркман Л.В., Стрілець В.М. Комп'ютерні мережі та телекомунікації: теорія та практика : навчальний посібник. Київ : Центр учбової літератури, 2018. 320 с.

2. SIP: Session Initiation Protocol. RFC 3261. The Internet Society, 2002. [Електронний ресурс]. – Режим доступу: https://datatracker.ietf.org/doc/html/rfc3261

3. Нагірний Ю.М., Приймак О.С. Управління трафіком у телекомунікаційних мережах : навчальний посібник. Київ : КПІ ім. Ігоря Сікорського, 2018. 200 с.

4. Shelton D., Al-Shamma A. Cisco QOS Exam Certification Guide (CCIE Self-Study). Indianapolis, IN : Cisco Press, 2017. 720 p.

5. Коваленко В.В., Левченко О.В. Захист інформації в комп'ютерних мережах : навчальний посібник. Київ : НАУ, 2020. 270 с.

6. Tetz M. Cisco Express Forwarding. Indianapolis, IN : Cisco Press, 2019. 384 p.

7. Остапов С.Е. Проектування корпоративних мереж : навчальний посібник. Одеса : ОНАС ім. О.С. Попова, 2017. 310 с.

8. Kim M. Cisco CCNA Routing and Switching Official Cert Guide Library. Indianapolis, IN : Cisco Press, 2014.

9. Янко М.О., Бондаренко О.В. IP-телефонія та її інтеграція в корпоративні мережі : навчальний посібник. Київ : Основа, 2021. 230 с.

10. Harkins D., Orans D. IPsec: The Complete Guide to Protocols, Implementation, and Design. Boston, MA : Addison-Wesley Professional, 2009. 840 p.

11. Шишков В.М. та ін. Безпека інформаційних та кіберфізичних систем : монографія. Харків : ХНУРЕ, 2020. 415 с.

12. Cisco IOS Master Command List, All Releases. Cisco Documentation, 2023. [Електронний ресурс]. – Режим доступу:

https://www.cisco.com/c/en/us/td/docs/ios/mcl/all/mcl_all_book.html

13. Загірняк М.В., Барабаш В.В., Верескун С.М. Телекомунікаційні та інформаційні мережі : навчальний посібник. Харків : ХНУРЕ, 2019. 280 с.

14. Moyer S., Collier M. DMVPN: Secure, Scalable, and Flexible VPNs. Indianapolis, IN : Cisco Press, 2015. 480 p.

15. Кухарчук А.О., Дорожовець М.М. Сучасні технології комп'ютерних мереж : навчальний посібник. Вінниця : ВНТУ, 2017. 256 с.

16. Lammle T. CCNA Routing and Switching Study Guide. 7th ed. Indianapolis, IN : Wiley, 2020. 960 p.

17. Ткачук А.В., Мельник Р.В. Комп'ютерні мережі: Протоколи, архітектури, технології. Чернівці : Чернівецький національний університет, 2019. 340 с.

18. Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers. RFC 2474. The Internet Society, 1998. [Електронний ресурс]. – Режим доступу: https://datatracker.ietf.org/doc/html/rfc2474

19. Мельник В.І., Павловський В.Г. Основи побудови корпоративних комп'ютерних мереж : навчальний посібник. Львів : Видавництво Львівської політехніки, 2016. 295 с.

20. Awduche A. et al. Requirements for Traffic Engineering Over MPLS. RFC 2702. The Internet Society, 2000. [Електронний ресурс]. – Режим доступу: https://datatracker.ietf.org/doc/html/rfc2702

ДОДАТОК А – Охорона праці

А.1 Характеристика умов праці

Діяльність працівників відділу:

– моніторинг активного обладнання мережі, виявлення відмов та аварійних ситуацій на обладнанні;

– оповіщення відповідних підрозділів про виникаючі аварії;

– аналіз виникаючих аварій;

– організація оперативних дій по усуненню аварій, координація роботи технічних служб;

– підтримка актуального статусу аварії;

– контроль та координація дій операторів;

– формування звітів.

Відділ моніторингу мережі розташовується на першому поверху будівлі в приміщенні з установленою технікою згідно з СНиП II-90-81 «Виробничі будівлі промислових підприємств», загальна площа приміщення становить 30 м² (7,5х4м, висота 3 м), а загальний обсяг – 90 м³.

А.2 Заходи з охорони праці

А.2.1 Планування розташування робочих місць телекомунікаційного підрозділу

На сьогоднішній день в приміщенні телекомунікаційного відділу робочі місця розташовані в відповідності до наведеної схеми на рисунку А.1.

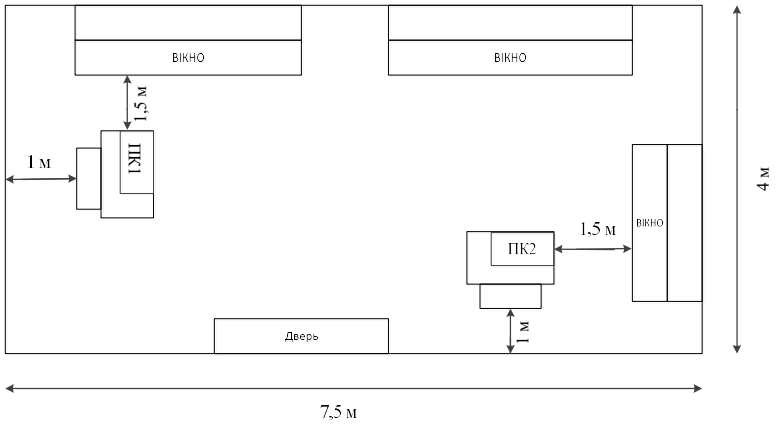

Рисунок А.1 – Розташування робочих місць відділу моніторингу згідно з ГОСТ

Облаштованість робочих місць відповідає вимогам санітарних норм та в приміщенні площею 30 м² та об’ємом 90 м³ можна розташовувати два робочих місць з ПК.

А.2.2 Розрахунок освітленості

Розрахунок проводиться для кімнати площею 30 м², довжина якої 7,5 м, ширина 4 м, висота 3 м. В якості джерела освітлення використовуються люмінесцентні лампи. Приміщення має світлу побілку: коефіцієнт відбиття стелі Рп = 70%, стін Рс=50%. Висота робочих поверхонь столів $h_р$ = 0,7 м. Для освітлення приймаємо світильники типу ЛБ40-1, які підвішуються до стелі $h_с$=0,35 м.

Визначимо висоту підвісів світильників над підлогою:

$$h_в = H - h_с = 3 - 0,32 = 2,68 \text{ м} \quad (А.1)$$

Визначаємо висоту підвісу світильника над робочою поверхнею:

$$h = h_в - h_р = 2,68 - 0,7 = 1,98 \text{ м} \quad (А.2)$$

Визначаємо рекомендовану відстань між світильниками:

$$L = 0{,}7 \times H = 0{,}7 \times 3 = 2{,}1 \text{ м} \quad \text{(А.3)}$$

Розрахуємо необхідну кількість світильників:

$$N = \frac{A \times B}{L^2} = \frac{4 \times 7{,}5}{2{,}1^2} = 6{,}8 \approx 7 \text{ шт.} \quad \text{(А.4)}$$

Приймаємо 7 світильників (за розрахунками не менше 7), враховуючи розміри приміщення розміщуємо їх у два ряди по 3 та 4 штуки відповідно.

Для визначення кількості світильників визначимо світловий потік, який падає на поверхню, за формулою:

$$F = \frac{E \times K \times S \times Z}{N \times n \times \eta}, \quad \text{(А.5)}$$

де F – потік, який потрібно розрахувати, Лм;

E – нормативна мінімальна освітленість, Лк (визначається за таблицею), у даному випадку E = 400 Лк

K – коефіцієнт запасу, що враховує зменшення світового потоку лампи в результаті забруднення світильників у процесі експлуатації (його значення залежить від типу приміщень та характеру робіт, що в ньому проводяться. У нашому випадку K=1,5).

S – площа приміщення, що освітлюється (S = 30 м²).

Z – відношення середньої освітленості до мінімальної (зазвичай дорівнює 1,1…1,2, для люмінесцентних ламп Z = 1,1).

N – кількість світильників;

n – кількість ламп у світильнику;

η – коефіцієнт використання (виражається відношенням світового потоку, який падає на поверхню, до сумарного потоку всіх ламп та розраховується у

долях одиниць, залежить від характеристик світильника, розмірів приміщення, забарвлення стін та стелі, які характеризуються коефіцієнтами відбиття від стін (Рс) та стелі (Рп)), значення коефіцієнтів Рс та Рп: 50% та 70% відповідно.

Значення n визначимо за таблицею коефіцієнтів використання різних світильників. Для цього розрахуємо індекс приміщення за формулою:

$$I = \frac{S}{h \times (A+B)}, \quad \text{(А.6)}$$

де:

S – площа приміщення

h – висота підвісу

A – ширина приміщення

B – довжина приміщення

Підставимо значення:

$$I = \frac{30}{2{,}68 \times (4+7{,}5)} = 0{,}97$$

Знаючи індекс приміщення I, визначаємо η =0,42.

Використовуємо світильник типу ОД, кожний з них комплектується двома лампами:

$$F = \frac{400 \times 1{,}5 \times 30 \times 1{,}1}{2 \times 8 \times 0{,}42} = 2946 \text{ лм}$$

Загальна електрична потужність усіх світильників становить:

$\sum P_{св}$ = P×N = 2×40×7=560 Вт

А.2.3 Мікроклімат робочого місця

Витрату повітря в приміщенні з додатковим тепловиділенням визначається

за формулою:

$$L = \frac{Q_{над}}{c \cdot \rho \cdot (t_в - t_н)}, м^3/год \quad (А.7)$$

де $Q_{над}$ – надлишкове виділення тепла в робочому приміщенні, ккал/год.;

с – теплоємність повітря (0,237 ккал/кг);

р – обсягова вага повітря (1,226 кг/м³);

$t_в$ – температура витяжного повітря (30ºС);

$t_н$ – температура повітря, що подається (20ºС);

Розрахуємо надлишкове надходження тепла по формулі:

$$Q_{над} = Q_{уст} + Q_{пер} + Q_{осв} + Q_{ср}, \quad (А.8)$$

де $Q_{уст}$ - виділення тепла від устаткування;

$Q_{пер}$ – виділення тепла робітниками;

$Q_{осв}$ – надходження тепла від електричного освітлення;

$Q_{ср}$ – надходження тепла від сонячної радіації через вікна.

Визначимо виділення тепла від устаткування за формулою:

$$Q_{уст} = P \times K_а \times K_б \times 860 \quad (А.9)$$

Р – сумарна потужність устаткування, кВт/год.;

$К_а$ – коефіцієнт установленої потужності (0,95);

$К_б$ – коефіцієнт одночасної роботи (1,0).

$$Q_{уст} = [(x_1 \cdot k_1) + (x_2 \cdot k_2) + (x_3 \cdot k_3) + (x_4 \cdot k_4)] \cdot K_а \cdot K_б \cdot 860 \quad (А.10)$$

Розрахуємо:

$$Q_{уст} = [(6 \cdot 0{,}5) + (6 \cdot 0{,}1) + (1 \cdot 0{,}4) + (1 \cdot 6{,}3)] \cdot 0{,}95 \cdot 1 \cdot 860 = 3268 \quad ккал/год.$$

Визначимо виділення тепла від обслуговуючого персоналу за допомогою формули:

$$Q_{пер} = n \times g \qquad (А.11)$$

n - кількість працюючих;

g - кількість тепла, що виділяє один працівник за годину (100 ккал/год.)

Розрахуємо:

$Q_{пер}$ = 2 х 100 = 200 ккал/год.

Визначимо надходження тепла від електричного освітлення за допомогою формули:

$$Q_{осв} = E_м \cdot g_1 \cdot S \qquad (А.12)$$

$E_м$ - нормована освітленість, для цієї зорової роботи приймаємо рівною 400 лк;

g_1 - питоме тепловиділення на 1 м^2 підлоги при 1 лк освітленості (для люмінесцентних ламп - 0,05 ккал/год.).

S - площа приміщення, м^2.

$$Q_{осв} = 400 \cdot 0{,}05 \cdot 30 = 600 ккал/год.$$

Визначимо надходження тепла від сонячної радіації через вікна за допомогою формули:

$$Q_{ср} = F \cdot g_2 \cdot K_{осл}, \qquad (А.13)$$

де F - площа віконних прорізів (1,55 м^2).

g_2 - кількість тепла, що надходить через 1 м^2 віконного прорізу

(65 ккал/год.).

$К_{осл}$ - коефіцієнт ослаблення, приймаємо - 0,4.

Розрахуємо:

$Q_{ср}$=1,55·65·0,4 = 40,3 ккал/год.

Визначимо кількість надлишкового тепла:

$Q_{над}$= 3268 + 200 + 600 + 40,3 = 4108,3 ккал/год.

Визначимо витрати повітря в приміщенні:

$$L = \frac{4108,3}{0,237 \cdot 1,226 \cdot (30 - 20)} = 1414 м^3 / год$$

Існуюча в наявності система кондиціонування FrostMaster Inc 2 має продуктивність 2000 куб. м./годину, що задовольняє необхідним нормативам.

Параметри мікроклімату на робочих місцях регламентуються ДСН 3.3.4.042-99 «Санітарні норми мікроклімату виробничих приміщень», що цілком відповідають фактичним даним приміщення відділу моніторингу.

А.2.4 Пожежна безпека

У приміщенні телекомунікаційного підрозділу розроблені заходи для забезпечення пожежної безпеки, що визначає Інструкція про заходи пожежної безпеки для службових приміщень. В інструкції про засоби пожежної безпеки для службових приміщень забороняється:

– улаштовувати тимчасові електромережі, застосовувати саморобні плавкі вставки в запобіжниках, прокладати електричні проводи безпосередньо по пальній основі, експлуатувати світильники зі знятими ковпаками (розсіювачами), використовувати саморобні подовжувачі, що не відповідають вимогам Правил пристрою електроустановок;

– пристосовувати вимикачі, штепсельні розетки для підвішування одягу й інших предметів, обгортати електролампи і світильники, заклеювати ділянки електромережі пальною тканиною, папером;

– використовувати побутові електрокип'ятильники, чайники тощо без незаймистих підставок, залишати без нагляду включеними в електромережу кондиціонери, комп'ютери, рахункові і друкарські машинки і т.п.;

– захаращувати підступи до засобів пожежогасіння, використовувати пожежні крани, рукави і пожежний інвентар не по призначенню, зберігати документи, різні матеріали, предмети й інвентар у шафах (нішах) інженерних комунікацій;

– курити (крім спеціально відведених для цього адміністрацією місць, позначених написом «Місце для паління» і забезпечених урною чи попільницею з матеріалу, що не горить), проводити зварювальні й інші вогневі роботи без оформлення відповідного дозволу, застосовувати легкозаймисті рідини.

По закінченню роботи необхідно:

– оглянути приміщення, переконатися у відсутності порушень, що можуть спричинити пожежу;

– відключити освітлення, електроживлення приладів і устаткування.

Електромережі, електроприлади і апаратуру необхідно експлуатувати тільки у справному стані. У випадку виявлення ушкоджень електромереж, вимикачів, розеток ті інших електровиробів варто негайно відключити їх і вжити необхідних заходів до приведення їх в пожежобезпечний стан.

А.3 Висновки

У даному розділі розроблено заходи щодо облаштування робочого місця оператора телекомунікаційного підрозділу та приміщення взагалі. Було наведено розрахунки освітленості, рівня шуму та мікроклімату. Розраховані величини задовольняють всі вимоги згідно з санітарними правилами та нормами:

– світловий потік F = 2946 Лм, тому використовуємо 7 світильників;

– витрати повітря в приміщенні L =1414 м³/год.

ДОДАТОК Б – Результати експериментального дослідження каналів зв’язку

Фрагмент результатів роботи сніфера:

```
23/04/2025  09:39:24.855341 10.0.0.138.4340 >
10.0.0.197.3128: S [tcp sum ok] 3298328004:3298328004(0) win
65535 <mss 1460,nop,nop,sackOK> (DF) (ttl 128, id 43021, len
48)
23/04/2025  09:39:24.855396 10.0.0.197.3128 >
10.0.0.138.4340: S [tcp sum ok] 1775499054:1775499054(0) ack
3298328005 win 5840 <mss 1460,nop,nop,sackOK> (DF) (ttl 64,
id 0, len 48)
23/04/2025  09:39:24.855567 10.0.0.138.4340 >
10.0.0.197.3128: . [tcp sum ok] 1:1(0) ack 1 win 65535 (DF)
(ttl 128, id 43023, len 40)
23/04/2025  09:39:24.885077 10.0.0.138.4340 >
10.0.0.197.3128: P 1:667(666) ack 1 win 65535 (DF) (ttl 128,
id 43024, len 706)
23/04/2025  09:39:24.885117 10.0.0.197.3128 >
10.0.0.138.4340: . [tcp sum ok] 1:1(0) ack 667 win 6660 (DF)
(ttl 64, id 39666, len 40)
23/04/2025  09:39:24.885669 10.96.16.197.41000 >
194.44.183.202.3128: S [tcp sum ok] 1764270339:1764270339 (0)
win 5840 <mss 1460,sackOK,timestamp 239693280 0,nop,wscale 0>
(DF) (ttl 64, id 52451, len 60)
23/04/2025  09:39:24.886516 10.0.0.197.3128 >
10.0.0.138.4340: . 1:1461(1460) ack 667 win 6660 (DF) (ttl
64, id 39667, len 1500)
23/04/2025  09:39:24.886548 10.0.0.197.3128 >
10.0.0.138.4340: P 1461:1656(195) ack 667 win 6660 (DF) (ttl
64, id 39668, len 235)
23/04/2025  09:39:24.887001 10.0.0.138.4340 >
10.0.0.197.3128: . [tcp sum ok] 667:667(0) ack 1656 win 65535
(DF) (ttl 128, id 43025, len 40)
23/04/2025  09:39:25.457499 10.0.0.138.4340 >
10.0.0.197.3128: P 667:1333(666) ack 1656 win 65535 (DF) (ttl
128, id 43032, len 706)
23/04/2025  09:39:25.458575 10.0.0.197.3128 >
10.0.0.138.4340: . 1656:3116(1460) ack 1333 win 7992 (DF)
(ttl 64, id 39669, len 1500)
23/04/2025  09:39:25.458605 10.0.0.197.3128 >
10.0.0.138.4340: P 3116:3311(195) ack 1333 win 7992 (DF) (ttl
64, id 39670, len 235)
23/04/2025  09:39:25.459081 10.0.0.138.4340 >
10.0.0.197.3128: . [tcp sum ok] 1333:1333(0) ack 3311 win
65535 (DF) (ttl 128, id 43033, len 40)
23/04/2025  09:39:25.658750 10.0.0.138.4340 >
10.0.0.197.3128: P 1333:1999(666) ack 3311 win 65535 (DF)
(ttl 128, id 43038, len 706)
```

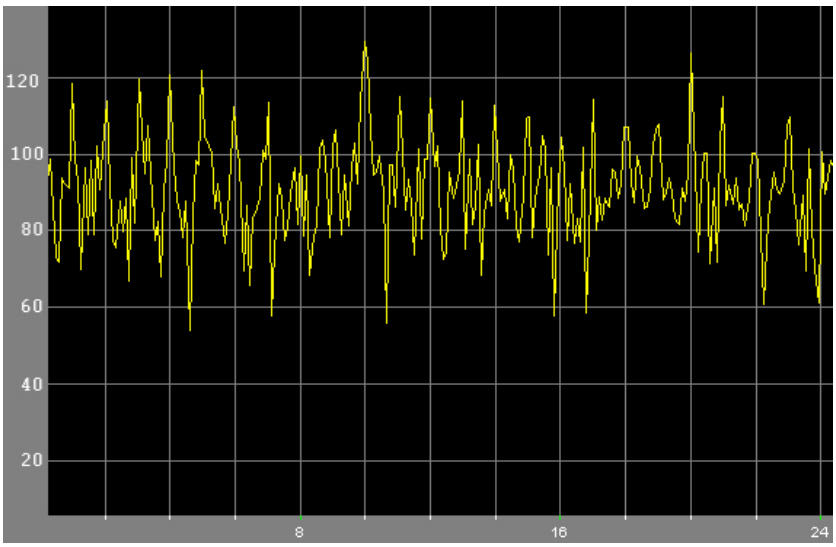

Рисунок Б.1 – Характеристика завантаженості канала Київ 1 – Інтернет

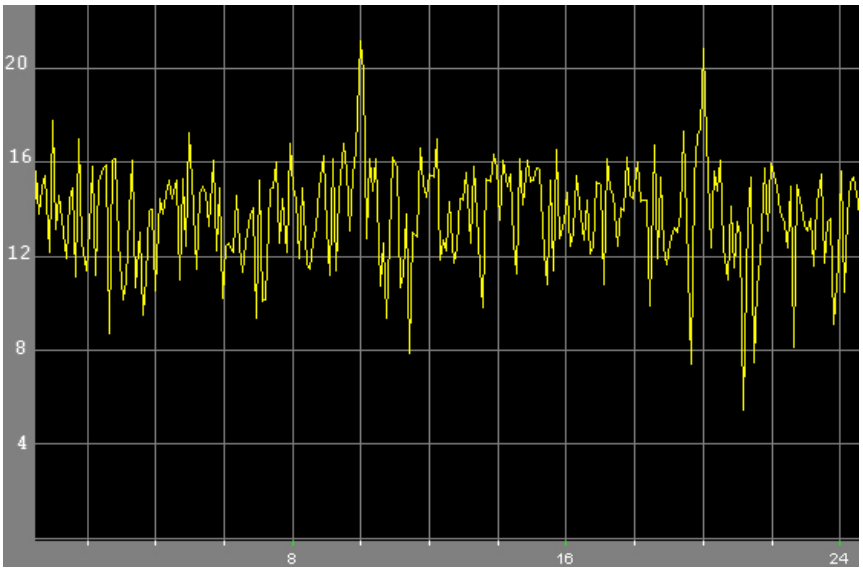

Рисунок Б.2 – Характеристика завантаженості каналу Київ 1 – Київ 2

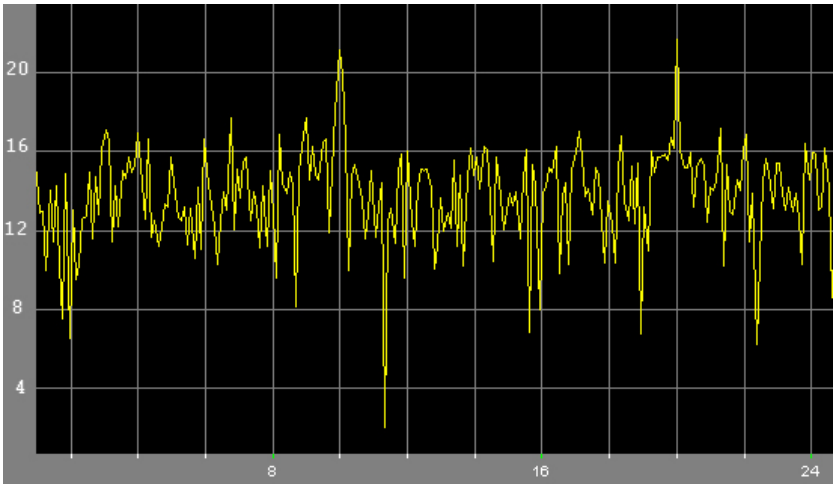

Рисунок Б.3 – Характеристика завантаженості каналу Київ 1 – Бровари

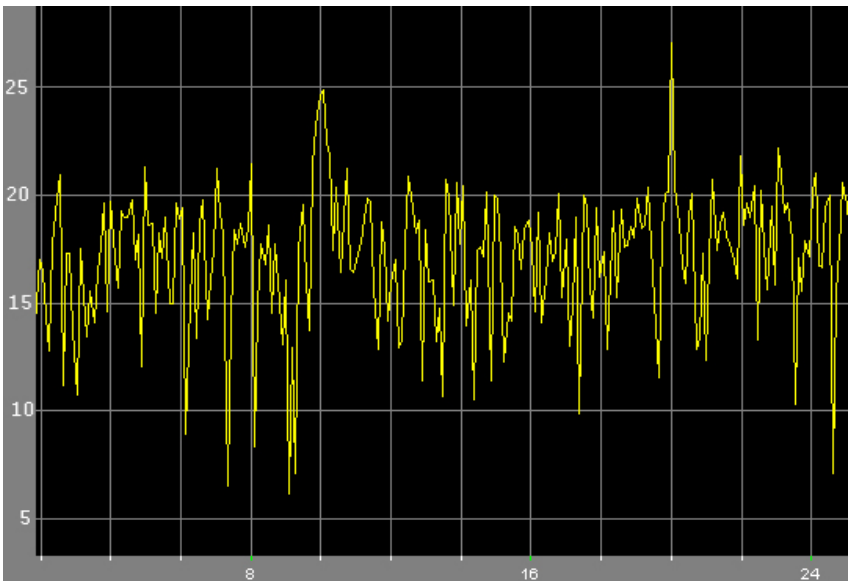

Рисунок Б.4 – Характеристика завантаженості каналу Київ 1 – Житомир

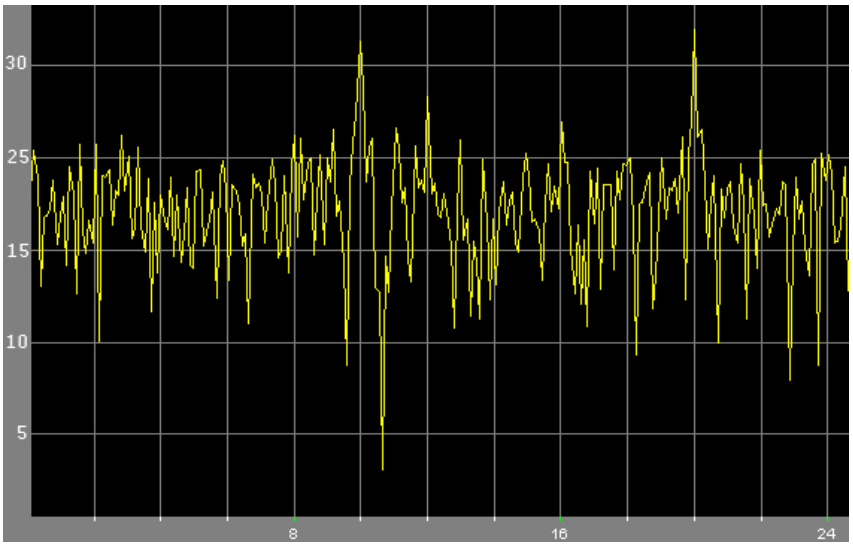

Рисунок Б.5 – Характеристика завантаженості каналу Київ 1 – Дніпро

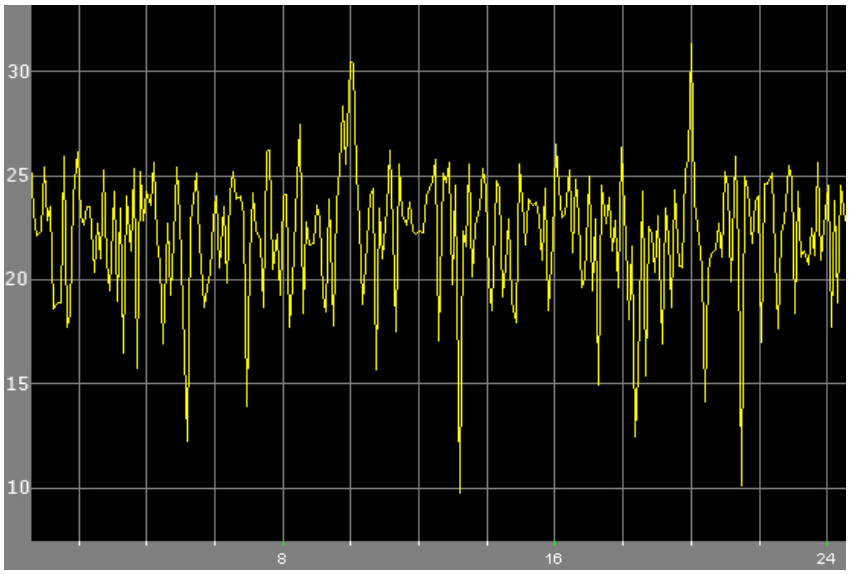

Рисунок Б.6 – Характеристика завантаженості каналу Київ 1 – Харків

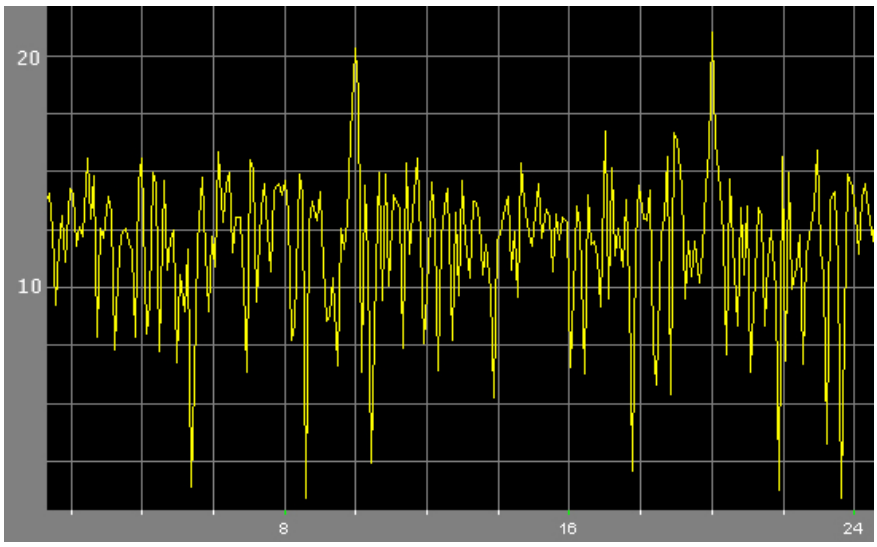

Рисунок Б.7 – Характеристика завантаженості каналу Київ 1 – Херсон

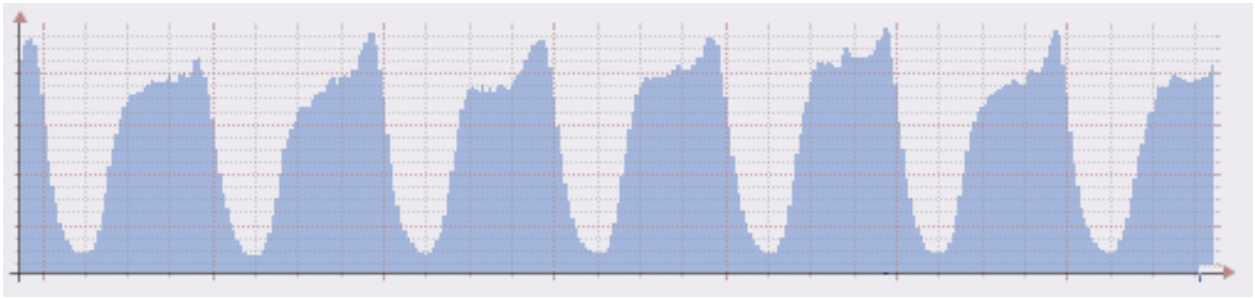

Рисунок Б.8 – Тижнева характерстика завантаженості каналу Київ 1 – Інтернет