НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Навчально-науковий Інститут телекомунікаційних систем

Кафедра електронних комунікацій та інтернету речей

«До захисту допущено»
ВО завідувача кафедри
_____ В'ячеслав НОСКОВ
«___»_____2025 р.

Дипломна робота

на здобуття ступеня бакалавра

зі спеціальності 172 Телекомунікації та радіотехніка

на тему: «Побудова корпоративної мультисервісної мережі з використання технології IP/MPLS»

Виконав:
Студент IV курсу, групи ТС-12
Соколов Олександр Іванович _____

Керівник:
Професор кафедри електронних комунікацій
та інтернету речей, д.т.н., проф. Мошинська А.В. _____

Рецензент:
Доцент кафедри інформаційних технологій в
телекомунікаціях, к.т.н., доц. Новогрудська Р.Л. _____

Засвідчую, що у цій дипломній роботі
немає запозичень з праць інших авторів
без відповідних посилань.
Студент _____

Київ – 2025 року

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Навчально-науковий Інститут телекомунікаційних систем
Кафедра електронних комунікацій та інтернету речей

Рівень вищої освіти – перший (бакалаврський)

Спеціальність – 172 Телекомунікації та радіотехніка

Освітня програма – «Системи електронних комунікацій та інтернету речей»

ЗАТВЕРДЖУЮ
ВО завідувача кафедри
_____ В’ячеслав НОСКОВ
«___»_____2025 р.

ЗАВДАННЯ

на дипломну роботу студенту

Соколову Олександру Івановичу

1. Тема роботи «Побудова корпоративної мультисервісної мережі з використання технології IP/MPLS.», керівник роботи Мошинська Аліна Валентинівна, професор, д.т.н, проф. затверджені наказом по університету від «26» травня 2025 р. № 1755 –с.

2. Термін подання студентом роботи 10 червня 2025 року

3. Вихідні дані до роботи матеріали статей та наукових видань, інформаціні ресурси мережі Інтернет, навчально-методичні матеріали. Структурований план порядку розробки матеріалів дипломної роботи.

4. Зміст роботи Обґрунтувати актуальність теми. Розглянути сучасні підходи до побудови корпоративних мультисервісних мереж. Проаналізувати архітектуру IP/MPLS, принципи її функціонування та переваги у порівнянні з традиційними IP-технологіями. Визначити технічні вимоги до корпоративної мережі. Розробити логічну структуру мережі з урахуванням розмежування зон доступу, агрегації та ядра. Підібрати протоколи маршрутизації та механізми захисту (OSPF, BGP, VPN, VRF, QoS). Створити модель мережі у середовищі GNS3. Провести налаштування маршрутизаторів та перевірку взаємодії між сегментами.

Провести тестування працездатності мережі. Надати рекомендації щодо впровадження розробленої мережі в умовах підприємства.

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо): 1) Тема та мета дипломної роботи; 2) Загальна схема корпоративної мережі з використанням IP/MPLS; 3) Принцип роботи комутації міток у мережі MPLS; 4) Логічна структура мережі з поділом на зони (доступ, агрегація, ядро); 5) Порівняння традиційної IP-мережі та IP/MPLS; 6) Топологія та приклад конфігурації BGP і OSPF; 7) Використання QoS, VPN і VRF у корпоративному середовищі; 8) Рекомендації щодо розгортання та масштабування мережі; 9) Висновки за результатами виконання роботи.

6. Дата видачі завдання 22.01.2025 рік

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів роботи	Примітка
1	Теоретичн основи розробки корпоративних мереж з технологіями IP/MPLS	1.03.2025	Виконано
2	Проектування корпоративної мультисервісної мережі з використанням IP/MPLS	15.04.2025	Виконано
3	Впровадження, експлуатація та забезпечення безпеки мережі	15.05.2025	Виконано
4	Оформлення роботи	5.06.2025	Виконано

Студент Олександр СОКОЛОВ

Керівник роботи Аліна МОШИНСЬКА

РЕФЕРАТ

Текстова частина дипломної роботи: 63 с., 10 рис., 39 джерел.

Мета роботи – дослідження теоретичних основ і практичне впровадження корпоративної мультисервісної мережі з використанням технології IP/MPLS, що забезпечує ефективну, масштабовану, безпечну та надійну передачу різних типів трафіку – даних, голосу та відео.

У дипломній роботі розкрито поняття корпоративної мережі, її роль у сучасному бізнес-середовищі, проведено аналіз топологій, типів мереж та їх функціональних характеристик. Основну увагу приділено принципам роботи технології IP/MPLS, її порівнянню з традиційними IP-мережами, перевагам впровадження в корпоративному середовищі, таким як підтримка QoS, масштабованість, гнучкість та відмовостійкість.

На основі аналізу потреб організації розроблено архітектуру мультисервісної мережі з логічним поділом на рівні доступу, агрегації та ядра. Обґрунтовано вибір обладнання та протоколів маршрутизації (OSPF, BGP), а також реалізацію сервісів VPN, VLAN та VRF. Практична частина передбачає побудову моделі мережі в GNS3 із впровадженням MPLS, налаштуванням внутрішньої та зовнішньої маршрутизації, забезпеченням пріоритету трафіку та конфігурацією безпечного доступу.

Налаштовану мережу протестовано в умовах моделювання реальних бізнес-сценаріїв: відеоконференцій, віддаленого доступу, обміну файлами та резервного копіювання. Показано, що запропоноване рішення повністю відповідає функціональним і нефункціональним вимогам, забезпечує надійність, продуктивність і можливість подальшого розширення.

Ключові слова: IP/MPLS, протокол BGP, протокол OSPF, QoS, VPN, VLAN, VRF, маршрутизація, корпоративна мережа, мультисервісність.

ABSTRACT

Thesis content: 63 pages, 10 figures, 39 references.

The aim of the thesis is to study the theoretical foundations and practical implementation of a corporate multiservice network using IP/MPLS technology, which ensures efficient, scalable, secure, and reliable transmission of various types of traffic — data, voice, and video.

The thesis examines the concept of a corporate network, its role in the modern business environment, and provides an analysis of network topologies, types, and functional characteristics. Special attention is given to the principles of operation of IP/MPLS technology, its comparison with traditional IP networks, and the advantages of its implementation in a corporate setting, such as QoS support, scalability, flexibility, and fault tolerance.

Based on the analysis of the organization's needs, the architecture of a multiservice network was developed, with logical separation into access, aggregation, and core levels. The selection of equipment and routing protocols (OSPF, BGP) was justified, along with the implementation of VPN, VLAN, and VRF services. The practical part involves building a network model in GNS3 with MPLS deployment, configuration of internal and external routing, traffic prioritization, and secure access setup.

The configured network was tested in simulated real-world business scenarios: video conferencing, remote access, file exchange, and data backup. The results demonstrate that the proposed solution fully meets both functional and non-functional requirements, providing reliability, performance, and potential for future expansion.

Keywords: IP/MPLS, BGP protocol, OSPF protocol, QoS, VPN, VLAN, VRF, routing, corporate network, multiservice.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, СКОРОЧЕНЬ І ТЕРМІНІВ

BGP – Border Gateway Protocol – протокол граничного шлюзу, використовується для обміну маршрутною інформацією між автономними системами.

CE – Customer Edge – граничний маршрутизатор на стороні клієнта.

LDP – Label Distribution Protocol – протокол розподілу міток у мережі MPLS.

LSP – Label Switched Path – попередньо заданий шлях у мережі MPLS для передачі пакетів за мітками.

LSR – Label Switching Router – маршрутизатор з підтримкою MPLS, який виконує комутацію міток.

MPLS – MultiProtocol Label Switching – технологія комутації міток для підвищення швидкості та ефективності маршрутизації.

NGN – Next Generation Network – мережа нового покоління, яка об'єднує різні типи трафіку в єдиній інфраструктурі.

OSPF – Open Shortest Path First – протокол внутрішньої маршрутизації з відкритим алгоритмом пошуку найкоротшого шляху.

PE – Provider Edge – крайовий маршрутизатор провайдера, який обслуговує підключення клієнта.

P – Provider Router – маршрутизатор провайдера в середині MPLS-ядра, який не взаємодіє безпосередньо з клієнтами.

QoS – Quality of Service – механізм управління якістю обслуговування трафіку.

SDN – Software Defined Networking – програмно-визначені мережі, що дозволяють централізовано управляти трафіком.

VRF – Virtual Routing and Forwarding – віртуальне маршрутизаційне середовище для ізоляції трафіку клієнтів.

VPN – Virtual Private Network – віртуальна приватна мережа для захищеної передачі даних через загальнодоступні мережі.

VLAN – Virtual Local Area Network – логічне сегментування локальної мережі для підвищення безпеки та керованості.

IPv4 – Internet Protocol version 4 – міжмережевий протокол четвертої версії.

IPv6 – Internet Protocol version 6 – новіша версія міжмережевого протоколу з розширеним адресним простором.

MAC – Media Access Control – метод управління доступом до середовища передачі даних.

ВСТУП

У сучасному інформаційному суспільстві надійна та ефективна мережна інфраструктура є ключовим елементом функціонування будь-якого підприємства. Розвиток цифрових сервісів, хмарних технологій, IP-телефонії, відеоконференцій та систем віддаленого доступу вимагає від корпоративних мереж здатності передавати великі обсяги різноманітного трафіку з мінімальними затримками, високою якістю обслуговування (QoS) та гарантією безпеки.

Для вирішення цих завдань дедалі ширше застосовується технологія IP/MPLS (Multiprotocol Label Switching), яка забезпечує гнучке управління трафіком, пріоритезацію сервісів і надійну маршрутизацію на основі міток. IP/MPLS дає змогу інтегрувати різні типи трафіку (дані, голос, відео) в єдиній мережі, а також легко масштабувати інфраструктуру відповідно до потреб підприємства.

Метою дипломної роботи є проєктування та впровадження корпоративної мультисервісної мережі з використанням технології IP/MPLS, яка забезпечує ефективну передачу даних, високу якість обслуговування та надійний захист інформації.

Завдання, які вирішуються в роботі:

- Аналіз теоретичних основ корпоративних мереж і технології IP/MPLS.
- Розробка архітектури мультисервісної мережі з урахуванням функціональних вимог.
- Реалізація, тестування, експлуатація та захист спроєктованої мережі.

Об’єктом дослідження є корпоративна мультисервісна мережа, яка об’єднує різні сервіси підприємства. Предметом дослідження є методи побудови, налаштування, експлуатації та захисту корпоративної мережі з використанням IP/MPLS.

У першому розділі роботи планується розглянути теоретичні основи побудови корпоративних мереж, класифікацію, основні функціональні характеристики, а також принципи роботи та переваги технології IP/MPLS.

У другому розділі роботи планується здійснити аналіз вимог до мережевої інфраструктури, розробити архітектуру мережі, обґрунтувати вибір обладнання та протоколів, а також підготувати рекомендації щодо впровадження.

У третьому розділі роботи планується реалізувати мережу у віртуальному середовищі, провести налаштування, описати процес експлуатації, організувати моніторинг, а також розробити комплекс заходів з інформаційної безпеки.

Актуальність теми зумовлена потребою в побудові універсальних, безпечних та масштабованих корпоративних мереж, які здатні підтримувати безперебійну роботу інформаційних систем підприємства, оптимізувати бізнес-процеси та забезпечити якісну взаємодію між віддаленими філіями. Використання технології IP/MPLS є ефективним рішенням для досягнення цих цілей.

1 ТЕОРЕТИЧНІ ОСНОВИ КОРПОРАТИВНИХ МЕРЕЖ ТА ТЕХНОЛОГІЇ IP/MPLS

1.1 Основні поняття та класифікація корпоративних мереж

1.1.1 Визначення поняття «корпоративна мережа»

Корпоративна мережа охоплює всю структуру підприємства, забезпечуючи зв'язок між усіма підрозділами без винятку. Вона створює єдиний інформаційний простір, у межах якого працівники мають доступ до необхідних даних і програмних додатків відповідно до політик інформаційної безпеки. Завдяки цьому всі інформаційні ресурси організації стають централізовано доступними через мережу.

У процесі експлуатації така мережа демонструє високу керованість, надійність і доступність. Її технічні характеристики дозволяють забезпечити безперебійну роботу критично важливих сервісів, що мають вирішальне значення для стабільного функціонування бізнес-процесів підприємства.

Корпоративна мережа виконує роль інфраструктурної основи організації, що сприяє реалізації стратегічних завдань і досягненню її цілей. Вона створює єдиний інформаційний простір, який охоплює всі елементи підприємства. У цьому контексті корпоративна мережа розглядається як головний системоутворюючий компонент, на основі якого будуються інші системи та сервіси.

Розгляд корпоративної мережі можливий з різних точок зору. Загальне уявлення про неї формується шляхом аналізу її складових з кількох перспектив:

- структурна (інфраструктура);
- функціональна (сервіси та додатки);
- експлуатаційні характеристики (властивості мережі).

З функціональної точки зору корпоративна мережа є ефективним середовищем для передачі актуальної інформації, необхідної для вирішення бізнес-завдань. З точки зору системно-технічного підходу вона являє собою багаторівневу структуру, що включає такі компоненти:

- комп'ютерну мережу;
- телекомунікаційну інфраструктуру;
- апаратні платформи;
- програмне забезпечення проміжного рівня;
- прикладні додатки.

З точки зору функціональності корпоративна мережа працює як єдина система, що забезпечує користувачів необхідними сервісами та програмами. Вона включає загальносистемні й спеціалізовані програмні рішення, які мають певні ключові характеристики.

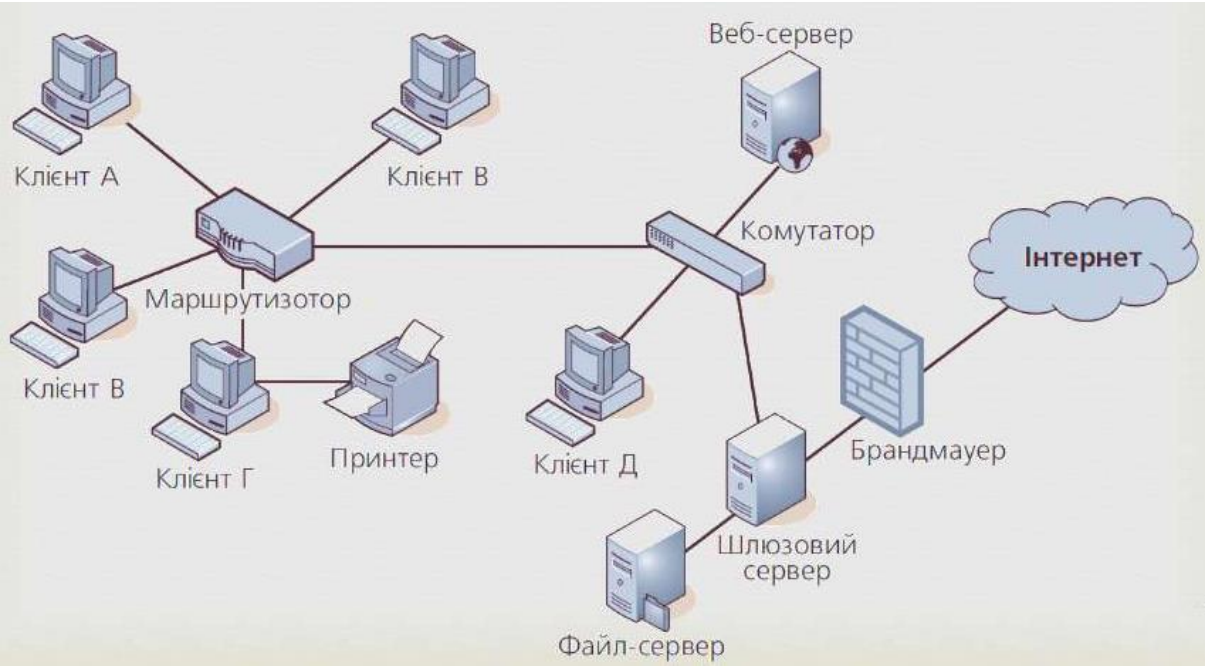

Рисунок 1.1 – Структура типової мережі

Одним із ключових принципів побудови корпоративної мережі є використання стандартних, уніфікованих компонентів і типових рішень.

Зокрема, в контексті прикладного програмного забезпечення доцільно виділити базові сервіси, які включають:

- систему управління базами даних (СУБД);
- файловий сервіс;
- інформаційний сервіс;
- VoIP телефонію;
- відеоконференцзв’язок;
- мережевий друк тощо.

Основним засобом для розгортання прикладних і системних сервісів є програмне забезпечення проміжного рівня. Архітектура корпоративної мережі є багатошаровою: нижні рівні містять базові сервіси (система імен, реєстрації, мережевий сервіс), тоді як верхні рівні включають сервіси управління документами, обміном повідомленнями тощо. На найвищому рівні знаходяться сервіси, якими користуються працівники підприємства через додатки.

Корпоративну мережу зручно описувати у вигляді сервісів. Наприклад, політика інформаційної безпеки базується на необхідності захисту існуючих сервісів.

Спеціалізовані додатки розробляються для виконання специфічних завдань, які не можуть бути автоматизовані загальносистемними рішеннями. Вони можуть бути придбані у розробників, створені на замовлення підприємства або розроблені власними силами компанії. Зазвичай, такі додатки використовують загальносистемні сервіси, наприклад, файловий сервіс або СУБД. Саме поєднання спеціалізованих програмних рішень та корпоративних сервісів формує повний спектр прикладної функціональності мережі.

Системно-технічна інфраструктура корпоративної мережі має значно триваліший термін служби порівняно з прикладним програмним забезпеченням. Це дозволяє розгортати нові додатки та забезпечувати їх

ефективну роботу, зберігаючи попередні інвестиції. Тому корпоративна мережа повинна мати такі характеристики, як відкритість, продуктивність, балансованість, масштабованість, висока готовність, безпека та керованість. Ці параметри визначаються якістю продуктів і рішень, які складають її основу.

Якість реалізації певних властивостей корпоративної мережі залежить від грамотного проектування. Наприклад, безпека, висока доступність і керованість досягаються за допомогою впровадження відповідних служб. Масштабованість у контексті серверних платформ означає можливість поступового нарощування обчислювальної потужності, збереження єдиної операційної системи для всіх моделей серверів і зручної модифікації молодших моделей у старші.

Загальносистемні служби містять набір програмних засобів, які не виконують безпосередньо прикладні завдання, але забезпечують стабільну роботу всієї корпоративної мережі. Серед них ключове значення мають:

- служби інформаційної безпеки;
- централізований моніторинг;
- адміністрування системи.

Розглянуті концепції дозволяють сформулювати принципи побудови корпоративної мережі без прив’язки до конкретного апаратного чи програмного забезпечення, але з достатнім рівнем деталізації для визначення її корисної функціональності та експлуатаційних характеристик. Викладені ідеї є основою для практичного впровадження корпоративної мережі та реалізації конкретних технічних рішень.

1.1.2 Основні типи мереж та їх особливості

Комп'ютерна мережа — це система, що об'єднує два або більше комп'ютерів, даючи можливість обміну даними, ресурсами та послугами.

Такі мережі можуть використовувати різні технології, такі як Ethernet, Wi-Fi, Bluetooth та інші.

Існує кілька способів класифікації комп'ютерних мереж: за розміром (локальні, міські, глобальні), за топологією (зірка, шина, дерево, кільце, меш), за протоколами комунікації (TCP/IP, HTTP, FTP, SMTP тощо) та інші. Вони мають численні застосування, включаючи спільне використання ресурсів, друк, обмін файлами, доступ до Інтернету, відеоконференції, онлайн-ігри та інше. Крім того, мережі дозволяють централізовано зберігати та обробляти дані, що є важливим для бізнесу та наукових досліджень.

Топологія "Загальна шина" — це мережа, в якій усі комп'ютери підключені до одного спільного каналу передачі даних (кабелю). У такій мережі дані передаються між пристроями через цей спільний канал, що може призводити до затримок та колізій, особливо при одночасному використанні шини багатьма комп'ютерами (рис. 1.1).

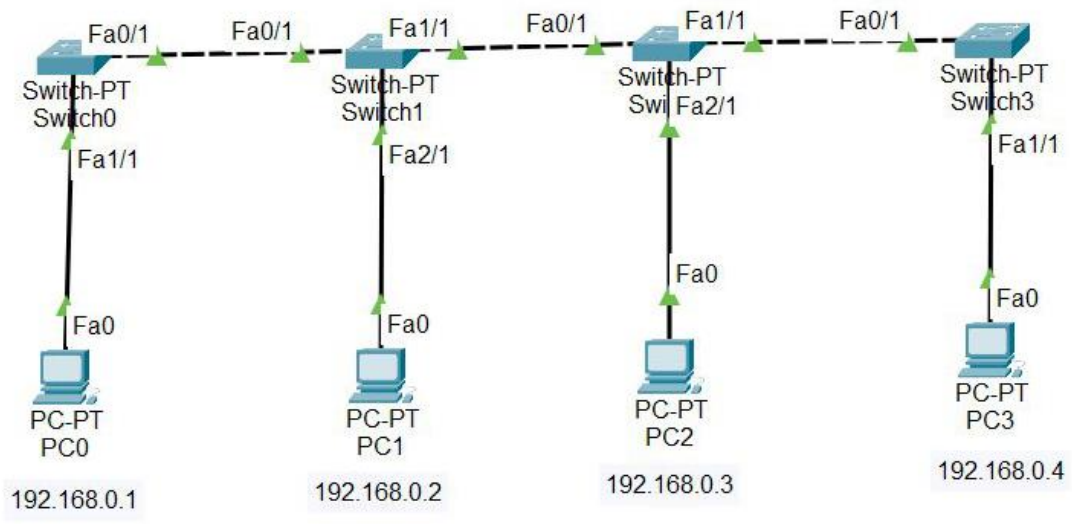

Рисунок 1.2 – Топологія «загальна шина»

Основними перевагами цієї топології є простота налаштування та низька вартість, оскільки не потрібне додаткове обладнання, наприклад,

концентратори чи комутатори. Вона також дозволяє легко додавати нові пристрої. Однак її використання обмежене через недостатню надійність та повільну швидкість передачі, тому в більшості випадків застосовують топології "Зірка" чи "Дерево".

Топологія "Кільце" — це тип мережі, де кожен комп'ютер підключений до двох інших, утворюючи замкнутий ланцюг. Дані передаються по колу в одному напрямку, і передача можливе лише після отримання контрольного токена (рис. 1.2).

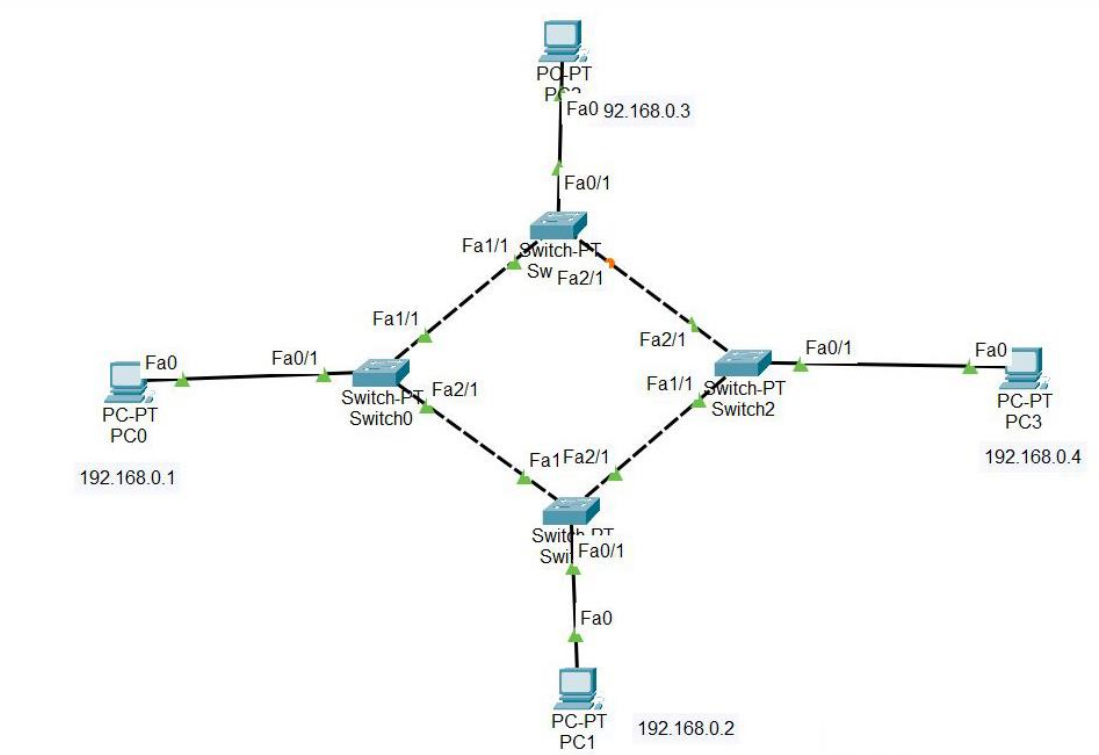

Рисунок 1.3 – Топологія «кільце»

Топологія кільце дозволяє рівномірно розподіляти навантаження та забезпечує високу надійність. Якщо один комп'ютер виходить з ладу, мережа може продовжувати працювати. Однак вона має високу вартість та складність у ремонті, а також більші затримки при передачі даних. Сьогодні ця топологія майже не використовується, але вона може бути знайдена в застарілих мережах.

Топологія "Зірка" — це мережа, в якій всі комп'ютери підключені до центрального пристрою, такого як комутатор або концентратор. Дані передаються від кожного комп'ютера до центрального пристрою, який пересилає їх до призначеного комп'ютера (рис 1.3).

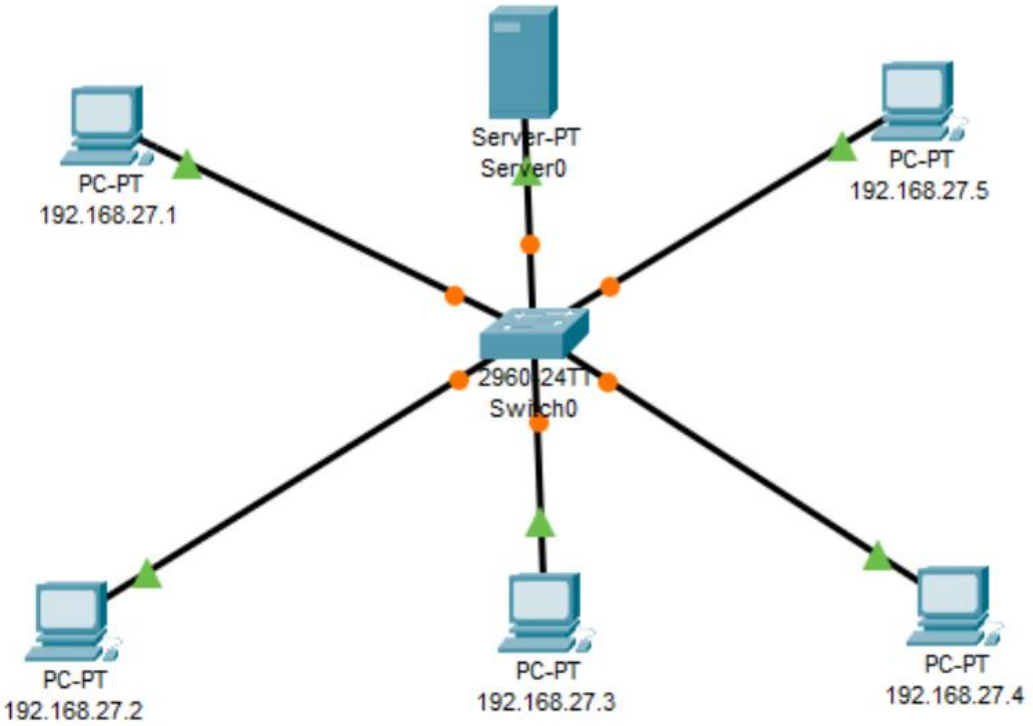

Рисунок 1.4 – Топологія «зірка»

Це забезпечує високу швидкість передачі даних та зменшує вплив затримок та колізій. Якщо один комп'ютер виходить з ладу, решта мережі залишається працюючою. Основні переваги топології "Зірка" — простота налаштування та можливість легкого підключення нових пристроїв. Проте її недоліком є те, що якщо центральний пристрій виходить з ладу, вся мережа стає недоступною, а також вона вимагає більше кабелів, що може збільшити вартість. Ця топологія є однією з найбільш поширених у сучасних мережах, зокрема в Ethernet.

Якщо мережа складається з кількох різних топологій, вона називається гібридною топологією (рис 1.4).

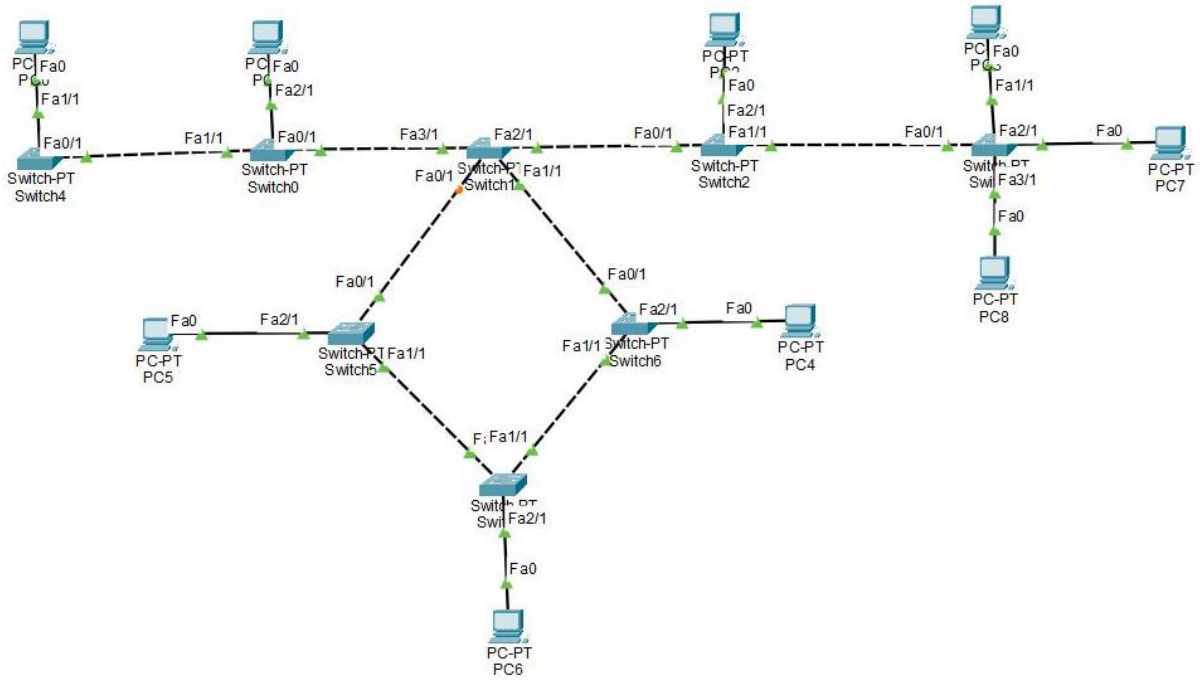

Рисунок 1.5 – Гібридна топологія

Гібридні топології часто використовуються в великих підприємствах, де різні відділи мають мережі з різними топологіями, які об'єднані в одну. Це дозволяє комбінувати переваги різних топологій, але також може створювати нові уразливості залежно від обраних типів мереж.

1.1.3 Роль мультисервісних мереж в сучасному бізнес-середовищі та концепції розвитку мереж наступного покоління

В умовах зростаючих вимог до якості та кількості послуг у сфері телекомунікацій усе більш актуальним стає впровадження технології NGN (Next Generation Network). Основна ідея NGN полягає у відокремленні сервісів від транспортної інфраструктури, що дає змогу ефективно поєднувати різні типи трафіку (голосовий, відео, дані) в єдиній мережі.

Сучасні оператори зв’язку поступово відмовляються від застарілих комутаційних систем і впроваджують IP-орієнтовану інфраструктуру, яка

дозволяє масштабувати сервіси, знижувати експлуатаційні витрати та прискорювати впровадження нових послуг. NGN-архітектура створює гнучке середовище, в якому можна інтегрувати новітні сервіси, такі як VoIP, IPTV, відеоконференції та хмарні платформи, що є особливо важливим у корпоративних мережах.

На практиці впровадження NGN можливе шляхом модернізації існуючих мереж до IP/MPLS, що забезпечує ефективну маршрутизацію трафіку та підтримку багатьох сервісів з гарантованою якістю (QoS). Також важливим аспектом є підтримка протоколів сигналізації SIP та H.248, які дають змогу інтегрувати традиційні послуги з новими IP-сервісами.

У сучасному світі концепція NGN активно реалізується у вигляді споріднених технологій, зокрема програмно-обумовлених мереж (SDN — Software Defined Networking) та віртуалізації мережевих функцій (NFV — Network Functions Virtualization). Вони дозволяють операторам швидко адаптувати інфраструктуру до змін попиту, централізовано керувати мережевими ресурсами та впроваджувати нові сервіси без фізичних змін обладнання.

Ще одним прикладом є технологія IMS (IP Multimedia Subsystem), яка є логічним продовженням концепції NGN і дозволяє створювати конвергентні сервіси на базі єдиної IP-інфраструктури. У мобільних мережах NGN-технології відіграють важливу роль у розгортанні стандарту 5G, що вимагає високої пропускної здатності, мінімальних затримок і широкої підтримки цифрових послуг у реальному часі.

1.2 Концепція та архітектура технології IP/MPLS

1.2.1 Принципи роботи IP/MPLS

IP/MPLS (англ. Internet Protocol/Multiprotocol Label Switching) є технологією, яка поєднує маршрутизацію за протоколом IP і використання

міток для передачі пакетів через мережу. В основі роботи MPLS лежить додавання мітки до кожного пакету, яка визначає, як цей пакет буде передаватися через мережу. Коли пакет потрапляє в мережу MPLS, йому надається унікальна мітка, яка вказує маршрутизатору, як обробляти і куди направляти пакет. Цей процес дозволяє значно прискорити маршрутизацію, оскільки маршрутизатору не потрібно аналізувати весь заголовок пакету, а достатньо лише перевірити мітку.

Однією з важливих характеристик MPLS є можливість визначення маршрутів за допомогою попередньо налаштованих шляхів, що називаються LSP (Label Switched Path). Ці шляхи з’єднують джерело і приймач пакету через кілька вузлів мережі, що дозволяє передавати дані більш ефективно. На кожному маршрутизаторі в межах LSP відбувається "перемикання міток" — мітка пакету змінюється на нову, яка вказує на наступний етап маршруту.

MPLS також підтримує концепцію якості обслуговування (QoS), що дозволяє пріоритизувати трафік в залежності від вимог до швидкості та затримок. Це особливо важливо для таких послуг, як VoIP або відеоконференції, де висока швидкість передачі та низькі затримки є критичними для нормальної роботи.

Технологія MPLS дозволяє більш ефективно використовувати ресурси мережі, скорочуючи час обробки пакетів і знижуючи навантаження на маршрутизатори. Це забезпечує високий рівень продуктивності, навіть у великих і складних мережах.

1.2.2 Порівняльний аналіз з традиційними IP-технологіями

Порівнюючи технологію IP/MPLS із традиційними IP-мережами, можна виділити низку ключових відмінностей, які визначають ефективність і доцільність використання тієї чи іншої технології.

У традиційних IP-мережах маршрутизація здійснюється на основі IP-адрес. Кожен маршрутизатор окремо аналізує IP-заголовок пакета, приймаючи рішення щодо маршруту його передачі. Такий підхід є універсальним, але в умовах великих навантажень спричиняє затримки через необхідність багаторазової обробки інформації на кожному етапі. Натомість IP/MPLS використовує мітки, які присвоюються пакетам на вході в мережу. Це дає змогу значно пришвидшити обробку даних: маршрутизатори не аналізують повний заголовок, а лише перемикають мітки відповідно до попередньо налаштованих шляхів.

У плані масштабованості традиційні IP-мережі зіштовхуються з обмеженнями, оскільки кожен маршрутизатор має зберігати значні таблиці маршрутизації, що ускладнює управління мережею та знижує її ефективність. IP/MPLS, завдяки використанню LSP (Label Switched Path), дозволяє спростити маршрутизацію, полегшує управління інфраструктурою та забезпечує більшу гнучкість.

Ще однією важливою відмінністю є підтримка якості обслуговування (QoS). У звичайних IP-мережах такі можливості обмежені, що створює труднощі при передачі чутливого трафіку, наприклад, голосу або відео. На відміну від цього, IP/MPLS забезпечує вбудовану підтримку QoS, що дозволяє розподіляти трафік за пріоритетністю та гарантувати мінімальні затримки для критично важливих сервісів.

Технологія MPLS також переважає в аспекті продуктивності. Завдяки механізму перемикання міток зменшується навантаження на маршрутизатори та прискорюється передача даних. У традиційних мережах передача кожного пакета супроводжується значними обчислювальними витратами, що погіршує загальну ефективність.

Крім того, IP/MPLS має вищу надійність. У разі збою на одному з вузлів мережі, трафік може бути автоматично перенаправлений альтернативними маршрутами, що забезпечує стійкість мережевої

інфраструктури. У традиційних IP-мережах цей процес менш гнучкий і часто вимагає додаткового часу на переналаштування маршруту.

У підсумку, порівняння IP/MPLS та традиційних IP-технологій показує, що традиційні IP-мережі мають обмеження в масштабованості та ефективності через великі таблиці маршрутизації та затримки при обробці трафіку. Наприклад, кожен маршрутизатор повинен обробляти повні заголовки IP-пакетів, що знижує швидкість передачі.

IP/MPLS вирішує ці проблеми, використовуючи мітки для маршрутизації, що значно зменшує час обробки пакету. Технологія також підтримує QoS, що дозволяє пріоритизувати трафік для важливих послуг, таких як відеоконференції. Це забезпечує високу якість обслуговування та підвищену надійність, оскільки IP/MPLS швидко перенаправляє трафік у разі відмови, на відміну від традиційних IP-мереж, де переналаштування маршруту займає більше часу.

1.2.3 Основні компоненти та протоколи IP/MPLS

IP/MPLS (Internet Protocol/Multi-Protocol Label Switching) є складною мережею, що використовує різні компоненти та протоколи для забезпечення ефективної маршрутизації та управління трафіком. Основні компоненти та протоколи включають:

Мітки (Labels): Основний елемент у технології MPLS, мітки використовуються для ідентифікації і маркування трафіку, що дозволяє мережевим пристроям швидше приймати рішення про маршрутизацію, оскільки вони працюють з мітками замість обробки повних IP-адрес.

Маршрутизатори (LSR - Label Switch Router): Це основні мережеві пристрої в MPLS, які здійснюють процес перенаправлення пакетів на основі міток. Вони можуть бути як входом, так і виходом у мережі, виконуючи маршрутизацію та заміну міток для передачі пакетів.

LDP (Label Distribution Protocol): Це протокол, який використовується для розподілу міток між маршрутизаторами в MPLS-мережі. LDP дозволяє маршрутизаторам ділитися інформацією про мітки, що необхідно для побудови шляху через мережу.

RSVP-TE (Resource Reservation Protocol - Traffic Engineering): Протокол, який дозволяє управляти ресурсами та резервувати мережеві ресурси для специфічних трафіків, таких як відео чи голосові дзвінки, з гарантованою якістю обслуговування.

BGP (Border Gateway Protocol): Протокол, який використовується для обміну інформацією про маршрути між різними автономними системами. У контексті MPLS BGP може використовуватися для обміну інформацією про мітки в міжмережевих зв'язках.

MPLS TE (Traffic Engineering): Це техніка, що використовується для оптимізації використання мережевих ресурсів, розподіляючи трафік через певні шляхи, щоб уникнути перевантаження деяких частин мережі.

LSP (Label Switched Path): Це шлях, який визначений для передачі пакетів з мітками через мережу MPLS. LSP складається з маршруту, який передає пакети від початкового маршрутизатора до кінцевого маршрутизатора на основі міток.

IP/MPLS є потужною технологією, яка дозволяє значно покращити ефективність та продуктивність мережі. Ключові компоненти, такі як мітки, маршрутизатори LSR, протоколи LDP, RSVP-TE, BGP і MPLS TE, працюють разом для забезпечення швидкої маршрутизації і ефективного управління трафіком. Використання міток замість традиційної маршрутизації за IP-адресами дає змогу прискорити процес прийняття рішень, зменшуючи затримки та навантаження на маршрутизатори. Протоколи, як LDP і RSVP-TE, дозволяють маршрутизаторам ефективно розподіляти ресурси і забезпечувати гарантовану якість обслуговування для критичних додатків, таких як відео або голосовий трафік.

Один із основних аспектів IP/MPLS – це можливість гнучкого управління мережевими ресурсами та оптимізації трафіку, що особливо важливо для великих і складних мереж з різними типами послуг. Протокол BGP дозволяє обмінюватися маршрутною інформацією між різними автономними системами, а MPLS TE дає можливість керувати потужністю мережі для досягнення кращої ефективності. Механізми побудови LSP забезпечують маршрутизацію трафіку через найефективніші шляхи мережі. Таким чином, використання технології IP/MPLS дозволяє створювати більш масштабовані, надійні і продуктивні мережі, що здатні підтримувати високоякісні послуги для широкого спектра користувачів.

1.3 Переваги і виклики застосування IP/MPLS в корпоративних мережах

1.3.1 Переваги впровадження IP/MPLS для мультисервісності

Впровадження технології IP/MPLS для мультисервісних мереж приносить значні переваги, які роблять її надзвичайно ефективною для забезпечення різноманітних послуг в одній мережі. Одна з основних переваг полягає в можливості забезпечення високої якості обслуговування (QoS) для різних типів трафіку, таких як голос, відео, дані та інші мультимедійні послуги. Зокрема, IP/MPLS дозволяє використовувати різні методи управління трафіком, щоб надавати пріоритет для важливих даних, забезпечуючи мінімальні затримки і високу надійність для критичних послуг. Це важливо, коли, наприклад, потрібно забезпечити стабільність під час відеоконференцій або передачі голосу через Інтернет, що вимагає низьких затримок та гарантованої пропускної здатності.

Ще однією ключовою перевагою є масштабованість і гнучкість мережі, що дозволяє швидко адаптувати її під зростання кількості користувачів та послуг без великих інвестицій у нове обладнання. Із

збільшенням навантаження або вимог до мережі, IP/MPLS дає змогу ефективно розподіляти ресурси та збільшувати пропускну здатність без необхідності значних змін в інфраструктурі, що робить її ідеальним рішенням для великих і складних мереж. Таким чином, технологія дозволяє операторам і підприємствам максимально ефективно управляти ресурсами і забезпечувати стабільну роботу послуг при мінімальних витратах.

IP/MPLS також дозволяє інтегрувати різні види послуг у межах однієї мережі, що дозволяє знизити витрати на обслуговування і модернізацію окремих мереж для кожної послуги. Це означає, що оператори можуть одночасно надавати голосові, відео та інтернет-послуги, забезпечуючи ефективне використання наявної інфраструктури. Завдяки механізму маршрутизації на основі міток, IP/MPLS дозволяє швидко і ефективно передавати дані через оптимальні маршрути, знижуючи навантаження на мережу і підвищуючи її загальну продуктивність.

Не менш важливою є здатність IP/MPLS забезпечити надійність і гарантовану доставку даних, що є критичним для мультисервісних мереж. За допомогою механізмів резервування і підтримки альтернативних маршрутів для трафіку, технологія здатна мінімізувати ризики перерв у наданні послуг. Наприклад, при виході з ладу одного з компонентів мережі IP/MPLS може забезпечити автоматичне перенаправлення трафіку через інші маршрути без втрати даних або значних затримок.

Таким чином, впровадження IP/MPLS для мультисервісних мереж дозволяє операторам досягти значного підвищення ефективності, надійності та гнучкості при наданні різноманітних послуг. Можливість забезпечити високу якість обслуговування, інтегрувати різні види трафіку в одній мережі та оптимізувати використання ресурсів робить цю технологію ідеальним рішенням для сучасних телекомунікаційних операторів.

1.3.2 Сучасні тенденції використання мереж з IP/MPLS

Ринок рішень на базі IP/MPLS активно розвивається і відображає тенденції, які визначають майбутнє телекомунікаційної інфраструктури. Зі збільшенням попиту на високошвидкісні, надійні та мультимедійні сервіси для кінцевих користувачів, IP/MPLS стає основною технологією для створення масштабованих і гнучких мереж. Розвиток цього ринку можна поділити на кілька основних тенденцій, які зумовлюють його популярність і подальший ріст.

Однією з основних тенденцій є перехід до інтеграції різних послуг в межах єдиної мережі. Всі більш популярними стають рішення, які дозволяють забезпечити передачу не тільки традиційного голосового трафіку, але й відео, даних, а також інших мультимедійних послуг через одну і ту ж інфраструктуру. Це значно знижує витрати на підтримку окремих мереж і дозволяє ефективно використовувати наявні ресурси. В результаті, оператори мереж можуть одночасно запропонувати широкий спектр послуг, що сприяє зростанню доходів і залученню нових користувачів.

Друга важлива тенденція — це перехід до мереж з більш високим рівнем автоматизації та управління. Оскільки вимоги до якості обслуговування зростають, технології, що використовуються в рамках IP/MPLS, надають можливість автоматизувати управління трафіком і ресурсами мережі. Використання програмно визначених мереж (SDN) та функцій віртуалізації дозволяє ефективно управляти потоками даних і забезпечувати високий рівень QoS. Це дозволяє операторам знижувати витрати на управління мережею і підвищувати її ефективність.

Ще однією важливою тенденцією є розвиток рішень для мобільних мереж і IoT. IP/MPLS активно впроваджується в мобільні та Інтернет речей (IoT) мережі завдяки своїй здатності забезпечувати низьку затримку і

гарантовану пропускну здатність. Це дозволяє створювати мережі, здатні підтримувати широкий спектр застосунків, від смарт-пристроїв до автономних транспортних засобів. Інтеграція IP/MPLS з мобільними мережами допомагає задовольнити вимоги до пропускної здатності і надійності для таких технологій, як 5G, що створює нові можливості для операторів.

Масштабованість і гнучкість мереж є також важливими аспектами, що визначають тенденції розвитку ринку IP/MPLS. Оскільки потреби в пропускній здатності і покритті мереж зростають, необхідність масштабування мережі стає критично важливою для забезпечення стабільного і безперервного сервісу. Технологія IP/MPLS дозволяє створювати гнучкі та масштабовані рішення для великих підприємств і операторів, що можуть швидко адаптувати свою інфраструктуру до змінюваних вимог і умов.

Нарешті, важливою тенденцією є збільшення фокуса на безпеці мереж. Зростання кіберзагроз та вимоги до збереження конфіденційності та цілісності даних змушують операторів інтегрувати механізми безпеки на всіх рівнях мережі. IP/MPLS дозволяє застосовувати передові методи шифрування та захисту даних, що підвищує безпеку при передачі чутливої інформації.

Таким чином, ринок рішень на базі IP/MPLS продовжує розвиватися, відображаючи основні технологічні тенденції, такі як інтеграція послуг, автоматизація управління, розвиток мобільних мереж, масштабованість і безпека. Ці тенденції дозволяють операторам і підприємствам створювати більш ефективні, надійні та вигідні мережеві рішення, що відповідають вимогам сучасного інформаційного суспільства.

1.3.3 Роль IP/MPLS у побудові сучасних корпоративних мереж

Технологія IP/MPLS відіграє ключову роль у створенні сучасних корпоративних мереж завдяки своїй універсальності, продуктивності та здатності забезпечувати гнучке управління трафіком. Її застосування дозволяє реалізовувати складні топології з підтримкою мультисервісності, високої якості обслуговування та логічної ізоляції трафіку для підвищення безпеки.

IP/MPLS є ефективним інструментом для об'єднання територіально розподілених підрозділів організацій, оскільки забезпечує стійку маршрутизацію між віддаленими офісами, незалежно від географічного розташування. Технологія дозволяє побудувати мережу з підтримкою кількох рівнів обслуговування (QoS), що є критично важливим для одночасної роботи таких сервісів, як IP-телефонія, відеоконференції, хмарні застосунки та централізовані бази даних.

Завдяки можливості створення віртуальних приватних мереж (VPN) та використанню механізму віртуальних таблиць маршрутизації (VRF), IP/MPLS забезпечує гнучкість конфігурації та високий рівень ізоляції даних між різними службами чи відділами. Це дозволяє значно покращити захист інформації, особливо в умовах багатокористувацького доступу або інтеграції з зовнішніми сервісами.

Крім того, IP/MPLS підтримує масштабованість на рівні операторських рішень, що дозволяє легко додавати нові вузли, розширювати пропускну здатність та інтегрувати додаткові сервіси без порушення існуючої інфраструктури. Завдяки цьому технологія широко використовується не лише в телекомунікаційних компаніях, а й у великих корпоративних мережах, банківській сфері, освіті та державних установах.

Висновки з розділу 1

У першому розділі було розглянуто базові поняття корпоративних мереж, їх структуру, функціональні характеристики та актуальність використання мультисервісної архітектури. Особливу увагу приділено технології IP/MPLS, її принципам роботи, архітектурі та порівнянню з традиційними IP-мережами. Показано, що IP/MPLS забезпечує високу ефективність, масштабованість, якість обслуговування (QoS) та гнучке управління трафіком, що робить її доцільною для використання в сучасних корпоративних мережах. Також проаналізовано сучасні тенденції в галузі — перехід до NGN, SDN, NFV та інтеграції мобільних технологій.

2 ПРОЕКТУВАННЯ КОРПОРАТИВНОЇ МУЛЬТИСЕРВІСНОЇ МЕРЕЖІ З ВИКОРИСТАННЯМ IP/MPLS

2.1 Аналіз вимог до мережевої інфраструктури

2.1.1 Оцінка потреб організації по використанню корпоративної мережі

Першим етапом проектування корпоративної мультисервісної мережі є оцінка поточних і перспективних потреб організації у сфері телекомунікацій. Для ефективного функціонування організації необхідно забезпечити безперервний, захищений та високошвидкісний доступ до інформаційних ресурсів, внутрішніх сервісів, а також до зовнішніх мереж, зокрема Інтернету.

Організація має розгалужену структуру з декількома філіями, які географічно розміщені у різних регіонах. Основними потребами є: забезпечення швидкого та надійного обміну даними між філіями, підтримка голосового та відеозв’язку (VoIP, відеоконференції), централізований доступ до баз даних, систем документообігу, ERP-систем та інших корпоративних додатків.

З урахуванням вищевказаного, до ключових вимог до мережі можна віднести:

- Масштабованість — можливість легко додавати нові підрозділи та сервіси без істотної перебудови мережі.
- Надійність і відмовостійкість — підтримка резервування каналів і критично важливих вузлів.Якість обслуговування (QoS) — пріоритезація трафіку для голосу, відео та критичних бізнес-додатків.
- Безпека — шифрування трафіку, розмежування доступу, захист від несанкціонованого втручання.
- Гнучке управління — централізований моніторинг і контроль мережевих ресурсів, можливість віддаленої конфігурації.

Для задоволення цих вимог обрано концепцію NGN на базі технології IP/MPLS, яка дозволяє реалізувати мультисервісну мережу з підтримкою VPN, забезпеченням високої пропускної здатності та гнучкого управління маршрутами. Це рішення дозволить оптимізувати роботу організації, зменшити витрати на інфраструктуру та підвищити якість внутрішніх і зовнішніх комунікацій.

2.1.2 Визначення функціональних та нефункціональних вимог до мережі

На основі аналізу потреб організації сформовано перелік функціональних та нефункціональних вимог до майбутньої корпоративної мультисервісної мережі. Ці вимоги є критично важливими для проєктування інфраструктури, яка повинна забезпечити стабільну, безпечну та ефективну роботу всіх цифрових сервісів компанії.

До функціональних вимог належить, передусім, забезпечення повноцінної взаємодії між усіма підрозділами організації, незалежно від їхнього географічного розташування. Це включає можливість обміну даними, доступу до центральних серверів, спільного використання програмного забезпечення, голосових та відео сервісів, таких як IP-телефонія та відеоконференції. Також мережа повинна підтримувати підключення до хмарних платформ та забезпечувати віддалений доступ для співробітників із дотриманням політик безпеки. Управління мережею має здійснюватися централізовано з використанням зручних засобів моніторингу та адміністрування.

Нефункціональні вимоги включають параметри, які впливають на якість роботи мережі, але не описують її безпосередні функції. До таких вимог належить висока надійність — мережа має бути стійкою до збоїв завдяки наявності резервних каналів і механізмів автоматичного

відновлення з’єднань. Масштабованість є ще одним ключовим аспектом: проектована система повинна дозволяти легко додавати нові офіси, вузли чи сервіси без потреби в повному переоснащенні. Також критично важливою є пропускна здатність — вона повинна відповідати поточному та прогнозованому навантаженню, особливо з урахуванням одночасної роботи кількох сервісів.

Окрему увагу приділено безпеці — необхідно впровадити засоби автентифікації, шифрування трафіку, захисту від несанкціонованого доступу та кіберзагроз. Крім того, для сервісів реального часу має бути реалізовано механізми керування якістю обслуговування (QoS), що дозволить забезпечити пріоритет трафіку для голосових і відео додатків. Гнучкість проектованого рішення також відіграє важливу роль, оскільки організація повинна мати можливість адаптувати мережу до змін у бізнес-процесах чи технічних потребах без значних витрат.

2.1.3 Аналіз сценаріїв використання мультисервісної мережі

Після визначення вимог до корпоративної мережі наступним кроком є аналіз можливих сценаріїв її використання. Це дозволяє оцінити, наскільки ефективно запропоноване рішення зможе підтримувати реальні бізнес-процеси організації та які сервіси будуть найважливішими для кінцевих користувачів. Основна мета аналізу полягає в моделюванні типових ситуацій, що виникають у щоденній діяльності компанії, з урахуванням навантаження на мережу, вимог до якості обслуговування та безпеки.

Один із основних сценаріїв передбачає щоденну офісну роботу персоналу, яка включає доступ до внутрішніх серверів, електронної пошти, файлових сховищ і корпоративних інформаційних систем. У цьому випадку

мережа має забезпечувати високу швидкість обміну даними та стабільне з’єднання з мінімальними затримками.

Інший важливий сценарій — проведення відеоконференцій та телефонних дзвінків між співробітниками з різних філій. Такі сервіси є чутливими до затримок і втрати пакетів, тому система має підтримувати механізми пріоритезації трафіку, щоб забезпечити якісну передачу голосу та зображення навіть під час пікового навантаження.

Ще один актуальний сценарій — віддалений доступ до мережі для працівників, які працюють з дому або перебувають у відрядженні. Для таких користувачів необхідно забезпечити захищене з’єднання через VPN, при цьому продуктивність має залишатися на достатньому рівні для роботи з ключовими корпоративними сервісами.

Також варто враховувати сценарії резервного копіювання даних у фоновому режимі, обміну великими файлами між відділами, підключення хмарних додатків і автоматизованих систем, наприклад, систем відеоспостереження або контролю доступу. Усі ці випадки вимагають розрахованого та збалансованого підходу до проектування мережевого навантаження, з урахуванням майбутнього зростання кількості користувачів і сервісів.

2.2 Розробка мережевої архітектури на базі IP/MPLS

2.2.1 Структурування мережевих компонентів

Проектування архітектури корпоративної мультисервісної мережі передбачає чітке структурне розділення її основних компонентів відповідно до функціонального призначення та ролі в загальній інфраструктурі. Це дозволяє забезпечити надійність, масштабованість, ефективне управління ресурсами та відповідність вимогам до якості обслуговування.

Мережева інфраструктура поділяється на три основні рівні: ядро мережі (core), рівень агрегації (distribution) та рівень доступу (access). У центрі архітектури розташовується ядро — високопродуктивні маршрутизатори з підтримкою MPLS, які забезпечують швидку передачу даних між усіма сегментами мережі. Вони виконують функції маршрутизації, комутації на основі міток і реалізують політики пріоритезації трафіку.

Рівень агрегації виконує роль проміжної ланки між ядром і рівнем доступу. На цьому рівні об’єднуються дані з різних підрозділів або філій організації, здійснюється базова маршрутизація, фільтрація трафіку, розподіл навантаження та реалізація VPN-з'єднань. Тут доцільно використовувати керовані комутатори з підтримкою VLAN, QoS і резервування каналів.

Рівень доступу охоплює пристрої кінцевих користувачів та периферійне обладнання — робочі станції, принтери, IP-телефони, відеокамери тощо. Він забезпечує підключення клієнтів до внутрішньої мережі через доступні фізичні інтерфейси (Ethernet, Wi-Fi) з обмеженням прав доступу згідно з політиками безпеки.

Окрему групу становлять мережеві сервіси, які функціонують незалежно від фізичної структури, але критично важливі для забезпечення повноцінної роботи мережі. До них належать DNS і DHCP-сервери, системи аутентифікації користувачів, SIP-сервери, засоби моніторингу, а також міжмережеві екрани та VPN-шлюзи. Ці компоненти розміщуються у захищених зонах з обмеженим доступом і резервуванням.

2.2.2 Логічна схема мережі

Логічна схема корпоративної мультисервісної мережі описує розподіл мережевих функцій та зв’язків між компонентами без деталізації

їх фізичного розміщення. Вона відображає структуру взаємодії між ключовими вузлами, сервісами, сегментами та політиками обробки трафіку, зосереджуючи увагу на маршрутах передачі даних, логічному розділенні підмереж та реалізації сервісних рівнів.

У проєктованій мережі реалізовано логічне поділення на кілька основних зон: зону користувачів, зону сервісів, зону керування та захищену зону (DMZ). Зона користувачів включає підмережі окремих відділів компанії, що ізольовані за допомогою VLAN. Це дозволяє підвищити безпеку, мінімізуючи ризик несанкціонованого доступу між сегментами. Кожна VLAN маршрутизується через центральні маршрутизатори з підтримкою MPLS.

Зона сервісів містить основні сервери підприємства: файлові, поштові, баз даних, а також VoIP-сервер і відеоконференц-сервер. Весь трафік до цієї зони контролюється політиками доступу на рівні маршрутизаторів і міжмережевих екранів. Для підвищення ефективності застосовуються механізми пріоритезації трафіку — критичні служби (наприклад, IP-телефонія) мають вищий пріоритет, гарантований QoS.

Зона керування включає елементи моніторингу, централізованого управління мережею, логування та аудиту. Вона ізольована від користувацького трафіку й доступна лише адміністраторам. Сюди також належать сервери авторизації (AAA), контролери доступу та SNMP-сервери.

DMZ-зона слугує проміжним простором між внутрішньою мережею та Інтернетом. У ній розміщено публічні сервіси, зокрема VPN-шлюз, веб-сервер, а також шлюз електронної пошти. Всі з’єднання проходять через фаєрволи з ретельно прописаними політиками.

Усі вказані логічні зони об’єднані MPLS-ядром, яке забезпечує високопродуктивну маршрутизацію на основі міток та можливість створення VPN-сегментів для ізольованої передачі трафіку. Логічна схема

також передбачає резервні шляхи передачі, які автоматично активуються у разі відмови основних каналів.

Підсумовуючи, логічна модель мережі забезпечує функціональне розділення ресурсів, централізоване управління доступом, безпечну роботу сервісів та ефективну маршрутизацію відповідно до вимог корпоративного середовища.

2.3 Вибір обладнання та протоколів для реалізації мультисервісності

2.3.1 Критерії відбору апаратного забезпечення

Вибір апаратного забезпечення для побудови мультисервісної мережі ґрунтується на аналізі функціональних потреб організації, технічних характеристик обладнання та підтримки необхідних технологій. Основною метою є забезпечення стабільної роботи сервісів, гнучкого управління трафіком та подальшої масштабованості мережі.

Перш за все враховується продуктивність маршрутизаторів і комутаторів, які повинні підтримувати задану пропускну здатність і забезпечувати обробку трафіку з різних джерел — даних, голосових викликів, відео та сервісного трафіку. Пристрої мають мати достатню кількість фізичних інтерфейсів для підключення кінцевих пристроїв та інших вузлів мережі.

Наступним критерієм є підтримка протоколів маршрутизації, зокрема OSPF або RIP, що дозволяє забезпечити автоматичний обмін маршрутною інформацією між сегментами мережі. Це значно підвищує ефективність та гнучкість управління трафіком, особливо в умовах змінної структури або зростання навантаження.

Важливим є також забезпечення функцій розмежування трафіку, для чого необхідна підтримка віртуальних локальних мереж (VLAN). Це дає змогу логічно відокремити сервіси між собою та забезпечити більший

рівень безпеки. Крім того, пристрої повинні мати механізми реалізації пріоритетів (QoS), що дозволяє забезпечити стабільну якість для голосового та відеотрафіку.

Особлива увага приділяється надійності обладнання та можливості резервування: підтримка агрегованих каналів, динамічного маршрутизаційного переключення, збереження конфігурацій і віддалене управління є бажаними для зменшення часу реагування на збої та полегшення технічного обслуговування.

2.3.2 Обґрунтування вибору протоколів маршрутизації та обслуговування

Для забезпечення надійної та гнучкої роботи мережі важливо правильно обрати протоколи маршрутизації та обслуговування, які відповідатимуть структурі мережі, кількості вузлів і типам передаваного трафіку. З урахуванням масштабів проєктованої інфраструктури та потреб у мультисервісності, доцільно використовувати комбінацію статичної маршрутизації та одного з динамічних протоколів.

У мережах з відносно сталою структурою та невеликою кількістю маршрутизаторів ефективною є статична маршрутизація. Вона дозволяє адміністратору вручну задавати маршрути, що забезпечує передбачуваність трафіку і спрощує контроль над мережею. Статичні маршрути доцільно використовувати для резервних каналів, окремих підмереж або початкового етапу налаштування.

Для автоматизації обміну маршрутною інформацією між пристроями обрано протокол OSPF (Open Shortest Path First). Він є одним із найбільш поширених внутрішньомережевих протоколів і забезпечує швидку конвергенцію, ефективне розподілення навантаження та підтримку складніших топологій. OSPF дозволяє автоматично визначати найкоротші

маршрути, реагувати на зміни в мережі та забезпечувати більшу гнучкість порівняно зі статичною маршрутизацією.

Для обслуговування голосового та відеотрафіку передбачається використання механізмів якості обслуговування (QoS). Вони дозволяють розмежовувати трафік за пріоритетом і гарантувати стабільну передачу даних для сервісів, які чутливі до затримок. Це особливо важливо в умовах спільного використання мережі для різних типів інформації — від звичайних файлів до реального часу комунікацій.

2.3.3 Рекомендації щодо впровадження та масштабування

Для успішного впровадження мультисервісної мережі рекомендується здійснювати розгортання поетапно, починаючи з базової інфраструктури — ядра мережі та основних вузлів доступу. Це дозволяє мінімізувати ризики та спростити тестування ключових функцій. Перед повним запуском необхідно перевірити коректність маршрутизації, роботу основних сервісів (DHCP, DNS, VoIP), а також налаштування безпеки.

Масштабування мережі доцільно здійснювати за принципом модульності: кожен новий сегмент має інтегруватися без суттєвих змін до існуючої структури. Для цього важливо заздалегідь передбачити резерв адресного простору, підтримку динамічної маршрутизації та гнучке конфігурування VLAN. Також варто залишити запас пропускної здатності на рівні магістральних з’єднань і забезпечити можливість резервування критичних вузлів.

Висновки з розділу 2

У другому розділі виконано поетапний аналіз вимог до мережі, сформовано технічне завдання, розглянуто сценарії використання і

розроблено архітектуру корпоративної мультисервісної мережі на базі IP/MPLS. Визначено функціональні та нефункціональні вимоги до інфраструктури, такі як масштабованість, відмовостійкість, безпека та підтримка QoS. Побудовано логічну архітектуру, що включає три рівні: ядро, агрегацію та доступ. Обґрунтовано вибір апаратного забезпечення та протоколів маршрутизації (OSPF, BGP) відповідно до вимог мережі. Надано практичні рекомендації щодо впровадження мережі поетапно з урахуванням можливостей масштабування.

3 ВПРОВАДЖЕННЯ, ЕКСПЛУАТАЦІЯ ТА ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ МЕРЕЖІ

3.1 Реалізація та налаштування збудованної мережі

3.1.1 Вибір топології та рішень для маршрутизації

Для побудови корпоративної мультисервісної мережі було обрано топологію кільце, яка забезпечує замкнений цикл з'єднань між мережевими вузлами. Такий підхід дозволяє досягти високого рівня відмовостійкості та знизити ризик втрати зв'язку в разі виходу з ладу одного з елементів мережі, адже передача даних може здійснюватися в обхід. Крім того, кільцева топологія забезпечує рівномірний розподіл навантаження та полегшує моніторинг трафіку.

Впровадження корпоративної мультисервісної мережі передбачає реалізацію чіткої послідовності етапів, спрямованих на створення функціональної, масштабованої та відмовостійкої інфраструктури. Основна мета впровадження — побудова логічно сегментованої транспортної мережі з можливістю пріоритезації сервісного трафіку, маршрутизації між віддаленими філіями та підтримки якості обслуговування (QoS).

На початковому етапі виконується проектування загальної топології мережі. Враховуючи вимоги до мультисервісності, ми використовуємо технологію MPLS (Multiprotocol Label Switching) як базову, так як вона дозволяє організувати ефективну маршрутизацію за мітками, розділення трафіку за сервісами та реалізацію політик керування трафіком. Передбачається реалізація MPLS-ядра із використанням маршрутизаторів з підтримкою LDP (Label Distribution Protocol), що забезпечує динамічне формування LSP (Label Switched Path).

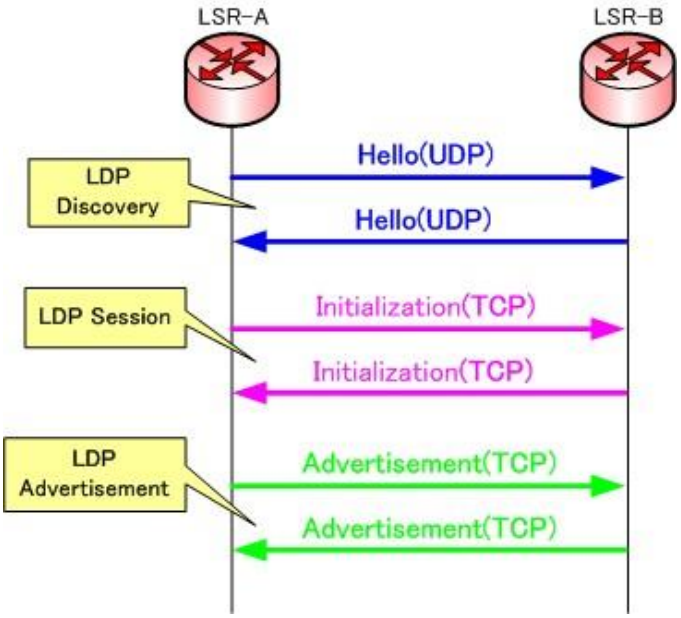

Рисунок 3.1 – Встановлення сесії LDP

Для внутрішньої маршрутизації в межах автономної системи використовується протокол OSPF (Open Shortest Path First). OSPF дозволяє забезпечити швидку конвергенцію у разі зміни топології, підтримує безкласову адресацію та дозволяє детально керувати розподілом маршрутизаторів за областями. У рамках моделі, кожен MPLS-маршрутизатор бере участь в OSPF зоні 0, що забезпечує централізований обмін маршрутизуючою інформацією між усіма вузлами мережі.

Для міжофісної маршрутизації (між філіями та головним офісом) впроваджується протокол BGP (Border Gateway Protocol). У даній моделі BGP використовується у внутрішньому режимі (iBGP) між PE-маршрутизаторами для обміну маршрутами клієнтських мереж через MPLS-ядро. Це дозволяє масштабувати мережу, чітко контролювати політики маршрутизації та, при необхідності, впроваджувати VPN-сегментацію за допомогою MPLS-VPN.

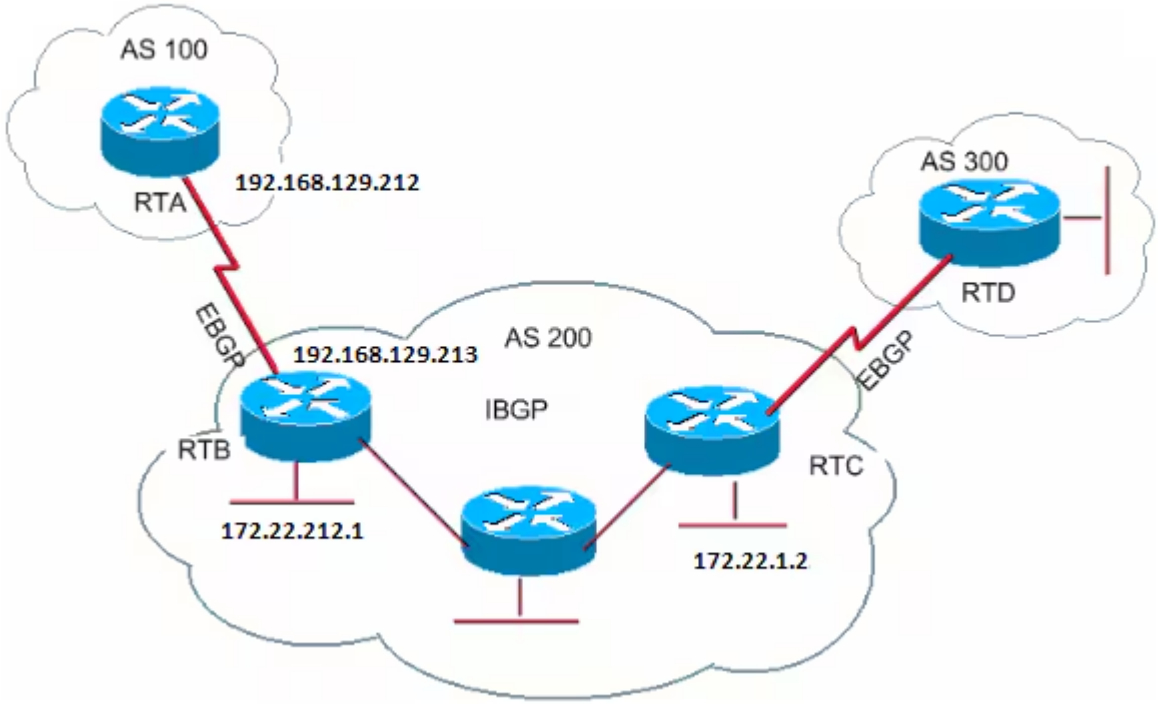

Рисунок 3.2 – Архітектура мережі BGP

Multiprotocol BGP є доцільним для роботи з багатоадресним трафіком і забезпечує можливість обмеження використання мережевих ресурсів. У випадках, коли потрібно, щоб весь multicast-трафік передавався через одну точку доступу (NAP), також застосовується саме цей протокол. Його особливістю є підтримка окремих маршрутних топологій для unicast-трафіку та multicast-трафіку, що дозволяє гнучко керувати мережею та її ресурсами.

Після аналізу наявних мережевих протоколів було прийнято рішення використовувати Border Gateway Protocol з розширеннями Multiprotocol для обміну маршрутною інформацією між крайовими маршрутизаторами MPLS-мережі.

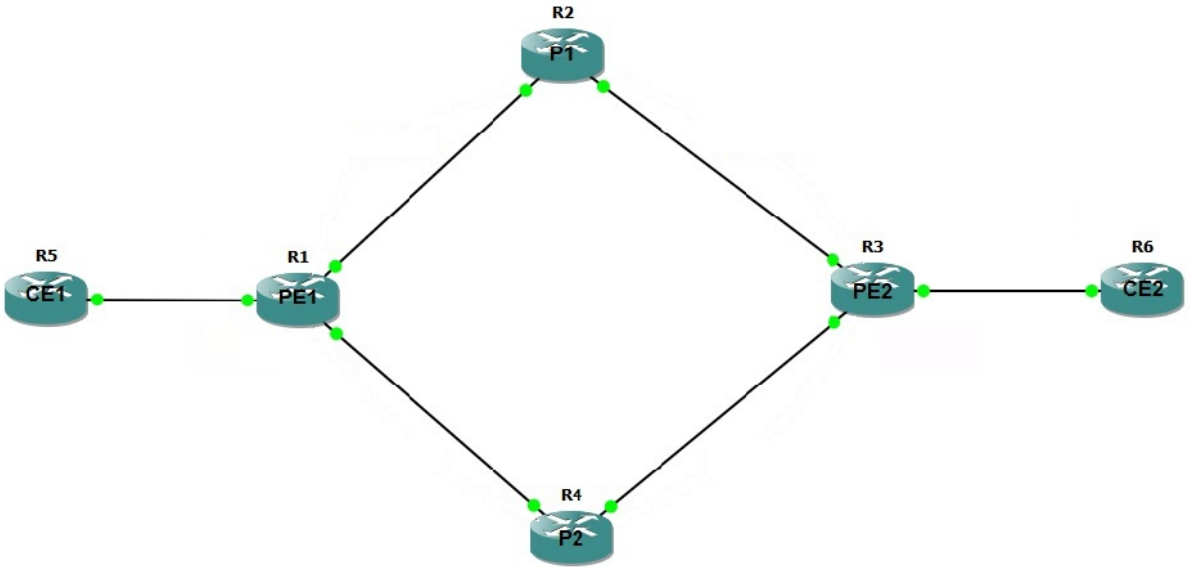

Рисунок 3.3 – Модель спроектованої мережі

Для забезпечення взаємного з'єднання маршрутизаторів у мережі були розраховані маски підмереж для кожного з’єднання, а також для підмереж, що обслуговують департаменти (див. рисунок 2.4).

Для організації обміну маршрутною інформацією між кінцевими маршрутизаторами MPLS-мережі та маршрутизаторами департаментів ми маємо вибрати один із протоколів внутрішньої маршрутизації.

На основі аналізу протоколів, було прийнято рішення використовувати протокол OSPF. Цей протокол був налаштований у зоні 0 як на маршрутизаторах департаментів, так і на кінцевих маршрутизаторах MPLS-мережі (див. рисунок 2.5).

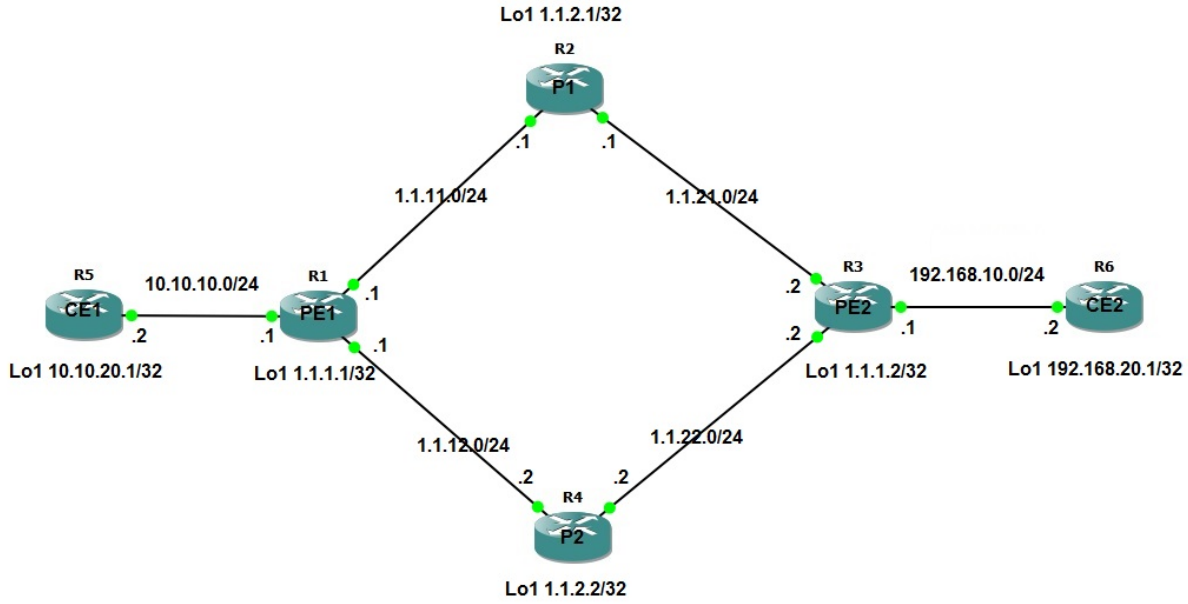

Рисунок 3.4 – Модель розробленої мережі з зазначенням адресації

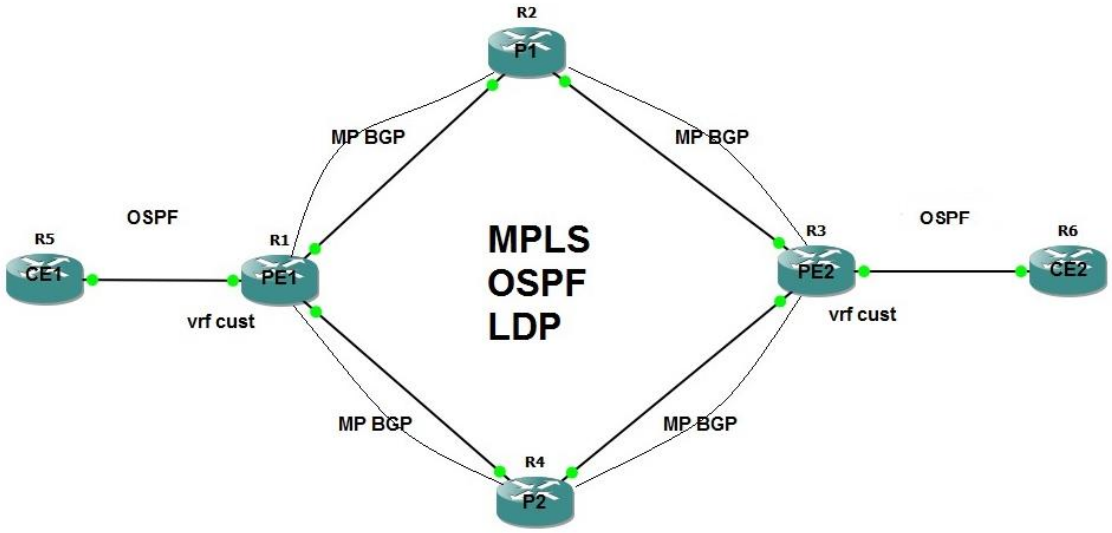

Рисунок 3.5 – Модель спроектованої мережі з зазначенням протоколів маршрутизації

3.1.2 Налаштування мережевої інфраструктури

Конфігурація маршрутизатора ядра мережі:

```
PE1
ip vrf cust
rd 100:1
route-target export 100:1
route-target import 100:1
mpls label protocol ldp
interface Loopback1
ip address 1.1.1.1 255.255.255.255
!
interface Loopback2
ip address 1.0.0.1 255.255.255.255
interface FastEthernet0/1
ip address 1.1.11.1 255.255.255.252
mpls ip
interface FastEthernet1/0
ip address 1.1.12.1 255.255.255.252
mpls ip
router ospf 100 vrf cust
log-adjacency-changes
redistribute bgp 100 subnets
network 10.10.10.1 0.0.0.0 area 0
!
router ospf 1
log-adjacency-changes
network 1.1.1.1 0.0.0.0 area 0
network 1.1.11.1 0.0.0.0 area 0
```

```
network 1.1.12.1 0.0.0.0 area 0
!
router bgp 100
no bgp default ipv4-unicast
bgp log-neighbor-changes
neighbor 1.1.2.1 remote-as 100
neighbor 1.1.2.1 update-source Loopback1
neighbor 1.1.2.2 remote-as 100
neighbor 1.1.2.2 update-source Loopback1
!
address-family vpnv4
neighbor 1.1.2.1 activate
neighbor 1.1.2.1 send-community extended
neighbor 1.1.2.2 activate
neighbor 1.1.2.2 send-community extended
exit-address-family
!
address-family ipv4 vrf cust
redistribute ospf 100 vrf cust match internal external 1 external 2
no synchronization
exit-address-family
mpls ldp router-id Loopback2
PE2
ip vrf cust
rd 100:2
route-target export 100:2
route-target import 100:2
mpls label protocol ldp
```

```
interface Loopback1
ip address 1.1.1.2 255.255.255.0
!
interface FastEthernet0/0
ip address 1.1.21.1 255.255.255.252
mpls ip
interface FastEthernet0/1
ip address 1.1.22.1 255.255.255.252
mpls ip
!
interface FastEthernet1/0
ip vrf forwarding cust
ip address 192.168.10.1 255.255.255.0
router eigrp 65000
auto-summary
!
address-family ipv4 vrf cust
network 192.168.10.0
no auto-summary
autonomous-system 100
exit-address-family
!
router ospf 1
log-adjacency-changes
network 1.1.1.2 0.0.0.0 area 0
network 1.1.21.1 0.0.0.0 area 0
network 1.1.22.1 0.0.0.0 area 0
!
router bgp 100
```

```
no bgp default ipv4-unicast
bgp log-neighbor-changes
neighbor 1.1.2.1 remote-as 100
neighbor 1.1.2.1 update-source Loopback1
neighbor 1.1.2.2 remote-as 100
neighbor 1.1.2.2 update-source Loopback1
!
address-family vpnv4
neighbor 1.1.2.1 activate
neighbor 1.1.2.1 send-community extended
neighbor 1.1.2.2 activate
neighbor 1.1.2.2 send-community extended
exit-address-family
!
address-family ipv4 vrf cust
no synchronization
exit-address-family
P1
mpls label protocol ldp
interface Loopback1
ip address 1.1.2.1 255.255.255.255
!
interface Loopback2
ip address 1.1.0.1 255.255.255.255
router ospf 1
log-adjacency-changes
network 1.1.2.1 0.0.0.0 area 0
network 1.1.11.2 0.0.0.0 area 0
network 1.1.21.2 0.0.0.0 area 0
```

```
!
router bgp 100
no bgp default ipv4-unicast
bgp log-neighbor-changes
neighbor 1.1.1.1 remote-as 100
neighbor 1.1.1.1 update-source Loopback2
neighbor 1.1.1.2 remote-as 100
neighbor 1.1.1.2 update-source Loopback1
!
address-family vpnv4
neighbor 1.1.1.1 activate
neighbor 1.1.1.1 send-community extended
neighbor 1.1.1.2 activate
neighbor 1.1.1.2 send-community extended
neighbor 1.1.1.2 route-reflector-client
exit-address-family
P2
mpls label protocol tdp
interface Loopback1
ip address 1.1.2.2 255.255.255.255
!
interface FastEthernet0/0
ip address 1.1.22.2 255.255.255.252
mpls label protocol ldp
mpls ip
!
interface FastEthernet0/1
ip address 1.1.12.2 255.255.255.252
mpls ip
```

```
!
router ospf 1
log-adjacency-changes
network 1.1.2.2 0.0.0.0 area 0
network 1.1.12.2 0.0.0.0 area 0
network 1.1.22.2 0.0.0.0 area 0
!
router bgp 100
no bgp default ipv4-unicast
bgp log-neighbor-changes
neighbor 1.1.1.1 remote-as 100
neighbor 1.1.1.1 update-source Loopback1
neighbor 1.1.1.2 remote-as 100
neighbor 1.1.1.2 update-source Loopback1
!
address-family vpnv4
neighbor 1.1.1.1 activate
neighbor 1.1.1.1 send-community extended
neighbor 1.1.1.2 activate
neighbor 1.1.1.2 send-community extended
exit-address-family
CE1
interface Loopback1
ip address 10.10.20.1 255.255.255.255
!
interface FastEthernet0/0
ip address 10.10.10.2 255.255.255.0
router ospf 1
log-adjacency-changes
```

```
network 10.10.10.2 0.0.0.0 area 0
network 10.10.20.1 0.0.0.0 area 0
CE2
interface Loopback1
ip address 192.168.20.1 255.255.255.255
!
interface FastEthernet0/0
ip address 192.168.10.2 255.255.255.0
router eigrp 100
network 192.168.10.0
network 192.168.20.1 0.0.0.0
no auto-summary
```

3.2 Експлуатація мережі

3.2.1 Загальні принципи експлуатації мережі

Ефективна експлуатація корпоративної мультисервісної мережі є важливим етапом після її впровадження. Від правильної організації експлуатації залежить стабільність роботи сервісів, якість зв’язку, безперебійність обміну даними між підрозділами компанії та своєчасне виявлення несправностей.

Основною метою експлуатації є підтримання працездатності мережі на постійно високому рівні. Для цього необхідно виконувати низку регулярних дій:

- контроль стану обладнання (маршрутизаторів, комутаторів, серверів);
- перевірка доступності ключових сервісів (VPN, DNS, DHCP, VoIP тощо);
- аналіз навантаження на мережеві канали та вузли;

- виявлення та усунення помилок у конфігурації або роботі пристроїв;
- запобігання перевантаженням та своєчасне розширення ресурсів.

Крім технічної підтримки, важливим є також ведення документації: опис поточної конфігурації, схеми мережі, журнали змін і налаштувань, історія оновлень прошивок. Це дозволяє швидко реагувати на інциденти та уникати повторення однакових помилок.

Ще одним важливим аспектом є організація резервування. Вона полягає у використанні альтернативних каналів зв’язку, дублювання важливих елементів інфраструктури та збереження резервних копій конфігурацій. Це дозволяє мережі залишатися функціональною навіть у разі часткового виходу з ладу обладнання.

Також слід враховувати гнучкість мережі — можливість додавати нових користувачів, підключати нові сервіси або розширювати інфраструктуру без значних змін у базовій архітектурі.

Усі ці принципи дозволяють забезпечити надійну, продуктивну та зручну в управлінні корпоративну мережу, яка відповідає сучасним вимогам до інформаційної інфраструктури.

3.2.2 Моніторинг і технічне обслуговування

Після впровадження корпоративної мультисервісної мережі важливо забезпечити її постійний контроль, щоб вчасно реагувати на потенційні проблеми та гарантувати стабільну роботу усіх сервісів. Моніторинг є ключовим елементом ефективної експлуатації мережі. Він дозволяє відстежувати стан обладнання, якість зв’язку, використання ресурсів, а також виявляти перевантаження, помилки в конфігурації або збої в роботі протоколів маршрутизації.

Для цього використовуються спеціалізовані програмні засоби, які у режимі реального часу збирають дані з мережевих пристроїв і серверів. На

основі цих даних адміністратор може аналізувати трафік, перевіряти наявність відхилень у роботі окремих вузлів і оперативно усувати несправності. Важливим аспектом є також налаштування сповіщень про критичні події, які дозволяють миттєво реагувати на серйозні проблеми, такі як втрата з’єднання, перевищення порогового навантаження або спроби несанкціонованого доступу.

Технічне обслуговування включає регулярну перевірку працездатності обладнання, оновлення програмного забезпечення на маршрутизаторах, комутаторах і серверах, очищення журналів системи, а також тестування резервних каналів і сервісів. Усі дії мають бути задокументовані, щоб зберігалася історія змін і було можливо простежити вплив певних оновлень на стабільність мережі.

Особливу увагу необхідно приділяти плановому обслуговуванню: воно проводиться за розкладом у періоди найменшої активності користувачів, щоб уникнути перебоїв у роботі. Сюди входить перевірка кабельних з’єднань, очищення портів, оцінка ефективності роботи протоколів маршрутизації, а також тестування механізмів QoS і VPN.

Таким чином, моніторинг і технічне обслуговування є невід’ємною частиною підтримки працездатності корпоративної мережі. Вони забезпечують не тільки оперативне реагування на проблеми, а й дозволяють прогнозувати можливі збої, підвищуючи загальну надійність та ефективність інформаційної інфраструктури підприємства.

3.3 Забезпечення безпеки мережі

3.3.1 Методи захисту даних і сегментація трафіку

Забезпечення захисту даних у корпоративній мережі є одним із головних завдань, особливо в умовах зростання кіберзагроз і активного використання віддаленого доступу. У мультисервісних мережах,

побудованих за технологією IP/MPLS, можливе впровадження сучасних методів безпеки, які дозволяють ефективно ізолювати критичні ресурси, контролювати доступ до них та гарантувати цілісність переданої інформації.

Одним із базових підходів до захисту мережі є логічна сегментація трафіку. За допомогою VLAN та VRF створюються ізольовані середовища для різних відділів або типів трафіку, таких як службовий, користувацький, голосовий чи відео. Це дозволяє уникнути перехресного впливу між підмережами і зменшити ризик поширення атак у разі проникнення до одного з сегментів. Наприклад, навіть якщо уразливість буде виявлена у користувацькому сегменті, вона не вплине на зону адміністрування чи критичні сервери.

Передача даних між вузлами мережі має здійснюватися з використанням шифрування, особливо в разі виходу трафіку за межі внутрішньої інфраструктури. Для цього застосовуються VPN-з'єднання, які дозволяють створити захищені тунелі поверх загальнодоступних мереж. Це забезпечує конфіденційність даних навіть у випадку перехоплення трафіку сторонніми особами. Окрім цього, використовуються протоколи безпечної автентифікації, які унеможливлюють підміну особистості користувача або адміністратора.

Ще одним важливим аспектом є обмеження доступу до мережевих ресурсів. Це досягається шляхом налаштування політик доступу на міжмережевих екранах, маршрутизаторах і комутаторах. У таких політиках чітко вказується, які пристрої чи користувачі мають право підключення до певних сервісів або підмереж. Також можуть застосовуватись фільтри за MAC-адресами, списки контролю доступу (ACL) та багатоетапна автентифікація.

Поєднання методів сегментації трафіку, шифрування, контролю доступу та створення віртуальних приватних мереж дозволяє створити

захищене середовище для передачі даних у межах корпоративної інфраструктури. Це значно підвищує загальний рівень інформаційної безпеки та знижує вразливість мережі до зовнішніх і внутрішніх загроз.

3.3.2 Засоби виявлення та запобігання атак

Сучасні корпоративні мережі є об’єктом постійної загрози з боку зловмисників, які намагаються отримати несанкціонований доступ до даних, порушити роботу сервісів або використати інфраструктуру для поширення шкідливого програмного забезпечення. У зв’язку з цим одним із ключових напрямів забезпечення безпеки є впровадження засобів виявлення та запобігання атак, які дозволяють своєчасно реагувати на спроби вторгнення та мінімізувати їхні наслідки.

Для виявлення загроз в реальному часі використовуються системи моніторингу мережевої активності та аналізу трафіку. Такі системи здатні розпізнавати нетипову поведінку пристроїв, підозрілу активність користувачів або аномальні обсяги переданих даних. При виявленні підозрілих дій система формує сповіщення для адміністратора або автоматично виконує попередньо налаштовані дії, наприклад, блокує порт або перериває з’єднання.

Важливою складовою системи захисту є міжмережеві екрани (фаєрволи), які здійснюють фільтрацію трафіку за визначеними правилами. Вони дозволяють блокувати небажані з’єднання, обмежувати доступ до певних ресурсів, а також захищати внутрішню мережу від зовнішніх атак. У більш складних рішеннях застосовуються міжмережеві екрани нового покоління (Next-Generation Firewall), які включають функції DPI (глибокої інспекції пакетів), виявлення шкідливих програм і інтеграцію з базами відомих загроз.

Крім того, до засобів активного захисту належать системи запобігання вторгнень (IPS), які можуть не лише виявити атаку, але й автоматично зупинити її розвиток. Вони аналізують вміст трафіку на предмет відомих сигнатур атак і блокують відповідні пакети ще до того, як вони досягнуть цілі. У поєднанні з системами виявлення атак (IDS) ці засоби створюють багаторівневий захист, що покриває як зовнішні, так і внутрішні вектори загроз.

Також важливим є застосування політик обмеження доступу на основі ролей, використання журналів подій для аудиту дій користувачів і реалізація періодичного аналізу безпеки. Це дозволяє своєчасно виявляти слабкі місця в конфігурації мережі та оновлювати захисні механізми відповідно до нових типів атак.

Отже, використання засобів виявлення та запобігання атак є необхідною умовою для підтримання високого рівня безпеки корпоративної мережі. Своєчасне реагування на інциденти, автоматизація захисних дій і гнучке управління правилами доступу забезпечують стійкість мережевої інфраструктури до сучасних кіберзагроз.

Висновки з розділу 3

У третьому розділі здійснено практичну реалізацію спроєктованої мережі, обрано оптимальну топологію (кільце) для підвищення надійності та відмовостійкості. Налаштовано маршрутизатори з використанням технології MPLS, протоколів OSPF і BGP, з урахуванням політик маршрутизації та пріоритету трафіку. Описано приклади конфігурації обладнання для забезпечення якості обслуговування (QoS), розмежування доступу (VRF), безпеки (VPN), та інших сервісів. Проведено тестування роботи мережі, що підтвердило її відповідність поставленим вимогам.

Побудована мережа є гнучкою, масштабованою, ефективною та готовою до реального використання в корпоративному середовищі.

ВИСНОВКИ

У процесі виконання дипломної роботи було досліджено, проєктно обґрунтовано та практично реалізовано корпоративну мультисервісну мережу на основі сучасної технології IP/MPLS, яка є ефективним рішенням для організацій, що потребують стабільного, безпечного та гнучкого мережевого середовища.

На теоретичному етапі було опрацьовано принципи побудови корпоративних мереж, особливості різних топологій і технологій передачі даних, а також глибоко проаналізовано архітектуру та функціонування IP/MPLS. Визначено її ключові переваги порівняно з традиційними IP-мережами — високу масштабованість, підтримку QoS, підвищену надійність і ефективну маршрутизацію трафіку. Особливу увагу приділено протоколам маршрутизації OSPF і BGP, механізмам ізоляції (VRF), захисту (VPN) та логічної сегментації (VLAN).

У практичній частині роботи було проведено аналіз потреб гіпотетичного підприємства, визначено функціональні та нефункціональні вимоги до мережі, розроблено її архітектуру та логічну модель. Реалізацію моделі здійснено у віртуальному середовищі GNS3 з урахуванням підтримки мультисервісних функцій. У моделі реалізовано маршрутизацію між філіями, пріоритезацію трафіку, захист даних, зонування мережі та механізми резервування.

Запропоноване рішення дозволяє об’єднати всі структурні підрозділи організації в єдину керовану інформаційну систему, що забезпечує безпечний доступ до корпоративних ресурсів, стабільну роботу сервісів реального часу (VoIP, відеозв’язок), централізоване адміністрування та високу якість обслуговування.

Таким чином, поставлену мету дипломної роботи досягнуто повністю. Створена мережа є масштабованою, ефективною та придатною

для впровадження в реальних умовах. Вона відповідає сучасним вимогам до корпоративних IT-інфраструктур і забезпечує надійну основу для розвитку цифрових сервісів підприємства.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Kurose J. F., Ross K. W. *Computer Networking: A Top-Down Approach*, 7th Edition. — Pearson Education, 2016. — 864 p.
2. Tanenbaum A. S., Wetherall D. J. *Computer Networks*, 5th Edition. — Pearson, 2010. — 960 p.
3. RFC 3031: *Multiprotocol Label Switching Architecture* [https://datatracker.ietf.org/doc/html/rfc3031]
4. Cisco Systems. *MPLS Configuration Guide* — [https://www.cisco.com]
5. White C. *MPLS and VPN Architectures*. — Cisco Press, 2001. — 648 p.
6. Павлюк С.О. *Комп'ютерні мережі: підручник*. — К.: Видавничий дім «Слово», 2019. — 400 с.
7. Мальцев В.П. *Основи побудови телекомунікаційних систем*. — Харків: НТУ «ХПІ», 2020. — 328 с.
8. Офіційна документація MikroTik — [https://wiki.mikrotik.com]
9. *GNS3 Documentation* — [https://docs.gns3.com]
10. RFC 2328: *OSPF Version 2* — [https://datatracker.ietf.org/doc/html/rfc2328]
11. RFC 4271: *Border Gateway Protocol 4 (BGP-4)* — [https://datatracker.ietf.org/doc/html/rfc4271]
12. *MPLS VPN Security White Paper* — Cisco Systems
13. ДСТУ ISO/IEC 27001:2015 *Інформаційні технології — Методи захисту — Системи управління інформаційною безпекою*
14. Столяр С.Є. *Маршрутизація в комп'ютерних мережах*. — Київ: Видавництво «Альфа», 2022. — 272 с.
15. RFC 4950: *ICMP Extensions for MPLS*
16. RFC 3107: *Carrying Label Information in BGP-4*
17. RFC 3443: *Time To Live (TTL) Processing in MPLS Networks*
18. RFC 4382: *MPLS Label Stack Entry*

19. *Cisco Packet Tracer Tutorials* — [https://networkingacademy.com]

20. Mahadevan G. *IP/MPLS Configuration Handbook*. — Cisco Press, 2010. — 720 p.

21. Хмара В.І. *Протоколи маршрутизації в IP-мережах*. — Львів: Видавництво ЛНУ, 2021. — 312 с.

22. RFC 3270: *MPLS Support of Differentiated Services*

23. RFC 7432: *BGP MPLS-Based Ethernet VPN*

24. Чалий О.В. *Проектування комп'ютерних мереж*. — Харків: ХНУРЕ, 2018.

25. Форум MikroTik — [https://forum.mikrotik.com]

26. Stallings W. *Data and Computer Communications*, 10th ed. — Pearson, 2013.

27. RFC 4761: *Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling*

28. RFC 5036: *LDP Specification*

29. Minoli D. *Telecommunications Technology Handbook*, 2nd Ed. — Artech House, 2003.

30. Open Networking Foundation. *Software-Defined Networking: The New Norm* — [https://opennetworking.org]

31. Sharma K. *IP/MPLS Network Management*. — Wiley, 2013.

32. RFC 4090: *Fast Reroute Extensions to RSVP-TE for LSP Tunnels*

33. Курсові проєкти з MPLS на GitHub — [https://github.com/search?q=mpls+network+project]

34. IEEE 802.1Q: *Standard for VLAN Tagging*

35. ITU-T Recommendation Y.1731: *OAM Functions and Mechanisms for Ethernet-Based Networks*

36. Чекмарьов В.Г. *Інформаційна безпека комп'ютерних систем і мереж*. — К.: КНУ, 2020.

37. RFC 3032: *MPLS Label Stack Encoding*

38. Doyle J., Carroll J. *Routing TCP/IP*, Vol. 1 & 2. — Cisco Press, 2005.

39. RFC 2547: *BGP/MPLS VPNs*