ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ
ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА ТЕХНІЧНИХ СИСТЕМ КІБЕРЗАХИСТУ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «Захист тимчасового каналу передачі даних у відкритій мережі загального користування»

на здобуття освітнього ступеня магістра

зі спеціальності __125 - Кібербезпека та захист інформації»
(код, найменування спеціальності)
освітньо-професійної програми Технічні системи інформаційного та кібернетичного захисту

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

_____ Дмитро РИМАРЧУК

Виконав: здобувач вищої освіти групи СЗДМ-61

_____ РИМАРЧУК Дмитро

Керівник: _____ ПЕПА Юрій
(ПРІЗВИЩЕ, Ім’я)

Рецензент: _____
(ПРІЗВИЩЕ, Ім’я)

Київ 2026

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ
ТА ЗАХИСТУ ІНФОРМАЦІЇ

Кафедра ___Технічних систем кіберзахисту_____
Ступінь вищої освіти ____магістр_____
Спеціальність ___Кібербезпека та захист інформації_____
Освітньо-професійна програма _Технічні системи інформаційного та кібернетичного захисту

ЗАТВЕРДЖУЮ
Завідувач кафедри ТСКБ
_____Олександр ТУРОВСЬКИЙ

«____» _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

РИМАРЧУКУ Дмитру Олександровичу
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: «Захист тимчасового каналу передачі даних у відкритій мережі загального користування».
Керівник кваліфікаційної роботи: ПЕПА Юрій, к.т.н., доцент.
(ПРІЗВИЩЕ Ім'я, науковий ступінь, вчене звання)

Затверджена наказом Державного університету інформаційно-комунікаційних технологій від «30» жовтня 2025 р. № 467

2. Строк подання кваліфікаційної роботи: 15.12.2025 р.

3. Вихідні дані до кваліфікаційної роботи:
Способи витоку інформації через радіоканал в ефір.
Радіомоніторинг на основі спектроаналізатору.
Програмно-апаратний комплекс моніторингу радіоефіру на основі SDR приймача.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити):
1. Провести аналіз способів моніторингу радіоефіру.
2. Аналіз методів оцінки небезпечних сигналів та властивостей цих сигналів.
3. Практичні експериментальні дослідження виявлення за спектрами небезпечних сигналів.

5. Перелік графічного матеріалу: Презентаційний матеріал на слайдах

6. Дата видачі завдання 15.10.2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Аналіз літературних джерел		
2	Написання першого розділу роботи		
3	Написання другого розділу роботи		
4	Написання третього розділу роботи		
5	Написання висновків по роботі		
6	Підготовка демонстраційних матеріалів		
7	Підготовка доповіді		

Здобувач вищої освіти _____ Дмитро РИМАРЧУК
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник роботи _____ Юрій ПЕПА
(підпис)

РЕФЕРАТ

Пояснювальна записка: 70 с., 57 рис., 7 табл., 17 джерел.

Об'єкт дослідження – мережа на основі технології MPLS

Предмет дослідження – алгоритм ефективності тунелювання MPLS

Мета роботи – аналіз, перевірка та обґрунтуванні алгоритму для визначення доцільності та ефективності побудови тунелю в мережі MPLS.

Методи досліджень – емпіричний аналіз, формалізація, розрахунки. та порівняння.

В останні кілька років широке поширення набула технологія багатопротокольної комутації по мітках – Multi Protocol Label Switching (MPLS). Ця технологія впроваджується як в корпоративних мережах, так і в мережах загального користування Основна перевага технології MPLS полягає в більш високому ступені масштабування – розширюваності, можливості функціонального нарощування системи шляхом додавання нових елементів або заміни застарілих на більш досконалі без зміни архітектури. Такими властивостями повинна володіти, перш за все, транспортна мережа.

В роботі було проведено аналіз ефективності тунелювання MPLS, також особливості даної технології Проаналізовано алгоритм ефективності створення тунелю в мережі та проведено розрахунки в середовищі Mathcad. Продемонстровано, що ефективність застосування технології MPLS при різних навантаженнях залежить від кількості вузлів. Виконано побудову та налаштування мережі в симуляторі GNS3. Налаштовано IP-мережу на основі протоколу динамічної маршрутизації OSPF, повех якої застосовані налаштування MPLS мережі.

Апробація:

Д.О. Римарчук, А.О. Довгополий, ВИЯВЛЕННЯ ТА АНАЛІЗ АУДІО СПЕКТРУ. *Всеукраїнської науково- практичної конференція: Актуальні проблеми безпеки інформаційно-телекомунікаційних систем*. м. Київ, 05 листопада 2025 року, Київ: РВЦ ДУІКТ. – 2025. С.51-52. https://duikt.edu.ua/uploads/p_2779_72486260.pdf

Ключові слова:

MPLS, ТУНЕЛЬ, ЕФЕКТИВНІСТЬ LSP, ТУНЕЛЮВАННЯ, LSR, МЕРЕЖА, АЛГОРИТМ, МАРШРУТИЗАТОР, МІТКА.

ABSTRACT

The report contains: 70 p., 57 figures, 7 tables, 17 sources.

The research object is the network based on MPLS technology

The subject of the research is the MPLS tunneling efficiency algorithm

An aim of work is to analyze, validate and justify the algorithm to determine the feasibility and effectiveness of tunneling in the MPLS network.

Methods of researches are empirical analysis, formalization, calculations. and comparison.

The over past few years multi-protocol label switching technology – Multi Protocol Label Switching (MPLS) has become widespread. This technology is implemented both in corporate and public networks The main advantage of MPLS technology is its greater scalability - extensibility, the ability to functionally scale the system by adding new elements or replacing outdated ones with more sophisticated architecture. These properties must have, above all, the transport network.

The analysis of MPLS tunneling was carried out in this work, also the features of this technology The algorithm of network tunneling efficiency was analyzed and the calculations were performed in Mathcad environment. It is demonstrated that the effectiveness of using MPLS technology at different loads depends on the number of nodes. The GNS3 simulator is built and configured. Configured an IP network based on OSPF dynamic routing protocol, to which MPLS network settings are applied.

MPLS, TUNNEL, LSP EFFICIENCY, TUNNELING, LSR, NETWORK, ALGORITHM, ROUTE, LABEL

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ

AGN – Aggregation Network – вузли агрегації мережі (мультисвіч)

ATM – Asynchronous Transfer Mode – асинхронній спосіб передачі даних

BGP – Border Gateway Protocol

CN – Core Network – ядро мережі – центральна система мережі, яка призначена для зберігання абонентських даних, і відповідає за встановлення з'єднань, аутентифікацію абонентів

CSPF – Constrained Shortest Path First – алгоритм обчислення найкоротшого шляху з урахуванням обмежень

Egress LSR – точка виходу з мережі MPLS

ERO – Explicit Route Object – Список вузлів складений CSPF

FEC – Forwarding Equivalence Class – клас еквівалентності пересилання

Frame Relay – протокол канального рівня, оснований на ретрансляції кадрів

IGP – Interior Gateway Protocol – протокол внутрішнього шлюзу

Ingress LSR – точка входу в мережу MPLS

IP – Internet Protocol – мережевий протокол

IPSec – IP Security – набір протоколів для захисту даних

ISIS – протокол маршрутизації проміжних систем

L2TP – Layer 2 Tunneling Protocol – протокол тунелювання канального рівня

LDP – Label Distribution Protocol – протокол, основним завданням якого є швидкий розподіл міток

LER – Label Edge Router – граничний вузол MPLS

LSP – Label Switched Path – віртуальний канал, тунель, шлях в протоколі MPLS

LSR – Label Switch Router – маршрутизатор із запущеною на ньому технологією MPLS

MPLS – multiprotocol label switching – багатопротокольна комутація за мітками

OSPF – Open Shortest Path First – протокол динамічної маршрутизації

PPTP – Point-to-Point Tunneling Protocol – тунельний протокол типу точка-точка.

PWE – Pseudowire Emulation

QoS – Quality of Service – технологія надання різним класам трафіку різних пріоритетів в обслуговуванні

RSVP-TE – Resource ReSer Vation Protocol-Traffic Engineering – протокол розподілення міток

TE – Traffic Engineering – технологія управління напрямом проходження трафіку

TED – Traffic Engineering Database – топологія мережі з урахуванням ресурсів

TCP – Transmission Control Protocol – протокол передачі даних

TDM – Time Division Multiplexing – часове мультиплексування

V1(N) – час перебування пакету в LSP-тунелі з N вузлів

V2(N) – час перебування пакету в мережі з N вузлів

VPN – Virtual Private Network – Віртуальна приватна мережа

ВСТУП

З плином часу безліч мереж різних компаній стрімко зростали і продовжують розвиватися й сьогодні. Кожного дня розвивалися магістральні лінії в різних містах, клієнтські бази, поглиблювалися знання інженерів.

Але час не стоїть на місці. Послуги широкосмугового доступу – це важливо і необхідно на сучасних мережах, але є ще значна частина ринку корпоративних клієнтів, яким необхідний VPN.

У зв'язку зі збільшенням обсягу «пакетного трафіку» (систем універсального доступу, додатків, орієнтованих на клієнта) звичні транспортні системи з часовим поділом каналів (TDM) перестають справлятися з передачею даних, тому виникає необхідність в новій транспортній платформі, здатній передавати трафік із заданою якістю обслуговування.

В останні кілька років широке поширення набула технологія багатопротокольної комутації по мітках – Multi Protocol Label Switching (MPLS). Ця технологія впроваджується як в корпоративних мережах, так і в мережах загального користування. Основна перевага технології MPLS полягає в більш високому ступені масштабування – розширюваності, можливості функціонального нарощування системи шляхом додавання нових елементів або заміни застарілих на більш досконалі без зміни архітектури. Такими властивостями повинна володіти, перш за все, транспортна мережа. Основна область застосування технології IP/MPLS – ядро транспортної мережі.

Подальше збільшення складності проблем управління транспортними мережами IP/MPLS, обумовлена зростанням вимог по обслуговуванню мультисервісного трафіку (мова, відео, Web-додатки). Найважливішим важелем такого управління є створення тунелів в транспортній мережі, що забезпечують передачу трафіку певного типу із заданою якістю обслуговування – QoS.

Технологія MPLS основана на тому, що дані пересилаються за допомогою міток, які присвоюються кожному пакету. Внутрішні вузли ядра мережі, що підтримують MPLS, не аналізують вміст пакетів. Таким чином, IP-адреса одержувача не розглядається, що дає можливість MPLS створити ефективний механізм інкапсуляції для передачі приватного трафіку, що передається по магістралі оператора. В даній технології були сформовані протоколом розподілу

міток, LDP – Label Distribution Protocol, маршрути просування пакетів від відправників до одержувачів LSP – Label Switched Path, LSP, які в свою чергу нерідко розглядають як тунелі через всю мережу MPLS або через її окрему частину. Основою будь-якого рішення є використання LSP-тунелю для просування даних між фронтальними маршрутизаторами постачальника послуг. Присвоюючи мітки відповідним пакетам, LSR надійно відділяють VPN-потоки від інших даних, що передаються по магістралі. Такий поділ являє собою ключовий механізм, за допомогою якого MPLS може підтримувати такі характеристики VPN-тунелювання, як інкапсуляція даних незалежно від застосовуваних протоколів, забезпечення необхідного рівня QoS, надійну комутацію та автоматичне перенаправлення LSP-тунеля при виході з ладу одного або декількох вузлів мережі, без втручання адміністратора. Дану тему висвітлював Захватов М. А. у своїй роботі, у видавництві Cisco Systems.

Мета роботи полягає в аналізі, перевірці та обґрунтуванні алгоритму для визначення доцільності та ефективності побудови тунелю в мережі MPLS. Створення фрагменту мережі, та налаштування MPLS на кожному вузлі.

Для вирішення поставленої задачі, в першому розділі було проведено аналіз тунелювання MPLS, виділено основні елементи мережі, окреслено переваги та недоліки. У другому розділі проаналізовано застосування технології. У третьому розділі проаналізовано алгоритм ефективності побудови тунелю. У зв'язку з цим розглянуто процес тунелювання та побудовано математичну модель. В четвертому розділі, застосовуючи проаналізований алгоритм, були проведені розрахунки в середовищі Mathcad. У п'ятому розділі побудовано фрагмент мережі з десяти вузлів. Налаштовано технологію MPLS. Продемонстровано команди, що дозволяють переглянути призначення MPLS міток для кожного маршрутизатора, сусідніх вузлів та показано один з побудованих LSP-тунелів.

Окремі результати роботи доповідалися на Всеукраїнському конкурсі студентських наукових робіт зі спеціальності «Телекомунікації» та на конференціях «Перспективи розвитку інфокомунікацій та інформаційно-вимірювальних технологій» в рамках 22-го та 23-го Міжнародних форумів «Радіотехніка і молодь в XXI столітті». Також окремі результати були представлені на П'ятій міжнародній науковій конференції студентів, магістрів, аспірантів «Інформатика, управління та штучний інтелект».

1 АНАЛІЗ ТУНЕЛІВ MPLS

1.1 Особливості технології MPLS

Використання технології інкапсуляції, або тунелювання є найбільш універсальним способом побудови VPN. Тунелювання в загальному випадку застосовується для того, щоб передавати пакети однієї мережі (первинної) по каналах зв'язку іншої (вторинної), протоколи яких не сумісні. Для цього пакети первинної мережі (дані і протоколи) інкапсулюються в пакети вторинної мережі, і можуть бути визначені як дані.

Таким чином, пакет просувається маршрутизаторами ядра мережі тільки на підставі зовнішнього заголовка, без інспекції вмісту оригінального пакету. Далі наводиться короткий опис найбільш поширених рішеннь по тунелюванні при створенні віртуальних приватних мереж.

Протокол PPTP (Point-to-Point Tunneling Protocol) дозволяє інкапсулювати (упаковувати або приховувати від використання) пакети PPTP в пакети протоколу Internet Protocol (IP) і передавати їх по мережах IP (в тому числі й Інтернет). Протокол PPTP забезпечує безпечну передачу даних від віддаленого клієнта до єдиного сервера підприємства шляхом створення в мережі TCP/IP приватної віртуальної мережі. Протокол PPTP може також застосовуватися для організації тунелю між двома мережами локального типу.

Протокол L2TP – Layer 2 Tunneling Protocol – протокол тунелювання канального рівня, який дозволяє організовувати VPN із заданими пріоритетами доступу, однак не містить в собі засобів для захисту даних і механізмів аутентифікації. Протокол L2TP використовує повідомлення двох типів: керуючі і інформаційні повідомлення. Керуючі повідомлення використовуються для встановлення, підтримки і ліквідації тунелів і викликів, для забезпечення доставки ними використовується надійний керуючий канал протоколу L2TP. Інформаційні повідомлення використовуються для інкапсуляції кадрів PPP, переданих по тунелю. При втраті пакету він не передається повторно.

Ще один дуже популярний протокол для побудови VPN – IPSec в режимі тунелювання. Розуміється, що тунельний режим встановлюється для шлюзів і є, по суті, IP-тунелем з аутентифікацією і шифруванням [1]. Їм передбачаються два

набори IP-заголовків: зовнішній і внутрішній. Перший містить IP-адресу VPN-шлюзу, тоді як другий – IP-адресу кінцевої системи. Протокол IPSec може бути корисний для будь-якої VPN навіть без його тунельних властивостей,не залежно від типу VPN, що застосовувався. Якщо потрібно заховати інформацію від чужих очей, то необхідно скористатися транспортним режимом IPSec поверх основного транспорту.

Технологія MPLS дозволяє пересилати дані застосовуючи мітки, що закріпляються за кожним пакетом. Внутрішні вузли ядра мережі, які підтримують MPLS, не аналізують вмісту кожного пакету. Так, IP-адреса одержувача не розглядається, що дає можливість MPLS організувати ефективний механізм інкапсуляції приватного трафіку, що передається по магістралі оператора [2].

Multiprotocol Label Switching або багатопротокольна комутація по мітках. До певної міри це переосмислення традиційної IP маршрутизації. В технології MPLS те, куди вирушає пакет, залежить не тільки від адреси призначення але й від спеціальної мітки. Якщо в IP кожен вузол сам приймав рішення, що робити з пакетом, то в MPLS шлях побудований заздалегідь. У міру просування пакета на ньому тільки перекидаються мітки. Тому, ключове слово тут Switching, а не Routing. MPLS заголовок мають довжину 32 біта або 12 байт і складається з поля Label – власне мітка 20 біт, полеТС – трафік клас 3 біта,S – ідентифікатора дна стека 1 біт, і TTL 8 біт (рис. 1.1).

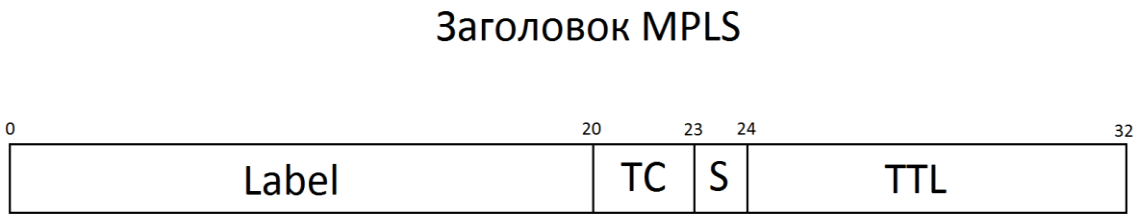

Рисунок 1.1 – Графічне зображення заголовку MPLS

MPLS можна розглядати як допоміжний інструмент для технологій L2/L3VPN і Traffic Engineering. Перша характерна риса MPLS-маршрутизатори не дивляться всередину MPLS пакета обмежуючись тільки аналізом мітки. Це дозволяє створити наскрізний канал, незалежно від того, що потрібно передати і поверх якого середовища. Друга – це наслідок з першої – мультипротокольні, всередині пакету MPLS можуть передаватися IP, Ethernet, ATM, Frame Relay. Але

в реальності MPLS працює тільки поверх IP-мереж [3], однак переносити може дійсно різні протоколи. Третя особливість полягає в тому, що Control Plane спирається на IP і є по суті Connectionless, тобто не орієнтованим на з'єднання. Але в той же час Data Plane – Connection Oriented пакети даних слід по заздалегідь побудованому шляху і це концептуальний момент. З одного боку є фіксований канал, який дозволяє прогнозувати затримки, джитер, забезпечити ширину пропускання, а з іншого – це все спирається на IP, отже може гнучко і швидко реагувати на перестроювання мережі.

Необхідно розглянути як це працює. Існує, так звана, хмара MPLS – це група пристроїв, на яких запущений безпосередньо сам механізм MPLS. Потрапляючи в нього IP пакет отримують мітку, далі пакет з міткою йде на наступний вузол, той бачить, наприклад, мітку 101 і знає, що її потрібно поміняти на мітку 500 і відправити в інтерфейс Fast Ethernet 0/0. Наступний вузол бачить на пакеті мітку 500 і знає, що її потрібно поміняти на нуль і відправити Fast Ethernet 0/1. При виході із хмари MPLS на граничному маршрутизаторі мітка видаляється і далі до одержувача йде чистий пакет. Для пакета в мережі MPLS заздалегідь заготовлений шлях. Це пояснюється тим, що у MPLS існують два застосування – L2/L3VPN і Traffic Engineering, жодне не можна реалізувати без використання MPLS досить легко і масштабовано.

Попередниками MPLS є ATM і Frame Relay. Їх важливою особливістю було те, що шлях, по якому будуть слідувати ячейки, був визначений заздалегідь і доля пакета в цілому була передбачувана і керована. Їх недолік в інертності, вони дуже погано реагували на перестроювання мережі. Мережа MPLS пристроїв працює поверх IP, за рахунок чого має гнучкість і масштабованість. Вона забезпечує заздалегідь визначений шлях як в ATM, це дозволить при певних умовах забезпечити ширину каналу, затримку, джитер та інші параметри.

Необхідно позначити елементи мережі MPLS і термінологію, яка використовується у цій технології (рис. 1.2). LSR – Label Switch Router – маршрутизатор із запущеною на ньому технологією MPLS, на цих маршрутизаторах відбувається зміна мітки. Label – мітка, число від 0 до 2^{20}, яка визначає дії з пакетом на кожному LSR. Ingress LSR – точка входу в мережу MPLS, вхідний, граничний маршрутизатор. Egress LSR – точка виходу, вихідний, граничний маршрутизатор. Будь-який маршрутизатор на межі хмари MPLS

називається LER – Label Edge Router. LSP – Label Switched Path – шлях, по якому доставляються пакети MPLS.

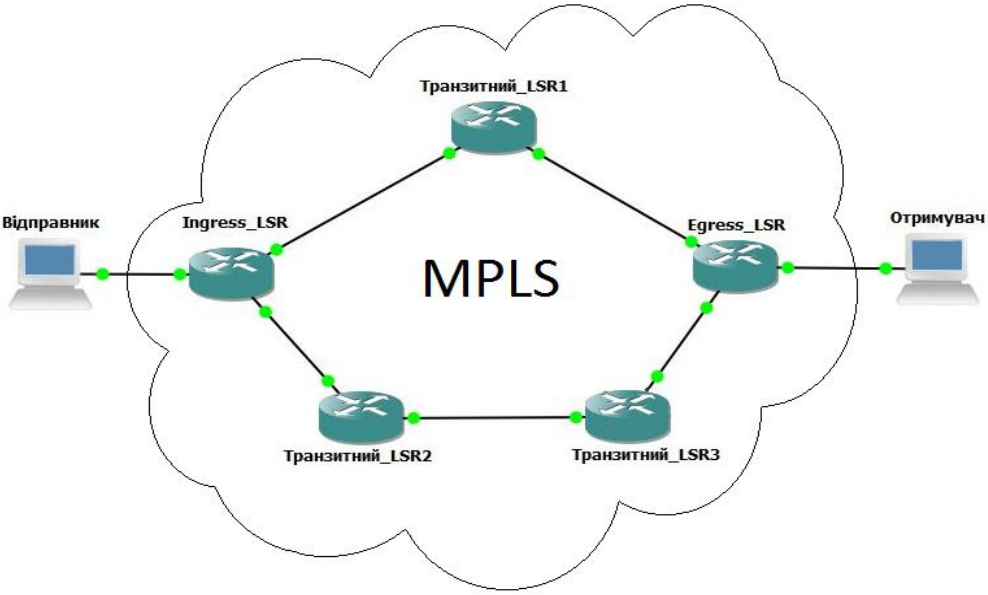

Рисунок 1.2 – Елементи мережі MPLS.

FEC – Forwarding Equivalence Class – IP-префікс пункту призначення, наприклад, 172.16.0.0/24. Це означає, що якщо два пакети йдуть на один префікс, навіть якщо від різних джерел для MPLS, вони еквівалентні. Також необхідно відзначити три операції з мітками: Push Label – прикріпити мітку в IP-пакет, проводиться ця операція на Ingress LSR; Swap Label – поміняти мітку, відбувається на кожному проміжному LSR; Pop Label – витягти мітку з IP-пакета, виконується на Egress LSR.

Необхідно відзначити наявність в MPLS зарезервованих міток. Вище згадувався приклад передачі пакета по мережі MPLS, де остання мітка, перед передачею пакета на порт одержувача, була нуль. Така мітка називається Explicit Null Label. Коли пакет з такою міткою надходить на Egress LSR, він розуміє, що мітку потрібно видалити і відправити пакет процесу IP. Мітка 1 – аналог опції Router Alert в IP. Мітка 2 – це те ж саме, що і мітка 0, тільки для IPv6. Мітка 3 – Implicit Null Label – необхідна, щоб повідомити передостанній LSR про добування мітки, таким чином на Egress LSR пакет перейде без верхньої транспортної мітки. Це необхідно для забезпечення якості обслуговування QoS. Поле TC в заголовку MPLS несе інформацію про пріоритет, якщо мітку прибрати на передостанньому

маршрутизаторі, то й інформація про пріоритет пропаде. У разі, якщо необхідно зберегти обробку пакета в правильних чергах потрібно використовувати Explicit Null. Тоді пакет між останнім і передостаннім маршрутизатором буде віддаватися відповідно пріоритету, прописаному в поле TC і оброблятися у відповідних чергах. Що стосується міток з 4 по 15 на даний момент вони зарезервовані і зараз не використовуються.

Також необхідно зазначити, що технологія MPLS підтримує стек міток. Щоб передати пакет через декілька LSP, необхідно мати можливість утримувати в пакеті більше однієї мітки. Це відбувається у вигляді стека, що дозволяє створювати ієрархію міток . На рис.1.3 зображено приклад дворівневого стека міток MPLS.

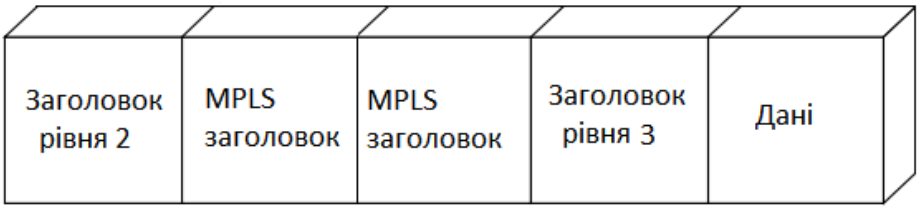

Рисунок 1.3 – Приклад дворівневого стека міток MPLS.

Функціональні засоби стека MPLS можуть забезпечити об'єднання кількох LSP в один. До стеку міток кожного з даних шляхів, поверх додається загальна мітка, таким чином створюється агрегований тракт MPLS. У точці закінчення такого тракту відбувається його розгалуження на складові самостійних LSP. Так відбувається об'єднання трактів, які мають спільну частину маршруту.

Отже, технологія MPLS здатна організувати ієрархічне пересилання, що може стати важливою та необхідною функціональною можливістю в тій чи іншій ситуації. При її використанні не потрібно переносити глобальну маршрутну інформацію, що робить мережу MPLS більш стабільною і масштабованою і зручною, ніж мережу з традиційною маршрутизацією.

1.2 Протоколи розподілу міток

Побудовою LSP займаються протоколи LDP і RSVP-TE. Також слід зауважити, що побудова шляху і рух трафіку від Ingress LSR до Egress LSR має назву Downstream. Відповідно Upstream – навпаки. Мітки завжди поширюються

вгору за течією. Тобто Маршрутизатор Egress LSR дає знати передостанньому маршрутизатору, що він чекає пакет, наприклад, з міткою нуль, і так далі. Мітки можуть поширюватися за запитом, а можуть прямо без запиту. Розповсюдження за запитом носить назву Downstreamon Demand. Наприклад, передостанній маршрутизатор запитує у Egress LSR, яку мітку він очікує, в свою чергу останній відповідає на його запит, відправляючи номер мітки. Другий випадок прямого розподілення без запиту називається Downstream Unsolicited. Egress LSR не чекає запиту,а відразу відправляє інформацію про мітку передостаннього маршрутизатора, який, в свою чергу, відправляє інформацію попереднім маршрутизаторам. LSR може передати мітку відразу, а може сидіти і чекати поки сусідній маршрутизатор не повідомить її перший. Такий випадок називається Independent Control. Тобто як тільки один з маршрутизаторів дізнається FEC мережі, то відразу виділяє мітку і передає її сусіднім вузлам. У другому випадку, який носить назву Ordered Control, поки маршрутизатор не отримає інформації від нижче стоячого вузла, то ніяких дій зроблено ним не буде. В такому випадку мітки розподіляються послідовно. Також LSR може зберігати зайві мітки, а може відразу їх видаляти. Зберігання міток необхідно для організації резервного шляху. Режим зберігання міток називається – Liberal Retention Mode. Відповідно Conservative Retention Mode – режим видалення переданих міток.

Протокол LDP – Label Distribution Protocol – основним завданням якого є швидкий розподіл міток. Даний протокол є протоколом незалежним, встановлює зв'язок через розсилку multicast (широкомовна розсилка, один до багатьох) всі його повідомлення обмежені однією лінією

Принцип роботи LDP (рис. 1.4): спочатку LSR розсилає LDP Hello на мультикастову адресу. Коли LSR обмінялися LDP Hello вони готові встановити TCP сесію, по якій вони в подальшому обмінюються мітками, а також помилками. Пошук мережі відбувається по протоколу UDP, а спілкування з протоколу TCP. Як тільки сесія встановлена і сусідні вузли один одного ініціалізували, вони обмінюються списками FEC – Forwarding Equivalence Class і мітками, які їм призначили.

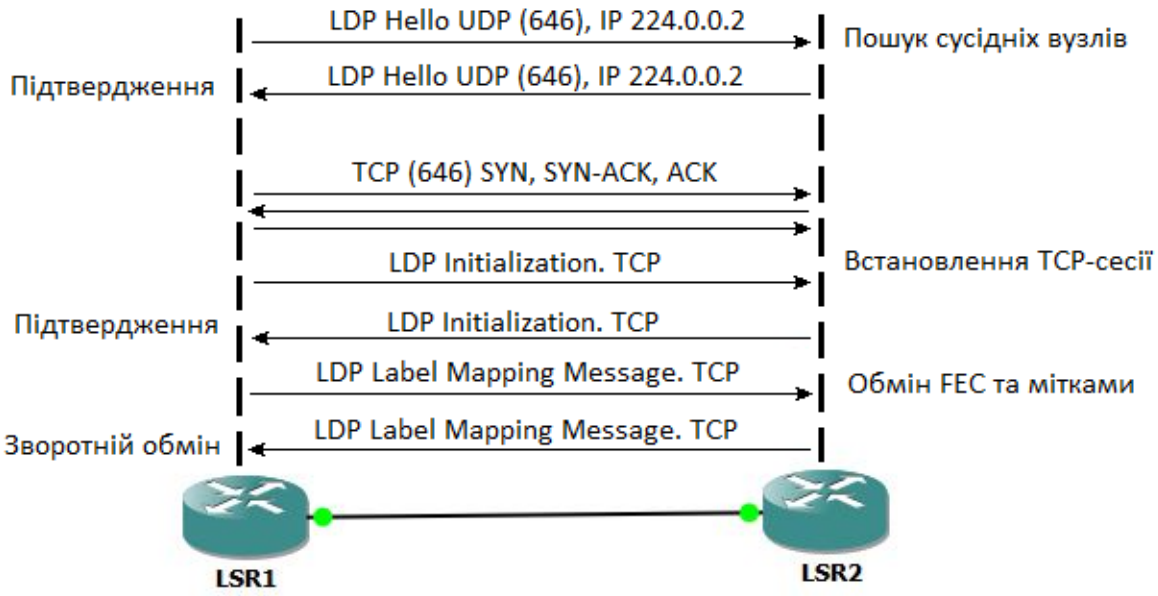

Рисунок 1.4 – Принцип роботи протоколу LDP

Зазвичай LDP застосовують в режимах Downstream Unsolicited, Independent Control, Liberal Retenttion Mode. Тобто запитів на мітку немає, будь-який LSR може почати анонсувати мітки, коли йому завгодно, не чекаючи відмашки від нижче стоячих вузлів і в результаті на кожному LSR від кожного сусіднього вузла будуть позначки для кожного FEC. Мітка вибирається на основі таблиці маршрутизації, який інтерфейс вважається найкращим, така позначка і буде обрана. Такий підхід виключає утворення петель. Це є концептуальним моментом LDP. Він спирається на доступну маршрутну інформацію, але сам не використовує протоколи маршрутизації. Якщо основний шлях виходить з ладу, то спочатку повинна запрацювати маршрутизація і тільки потім реагує LDP. Цей протокол хороший тим, що він простий у застосуванні, щоб за його допомогою налаштувати MPLS досить включити його на інтерфейсах, далі він все зробить сам. Мінусом же є його крайня надмірність. Тобто шлях будується від кожного LSR до кожного FEC, навіть якщо вимагається тільки один маршрут.

RSVP-TE – Resource ReSer Vation Protocol для Traffic Engineering – це розширення RSVP, створене для виконання потреб Traffic Engineering. Цей набір технологій дозволяє будувати LSP з урахуванням певних обмежень і резервувати ресурси на всіх кутах від Ingress LSR до Egress LSR. Наприклад, в разі відеоспостереження, для відеопотоку, який направляється від ПК 1 до 172.16.0.2 потрібно зарезервувати смугу 25Мб/с, при цьому шлях не повинен лежати через конкретний маршрутизатор. Цей шлях проходить через конкурента, по більш

оптимальному шляху. По-перше, цей протокол використовує ISIS, OSPF, IGP. Один з цих протоколів динамічної маршрутизації збирає по мережі інформацію про доступні ресурси, крім базової топології. Комбінуючи ці дані, протоколи динамічної маршрутизації створюють TED – Traffic Engineering Database – топологія мережі з урахуванням ресурсів. Так RSVP-TE дізнається схему всієї мережі, а також скільки і де доступних ресурсів. Після чого отримана схема разом із заданими обмеженнями передається алгоритму CSPF – Constrained Shortest Path First – алгоритм обчислення найкоротшого шляху з урахуванням обмежень. В результаті CSPF видає список вузлів від Ingress LSR до Egress LSR. Тепер на Ingress LSR формується повідомлення RSVP-TEPath. Отриманий на попередньому кроці список, вставляється в Path, як об'єкт ERO – Explicit Route Object – Список вузлів складений CSPF. Наступний об'єкт – Label Request (рис. 1.5).

Рисунок 1.5 – Графічне зображення повідомлення RSVP-TE Path

Повідомлення Path передається по мережі відповідно до ERO, а Label Request змушує кожен LSR виділити мітку, але поки не передавати. Коли Egress LSR отримує Path, він виділяє мітку і передає її назад повідомленням RSVP-TE Resv (рис. 1.6).

Рисунок 1.6 – Графічне зображення повідомлення RSVP-TE Resv

В об'єкті Label Resv передається назад тим самим шляхом, яким прийшов Path. Рухаючись по мережі Resv роздає мітки. Якщо з якоїсь причини CSPF не зміг побудувати маршрут з урахуванням умов, або повідомлення Resv або Path на своєму шляху виявив LSR, на якому недостатньо ресурсів, то LSP не буде побудований.

1.3 Основні відмінності та забезпечення безпеки мережі

З огляду на те, що сеанси в сучасних телекомунікаційних мережах потребують додаткового захисту, то створення тунелів є адекватним рішенням даного питання. В свою чергу тунелі MPLS дозволяють вирішити низку питань стосовно безпеки в приватних віртуальних мережах, а також – проблеми попередніх пропозицій тунелювання. Дану тему висвітлював Захватов М. А. у своїй роботі, у видавництві Cisco Systems.

Тунелі MPLS здатні передавати дані будь-якого протоколу вищого рівня (наприклад IP, IPX, кадри Frame Relay, комірки ATM), оскільки вміст пакетів вздовж усього шляху проходження не змінюється, змінам схильні лише мітки. На відміну від них, тунелі IPSec підтримують передачу даних тільки протоколу IP, а протоколи PPTP і L2TP дозволяють обмінюватися даними по протоколах IP, IPX або Net BEUI. Безпечна передача даних в MPLS забезпечується за рахунок певної мережевої політики, яка забороняє приймати пакети, наділені мітками, і маршрутну інформацію VPN-IP від неперевірених джерел. Безпека передачі підвищується впровадженням стандартних засобів аутентифікації або шифрування (наприклад шифрування IPSec).

Щоб безпечно передавати дані до протоколу IP Security внесені деякі способи шифрування IP-пакетів, аутентифікації, забезпечення захисту і цілісності даних при пересилці, в результаті чого тунелі IPSec можуть організовувати безпечну доставку інформаційного трафіку. Протокол L2TP здатний підтримувати процедури тунелювання та аутентифікації інформаційного потоку, а PPTP окрім зазначених функцій, також додано функцію шифрування. Застосування міток MPLS дозволяє реалізувати значно швидше транспортування пакетів по мережі провайдера. Транспорт MPLS не зчитує заголовки пакетів, що передаються, тому адресація в цих пакетах може мати приватний характер. Вміст пакетів також не зчитується і при проходженні по мережі IP-пакетів за протоколами IPSec, PPTP і L2TP.

Однак, на відміну від MPLS, традиційні протоколи тунелювання для транспортування IP-пакетів використовують традиційну IP-маршрутизацію. Під час вибору шляху передачі пакету в MPLS беруться до уваги різновидні параметри, що впливають на вибір подальшого маршруту. Групова робота технології багатопротокольної комутації і механізмів Traffic Engineering дає змогу для

кожного LSP-тунелю виділити потрібний рівень якості обслуговування за рахунок резервування ресурсів, уздовж шляху проходження пакету, на кожному вузлі. Крім зазначеного, з'являється можливість відстежувати маршрут, що проходить через організований тунель, також додаються можливості діагностики та адміністрування LSP-тунелів. Різноманітні тунелі, відповідно до необхідного рівня якості QoS між двома елементами мережі може підтримувати також протокол L2TP. В свою чергу технологія VPN IPSec не має змоги підтримувати параметри якості обслуговування встановленого з'єднання, а протокол PPTP підтримує єдиний тунель між двома точками. Необхідно відзначити і той факт, що весь трафік при застосуванні традиційних IP-тунелів передається до адресата уздовж одного і того ж шляху.

1.4 Переваги MPLS тунелів

Технологія MPLS дозволяє контролювати потоки, що передаються по безлічі всіх наявних шляхів до адресата.

Можливості, які надають тунелі в MPLS:

1. Можливість формування LSP-тунелів з урахуванням якості QoS та без.

2. Можливість динамічно змінювати маршрути сформованих LSP тунелів.

3.Можливість відстежувати дійсний маршрут, що проходить через сформований LSP тунель.

4. Можливість ідентифікувати і діагностувати LSP тунелі.

5.Можливість встановлювати сформований LSP тунель під адміністративний контроль.

6. Можливість здійснювати посилання запитів виділення міток, їх розсилку і об'єднання. І як наслідок MPLS-VPN [4] пропонує поліпшену продуктивність у порівнянні з IP-VPN, бо є можливість розділити дані на різні категорії, такі як реальний час трафіку, пріоритет трафіку, низький пріоритет трафіку і так далі. Ваш оператор мобільного зв'язку буде підтримувати ці пріоритети по всій своїй мережі, забезпечуючи якість обслуговування в будь-якому кінці. Також MPLS підтримує високий рівень безпеки, оскільки трафік сегментований від інших користувачів на мережі оператора.

2 АНАЛІЗ ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ MPLS

2.1 Використання технології MPLS на всіх рівнях мережі

Технологію MPLS називають технологією мережевої конвергенції, яка забезпечує підтримку транспортних додатків, кращу підтримку послуг і масштабована в мережах доступу. Це розкриває ряд привабливих можливостей: високу продуктивність і пропускну здатність, моделювання трафіку, простоту побудови мереж та їх експлуатація.

Використання технології MPLS на всіх рівнях мережі, що представляє собою єдиний MPLS простір, схематично показано на рис. 2.5.

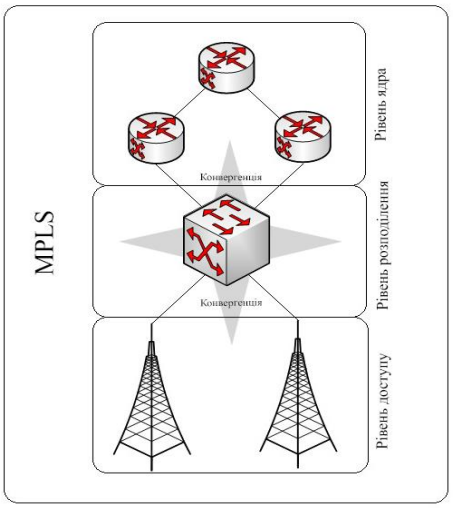

Рисунок 2.1 – Використання технології MPLS на всіх рівнях мережі

У традиційній технології MPLS виділяють деякі труднощі, пов'язані зі складністю реалізації сервісів у великих мережах. Це, наприклад, необхідність застосування складних механізмів рівня L3 при сполученні з протоколами рівня L2.

У Unified MPLS відсутні перераховані недоліки при тих же очевидних перевагах, пов'язаних з високою продуктивністю і пропускною спроможністю, а також простотою експлуатації мереж. Крім того, інтегруючи за допомогою MPLS сегменти доступу, агрегації і ядра, можна зменшити кількість вузлів адміністрування [5].

2.2 Побудова та аналіз можливої моделі мережі

З огляду на зазначені вимоги до побудови мережі, а також вимоги масштабованості, гнучкості, керованості і безпеки, запропонована наступна модель мережі (рис. 2.6).

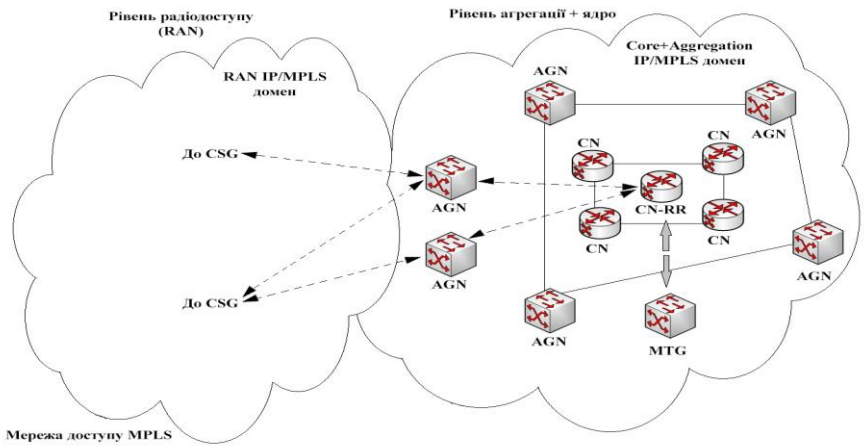

Рисунок 2.2 – Модель мережі до рівня ядро/агрегація

Єдина технологія MPLS формує транспортну основу для підтримки мереж LTE, 2G GSM і 3G.

Запропонована модель мережі з використанням єдиного стандарту MPLS для мобільного транспорту надасть операторам комплексне рішення, оптимізоване за вартістю, з підтримкою призначеного для користувача трафіку і трафіку бізнес-послуг з високими показниками якості обслуговування (QoS) в порівнянні з аналогічними стандартами.

Трьохрівнева опорна мережа оператора поділяється на рівень доступу, агрегації та ядра . На рівні доступу вузли CSG працюють в домені RAN. Рівні агрегації і ядра створюють один рівень – агрегація плюс ядро. Вузли агрегації – AGN і вузли ядра – CN, CN-RR і MTG. Декілька прилеглих базових станцій підключаються до одного вузла доступу. Протокол MPLS налаштовується на всіх рівнях мережі [6].

Дана система дає змогу водночас підтримувати декілька поколінь мобільного зв'язку в єдиній конвергентній мережевій архітектурі. Впровадження LTE забезпечується з підтримкою Pseudowire Emulation (PWE) для передачі 2G GSM, L2VPN для 3G UMTS/IP і L3VPN для 3G UMTS/IP і LTE відповідно підтримуються: синхронізація та наявні високі показники якості обслуговування

(QoS), протоколи OAM – протоколи експлуатації, адміністрування і обслуговування, швидка збіжність і управління продуктивністю. Система оптимізується для підтримки вимог стандарту 4G, таких як IPSec і аутентифікація, пряме з'єднання між eNodeB по інтерфейсу X2, мультикаст, віртуалізація, можливість розподілу EPC шлюзів і балансування трафіку.

Рівні агрегації і ядра об'єднані в один рівень (Core + Aggregation) інтегруються в єдиний IGP/LDP домен. Рівень доступу, так званий вузол попередньої агрегації (RAN), який в свою чергу складається з окремого IGP домену. Вузли агрегації об'єднують мобільні мережі рівня доступу протоколом MPLS і залучають їх бути частиною однієї автономної системи (AC) з мережею агрегації/ядра [7].

Вузли доступу включаються за допомогою різних інтерфейсів до відповідних їм L3VPN, які присутні на вузлах, до яких підключені MSS/RNC і ін. Тобто, зв'язок між базовою станцією і зазначеними мережевими елементами здійснюється ізольовано всередині L3VPN за допомогою протоколу Multiprotocol BGP (MP-BGP). Даний протокол є розширенням протоколу BGP, що дозволяє йому передавати інформацію про маршрутизації для декількох мережевих рівнів і адресних сімейств. MP-BGP може нести інформацію про односпрямовані маршрути, які використовуються для багатоадресної маршрутизації, окремо від шляхів, які використовуються для односпрямованого форвардингу IP [4].

2.3 Розрахунок швидкості передачі корисного навантаження

Для аналізу показників оперативності інформаційного обміну мережі проведений розрахунок швидкості передачі корисного навантаження. Відмінність корисної пропускної здатності від повної пропускної здатності залежить від довжини кадру. Технологія GE (Gigabit Ethernet) є розвитком технології Ethernet, тому формат кадру практично не відрізняється. Різниця лише в тимчасових параметрах. Міжкадровий інтервал складе 0,096 мкс. Для його обліку в розрахунку цей час переводиться на надлишкову інформацію. Так як швидкість фізичного середовища становить 1 Гбіт/с (тобто Bt = 1 073 741 824 біт/с), то міжкадровий інтервал (IPG) буде дорівнює:

$$IPG = 1073741824 \cdot 0{,}096 \cdot 10^{-6} = 13, \text{байт}. \quad (2.1)$$

При розрахунку кількості корисних даних (MSS) слід враховувати, що в технології GE максимальний розмір пакету 1526 байт, з яких 18 байт займає службова інформація (заголовок GE), і 8 байт – преамбула.

Тобто частка користувальницької інформації на інформацію пакета, сформованого за технологією GE становить:

$$\gamma_{GE} = \frac{1526-18-8}{1526+IPG} = \frac{1500}{1539} = 0{,}975, \quad (2.2)$$

Також необхідно залишити місце для міток MPLS ($N_{мітк.}$) і заголовків TCP/IP ($N_{заг.}$). У мережах MPLS при використанні VPN потрібно застосовувати стек з 2 міток по 32 біта ($N_{мітк}$ = 8 байт), де верхня визначатиме маршрут прямування, а нижня буде використана вихідним граничним маршрутизатором для вибору необхідного сайту VPN. Заголовки TCP/IP займають кожен 20 байт ($N_{заг.}$ = 40 байт).

З огляду на вищеописаний складу пакета, отримаємо кількість корисних даних в мережі з технологіями MPLS і GE:

$$MSS = 1526-18-8-2\cdot 4-2\cdot 20 = 1452, \text{байта} \quad (2.3)$$

Розрахуємо максимальний розмір пакета в каналі (MTU) з урахуванням міжкадрового інтервалу:

$$MTU = 1526+IPG = 1539, \text{байт} \quad (2.4)$$

При розрахунках не враховується час, необхідний для отримання підтверджень про доставку пакетів, не враховується час на встановлення і може призвести до втрати з'єднання, не враховується затримка мережі GE (так як вони не значні, 0,01–0,4 мс), а також службовий трафік (протоколи управління, маршрутизації і т.д.).

3 АНАЛІЗ ТА ОБҐРУНТУВАННЯ АЛГОРИТМУ ЕФЕКТИВНОСТІ ПОБУДОВИ ТУНЕЛЮ

3.1 Процес тунелювання в MPLS

Тунелювання або інкапсуляція – це метод передачі корисної інформації через проміжну мережу. Така інформація представляє собою пакети або кадри іншого протоколу. При інкапсуляції пакет не передається у вигляді створеному вузлом, який його відправляє, а до нього додається додатковий заголовок, що включає в себе інформацію про маршрут, що дозволяє інкапсульованим пакетам проходити через, проміжну додаткову мережу. На кінці тунелю вони деінкапсулюються і далі пересилаються до одержувача.

Даний процес, що включає інкапсуляцію та транспортування пакетів, і є туннелюванням. Отже, тунелем називається логічний шлях пересування інкапсульованих пакетів в транзитній мережі [8].

Тунельні передачі представлені на рис. 3.1. Всі прикордонні маршрутизатори MPLS, а саме LSR1, LSR5, LSR6 і LER10 застосовують протокол BGP і створюють комутований по мітках тракт LSP між ними. Ці чотири прикордонні LSR використовуватимуть протокол LDP для отримання і зберігання міток від вихідного LSR, в даному випадку це LSR10 аж до вхідного LSR – LSR1.

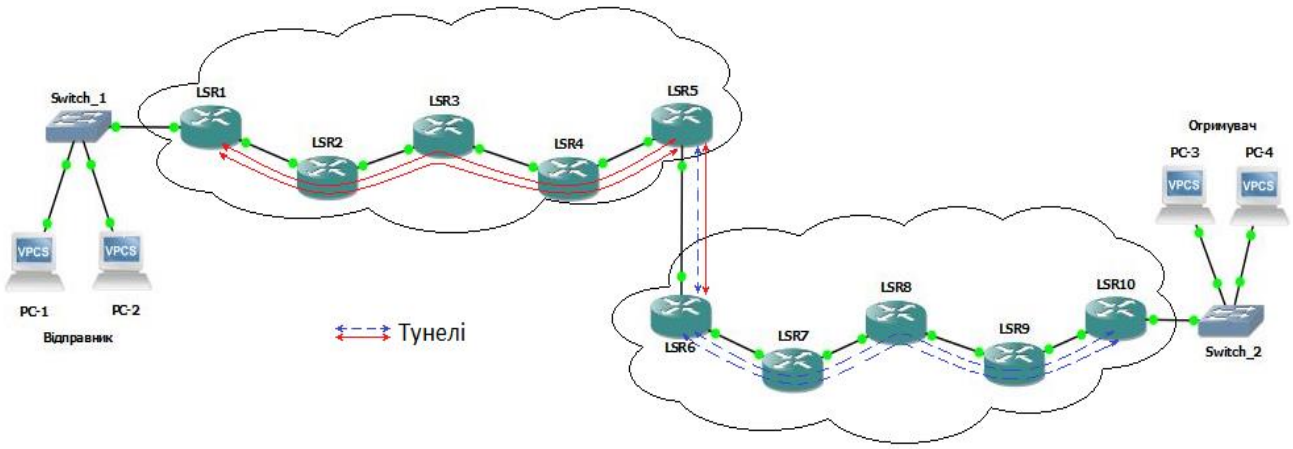

Рисунок 3.1 – Схема процесу тунелювання в MPLS

Щоб дані були передані від LSR1 до LER5, вони повинні пройти через кілька транзитних маршрутизаторів, в даному випадку це три транзитних вузла LSR. Між

двома LSR (LSR1 і LSR5) створюється окремий тракт LSP, який охоплює LSR2, LSR3 і LSR4. Він являє собою тунель між цими двома граничними LSR. Мітки в даному тракті відрізняються від міток, які LSR створили в першому випадку від LSR1 до LSR10. Це справедливо і для LSR6, LSR10, і для LSR, що розташовані між ними. Для цього останнього сегмента створюється тракт окремий LSP. Для досягнення цього результату при передачі пакета через два мережевих сегмента використовується концепція стека міток. Пакет повинен слідувати через всі три LSP, він буде переносити одночасно дві окремі мітки [9].

Коли пакет залишає першу мережу і приймається прикордонним маршрутизатором LSR5, то він розглядає мітку і замінює її на мітку для наступної мережі. У свою чергу граничний LSR10 видаляє обидві мітки перед відправкою пакету адресату.

3.2 Математична модель ефекту тунелювання MPLS

Математична модель ефекту тунелювання в MPLS є мережею масового обслуговування з послідовними чергами (рис. 3.2).

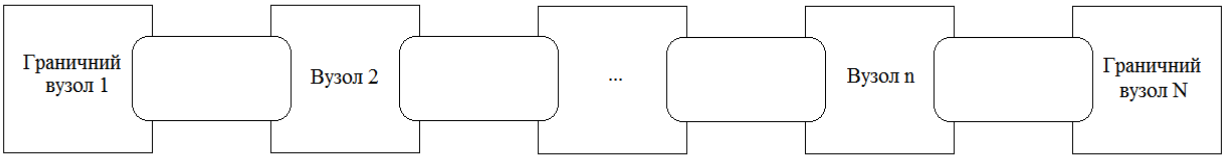

Рисунок 3.2 – Модель послідовних черг

Параметрами для оцінювання в подібній мережі є: середній час обслуговування без переривання (період зайнятості), а також середній час перебування пакета в n-вузлі.

Обслуговуються за період зайнятості, тобто безперервно та без звільнення, пакети об'єднуються в групу на виході вузла і називаються пачкою. Середня довжина такої пачки визначається числом пакетів.

У моделі на рис. 3.2 на вхід граничного вузла 1 надходить пуасонівський потік пакетів з інтенсивністю λ і з середнім часом обслуговування пакета $1/\mu$. На базі теореми Бурке будується ряд моделей, що описують поведінку трафіку, що

складається з пачок пакетів в тунелях MPLS-TP. Для цієї поведінки характерні процеси фрагментації і зчеплення пачок пакетів в тунелях, які суттєво впливають на якість обслуговування. На вхід граничного вузла 1 надходить пуасонівський потік повідомлень з інтенсивністю вхідного потоку заявок λ і середнім часом обслуговування 1/μ.

Якщо розглядати два наступних повідомлення, один за іншим на вузлі n (n≥2), інтервал часу між надходженням цих двох повідомлень залежить від часу надходження і обслуговування на попередніх вузлах. Повідомлення, згруповані на вузлі n (n≥2), залишаються згрупованими і на наступних вузлах n+1, n+2.

Як зазначено вище, в тунелюванні існують два явища: зчеплення пачок, що виходять від першого вузла, і фрагментація цих же пачок [10].

Перше явище називається зчеплення – відноситься не тільки до другого, але і до будь-якого не першого вузла n (n≠1) і пов'язане воно з тим, що перший пакет k-ї пачки наздоганяє на конкретному вузлі останній пакет (k-1)-ї пачки, і обидві пачки – k і (k-1) відповідно зчіплюються один з одним(рис. 3.3).

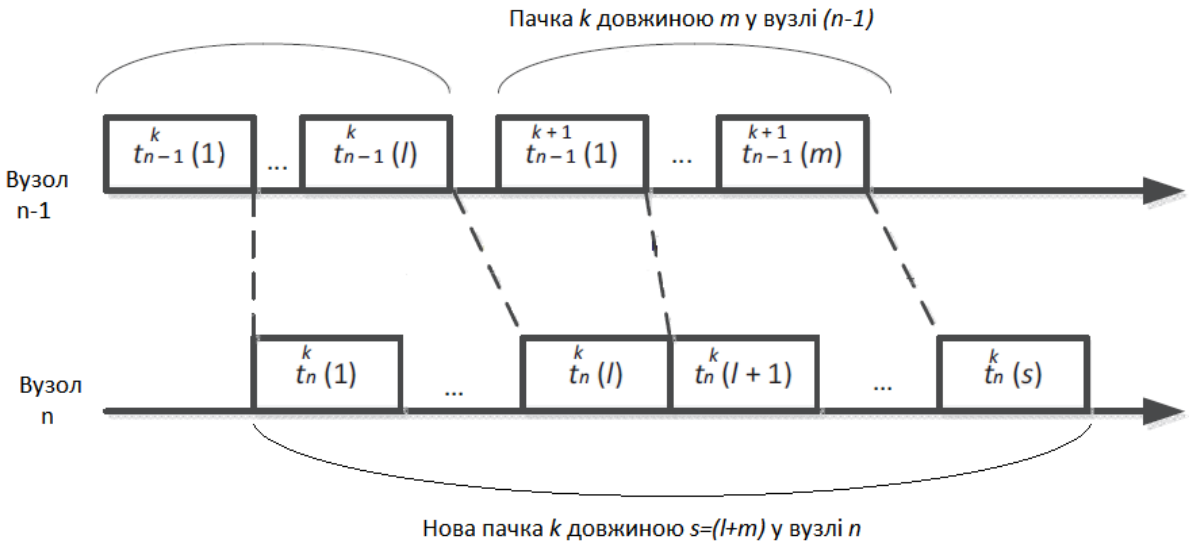

Рисунок 3.3 – Зчеплення пачок k–1 та k у вузлі n

Друге явище – фрагментації (рис. 3.4) – не настільки очевидне і може бути лише в другому вузлі, але теж цілком явно. Нехай в першому вузлі обслуговується пакет номер j з пачки k і в цей момент на той же перший вузол надходить наступний пакет номер j+1, час обслуговування якого перевершує час обслуговування пакета

j. Нехай на наступному другому вузлі в цей момент є черги і пакет j обслуговується, як тільки він надходить на вузол 2, пакети j+1 і j починають обслуговуватися одночасно на вузлах 1 і 2, відповідно. Коли пакет j залишає вузол 2, пакет j+1 все ще продовжує оброблятися на вузлі 1, оскільки час його обслуговування довше (рис. 3.4)

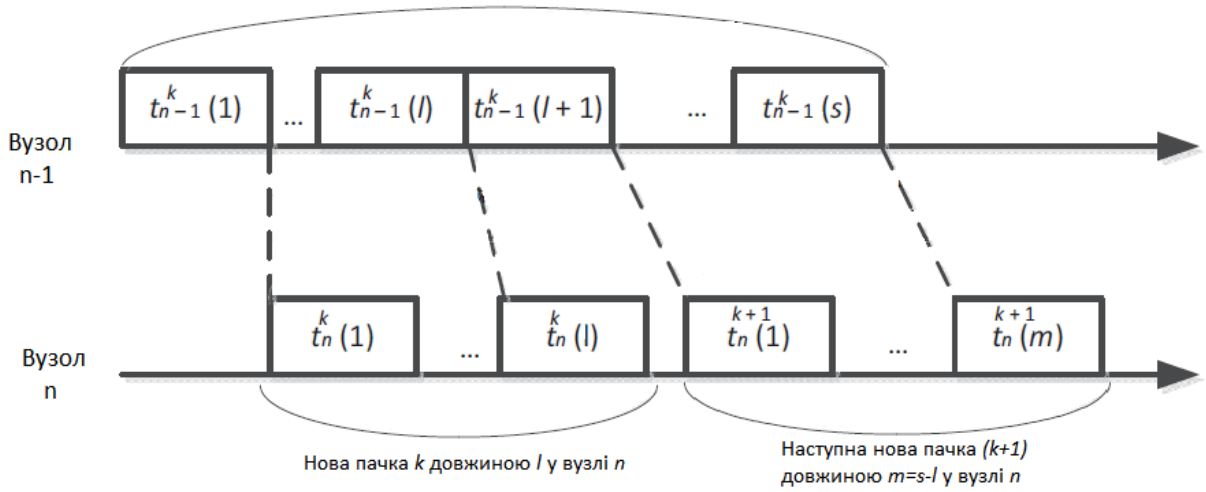

Рисунок 3.4 – Фрагментація пачки k у вузлі n

Математичний аналіз цих двох явищ ефекту тунелювання MPLS дозволяє використати наступну формулу для часу перебування пакета в тунелі, що складається з N вузлів.

$$V_1(N) = \ln\left[(N-2)! * \left(\frac{\rho}{1-\rho}\right)^N\right] + N(1+\gamma), \quad (3.1)$$

де γ – постійна Ейлера (γ = 0,577);

N – кількість проміжних вузлів;

ρ – завантаження мережі, N ≥ 2.

Формула (3.1) дозволяє оцінити доцільність організації тунелю в LSP-шляху для індивідуальних випадків при заданому навантаженні мережі.

На рис. 3.5 представлений маршрут в MPLS-мережі, який складається з N вузлів і фізичних каналів передачі даних між ними. Маршрут визначається місцем розташування LSR джерела, LSR призначення і класом обслуговування трафіку, що визначаються припустимим часом передачі. Нехай λ – інтенсивність

пуасонівського потоку запитів, а 1/μ означає усереднений час обслуговування повідомлень у вузлі. Відповідно, ρ=λ/μ означає навантаження, що обслуговується вузлом LSP-маршруту. Обслуговування ж цього навантаження вузлами, що входять в даний LSP-маршрут, і є основною роботою даного фрагмента мережі MPLS.

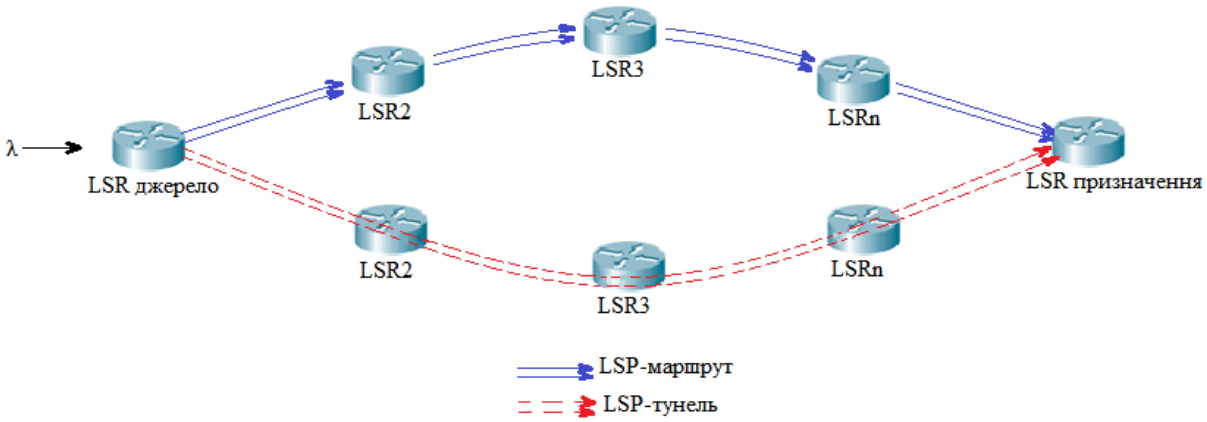

Рисунок 3.5 – Порівняльна оцінка величин V1(N) і V2(N)

На рис. 3.5 представлені обидва варіанти передачі повідомлень при наявності або при відсутності LSP-тунелю.

Для аналітичного дослідження ситуації відсутності LSP-тунелю вузол n передає пакети по LSP, доцільно описати за допомогою моделі M/M/1/K зі швидкістю передачі μ пакетів в секунду і максимальною кількістю K пакетів, які він може зберігати в своїй буферній пам'яті [11]. Пакети цієї моделі є тими ж самими, що в разі організації тунелю, а обмеження на розмір буфера вибрано так, щоб умови в варіантах наявності або відсутності тунелю були б абсолютно однакові.

Інженерні відмінності між MPLS і традиційним тунелюванням складається в моделі топології MPLS [12]. Традиційні тунелі завжди проходять від однієї границі до іншої наскрізь через мережу. У разі MPLS тунелі можуть створюватися усередині мережі для управління трафіком лише в частині мережі [13]. Тобто в LSP з M маршрутизаторів від вхідного LSR1 до вихідного LSRM можна створити LSP-тунель, наприклад, від вхідного LSR5 до вихідного LSRN, при N<M. Тобто навіть створювані на короткий час LSP-тунелі в MPLS можуть починатися всередині мережі, а не з призначеного для користувача додатка на кордоні мережі. Це особливо важливо для практичного використання: користувачі будуть

продовжувати застосовувати звичайні IP-пакети і адресацію в своїх додатках і навіть в локальних мережах. Однак, в разі підключення локальної мережі до глобальної, деякі IP-пакети користувачів або пакунки пов'язані з іншими протоколами можуть направлятися через тунелі MPLS з метою забезпечення їх привілейованого обслуговування [14].

Ефект, одержуваний від організації тунелю, демонструється різницею між V1(N) і V2(N). Наявність цього ефекту перевіряється, починаючи з максимально можливого значення N=M, тобто з максимально довгого тунелю від краю до краю. Якщо при цьому досягається позитивний ефект, то приймається рішення про організацію тунелю. Якщо немає, то спроба пошуку цього ефекту повторюється для більш короткого шляху N=M-1.

3.3 Алгоритм організації тунелю

Отже, можна вважати, що ефект від організації тунелю, відносно пакету який доставляється, дорівнює різниці V1(N) і V2(N). При цих припущеннях пропонується наступний алгоритм (рис. 3.6):

Крок 1. Припускається N = M.

Крок 2. Для n=1,2,...,N визначаються величини розміру пачки в $К_n$ за формулою (3.2):

$$K_n = 1 + n\frac{\rho}{1-\rho}. \quad (3.2)$$

Крок 3. Визначається час V2(N) перебування пакета мережі з N вузлів (маршрутизаторів) без організації LSP-тунелю при наявності обмеженої черги до вузла n довжиною $К_n$ за формулою (3.3):

$$V_2(N) = \sum_{n=1}^{N} \frac{1}{\mu}\frac{1-(K_n+1)\rho^{K_n}+K_n\rho^{K_n+1}}{(1+\rho^{K_n})(1-\rho)}. \quad (3.3)$$

Крок 4. Визначається час V1(N) перебування пакета в LSP-тунелі з N вузлів за формулою (3.1)

Крок 5. Відбувається порівняння величин V1(N) і V2(N). При отриманні позитивної різниці V1(N) і V2(N) організація тунелю між першим вузлом і вузлом

N є не доцільною. У цьому випадку здійснюється перехід до кроку 6. У протилежній ситуації приймається рішення організувати тунель між першим вузлом і вузлом n, і робота алгоритму на цьому закінчується.

Крок 6. Отримавши позитивну різницю V1(N) і V2(N) в вузлі n приймається рішення, щоб виключити вузол n з розгляду при побудові можливого LSP-тунелю.

Рисунок 3.6 – Схема алгоритму організації тунелю

Даний алгоритм дозволяє вибрати ефективний LSP-тунель десь всередині фрагмента мережі MPLS з N вузлів (маршрутизаторів) або відмовитися від його побудови. Саме по собі рішення про організацію LSP-тунелю згідно із запропонованим алгоритмом зводиться до аналізу двох значень середнього сукупного часу перебування пакета в вузлах від 1 до вузла N за наявності тунелю і без нього.

4 РОЗРАХУНОК ЕФЕКТИВНОСТІ ТУНЕЛЮВАННЯ ЗА ДОПОМОГОЮ СЕРЕДОВИЩА MATHCAD

4.1 Обґрунтування вибору середовища для розрахунків

Вибір середовища Mathcad обумовлений тим, що це характерний приклад математичного ПО, призначеного для здійснення, як чисельних, так і аналітичних розрахунків за формулами і візуалізації їх результатів у вигляді графіків.

Обчислювальні засоби Mathcad забезпечують розрахунки за складними математичним формулам, включаючи чисельні методи і аналітичні перетворення. Mathcad має великий набір вбудованих математичних функцій, дозволяє обчислювати ряди, суми, твори, інтеграли, похідні, працювати з комплексними числами, вирішувати лінійні і нелінійні рівняння, а також диференціальні рівняння і системи, проводити мінімізацію і максимізацію функцій, виконувати векторні і матричні операції, статистичний аналіз і т.д. Автоматично ведеться контроль розмірностей і перерахунок в різних системах виміру. Редактор формул забезпечує природний «багатоповерховий» набір формул в звичній математичній нотації (ділення, множення, квадратний корінь, інтеграл, сума і т.д.). Потужні засоби побудови графіків і діаграм поєднують простоту використання і ефективні способи візуалізації даних

Дана програма – це універсальний математичний пакет, створений для інженерних, а також виконання наукових розрахунків. Основна перевага пакету – природна математична мова, яка дає можливість правильно оцінити потреби поставленої задачі. Об'єднання текстового редактора з можливістю використання загальноприйнятого математичної мови дозволяє користувачеві отримати готовий підсумковий документ. Пакет має широкі графічні можливості.

Одна з важливих можливостей Mathcad – це можливість побудови в документі графіків. Необхідно виділити місце в документі і вставити XY-графік, тобто декартовий графік залежності отриманих значень V1 (N) від n і V2 (N) від n відповідно.

4.2 Розрахунки ефективності тунелювання

Існує фрагмент мережі MPLS, який включає в себе 10 вузлів – маршрутизаторів.

Нехай N=M=10. При цьому для n=1,2,...,10 визначається величина розміру пачки K_n за формулою (3.2). Розрахунки виконані для різних величин завантаження мережі, а саме: ρ=0,3; ρ=0,4; ρ=0,5; ρ=0,6; ρ=0,8; ρ=0,95. Результати розрахунків розмірності пачки при зазначеному навантаженні мережі зведені до таблиці 4.1.

Необхідно визначити час V2(10) просування пакета в мережі MPLS з 10 вузлів (маршрутизаторів) без організації LSP-тунелю при наявності обмеженої черги до вузла n довжиною K_n за формулою (3.3). У розрахунках використовується значення середньої швидкості обслуговування μ=22000 пак/с. Результати розрахунків часу перебування пакету в мережі без організації тунелю (V2) зведені до таблиці 4.3.

Наступним етапом необхідно визначити час перебування пакета в LSP тунелі V1(N) з n вузлів за формулою (3.1). Результати представлені в таблиці 4.2 Далі порівнюються величини V1(N) і V2(N). При їх позитивній різниці організація тунелю між першим вузлом і вузлом n недоцільна. При цьому здійснюється перехід до наступного кроку. В іншому випадку приймається рішення організувати тунель між першим вузлом і вузлом n. Якщо різниця позитивна V1(N) і V2(N), у вузлі n приймається рішення про виключення вузла n з розгляду на предмет можливого LSP-тунелю. Виграш у часі від організації тунелю дорівнює різниці V1 і V2.

Перш ніж перейти до безпосередніх розрахунків у середовищі Mathcad, необхідно позначити змінні, а також вхідні дані.

N – Кількість вузлів;

ρ – завантаження мережі;

γ – постійна Ейлера, що дорівнює 0,577;

V1N – час перебування пакету в LSP- тунелі;

V2N – час перебування пакету в мережі з N вузлів без організації тунелю;

n – номер вузла;

K_n – розмір пачки, довжина дерги до вузла;

μ – середня швидкість обслуговування (пак/с);

m – корегуючий коефіцієнт.

Внісши всі необхідні дані, потрібно вивести перші результати. Розрахунок ефективності побудови тунелю для завантаженості мережі ρ=0,3 показано на рис. 4.1. Графічне представлення результатів у вигляді графіків залежності часу перебування пакета в LSP-шляху при організації тунелю і без організації тунелю від кількості вузлів при ρ=0,3 показано на рис. 4.2

$N := 10 \quad \rho 1 := 0.3 \quad \rho 2 := 0.4 \quad \rho 3 := 0.5 \quad \rho 4 := 0.6 \quad \rho 5 := 0.8 \quad \rho 6 := 0.95$

$\gamma := 0.577 \quad \mu := 22000 \quad m := 1.06 \quad n := 1,2..N \quad \mu 1 := \frac{\mu}{1+\mu} = 1$

$K_n := 1 + n \cdot \frac{\rho 1}{1-\rho 1}$

$V21_n := \sum_{n=1}^{n} \left[m \cdot \frac{1}{\mu 1} \cdot \frac{\left[1 - (K_n + 1) \cdot \rho 1^{K_n} + K_n \cdot \rho 1^{K_n+1}\right]}{(1 - \rho 1^{K_n}) \cdot (1 - \rho 1)} \right]$

$n := 2..N$

$V11_n := \ln\left[(n-2)! \cdot \left(\frac{\rho 1}{1-\rho 1}\right)^n\right] + n \cdot (1+\gamma)$

$K_n =$	$V21_n =$	$V11_n =$
1.857	2.463	1.459
2.286	3.812	2.189
2.714	5.212	3.612
3.143	6.649	5.44
3.571	8.112	7.556
4	9.591	9.895
4.429	11.083	12.417
4.857	12.582	15.092
5.286	14.087	17.902

Рисунок 4.1 – Розрахунок ефективності побудови тунелю в мережі MPLS при навантаженні ρ=0,3

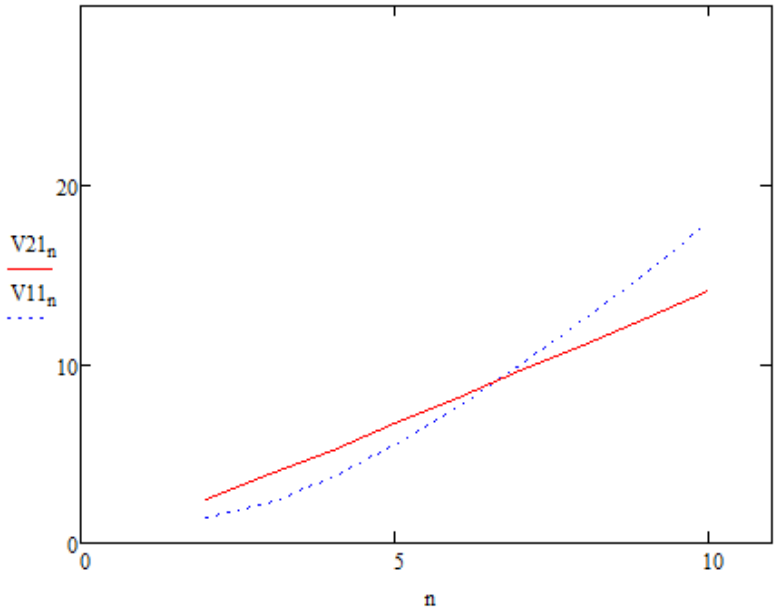

Рисунок 4.2 – Графік залежності часу перебування пакета в LSP-шляху при організації тунелю і без організації тунелю від кількості вузлів при ρ=0,3

На рис. 4.2 помітно, що час перебування пакета в мережі передачі даних з організацією тунелю – V1, на початковому етапі менше, ніж час проходження пакета по мережі без організації тунелю – V2. Проте необхідно зауважити, що після проходження пакетом сьомого вузла, час V1 починає суттєво збільшуватися, тоді як час проходження пакета по мережі без організації тунелю V2 зростає більш плавно.

Отже, після сьомого вузла пакет в мережі з організацією тунелю буде оброблятися повільніше, ніж в мережі без тунелю. Це відбувається через зчеплення пачок повідомлень, що робить істотний вплив на якість обслуговування. Процес зчеплення виникає в кожному вузлі n, починаючи з другого (n≠1), і визначається тим, що перший пакет k-й пачки пакетів наздоганяє у вузлі n останній пакет (k-1)-ї пачки, і обидві пачки – k і (k-1) – формують нову пачку («зчіплюються»). Детальніше дане явище висвітлено у третьому розділі.

Таким чином, організація тунелю при навантаженні мережі ρ=0,3 і середньої швидкості обслуговування 22 000 пак/с буде ефективна на мережі, що складається з семи вузлів.

Наступною дією є розрахунок ефективності тунелювання при навантаженні мережі ρ=0,4, що представлено на рис.4.3.

$$K2_n := 1 + n \cdot \frac{\rho 2}{1 - \rho 2}$$

$$V22_n := \sum_{n=1}^{n} \left[m \cdot \frac{1}{\mu 1} \cdot \frac{\left[1 - (K_n + 1) \cdot \rho 2^{K_n} + K_n \cdot \rho 2^{K_n + 1} \right]}{(1 - \rho 2^{K_n}) \cdot (1 - \rho 2)} \right]$$

$$n := 2 .. N$$

$$V12_n := \ln\left[(n-2)! \cdot \left(\frac{\rho 2}{1 - \rho 2} \right)^n \right] + n \cdot (1 + \gamma)$$

$K2_n =$	$V22_n =$	$V12_n =$
2.333	2.534	2.343
3	3.96	3.515
3.667	5.466	5.379
4.333	7.035	7.649
5	8.652	10.207
5.667	10.308	12.988
6.333	11.992	15.952
7	13.698	19.069
7.667	15.42	22.32

Рисунок 4.3 – Розрахунок ефективності побудови тунелю в мережі MPLS при навантаженні ρ=0,4

Графічне зображення результатів у вигляді графіків залежності часу перебування пакета в LSP-шляху при організації тунелю і без організації тунелю від кількості вузлів при ρ=0,4, що показано на рис.4.4

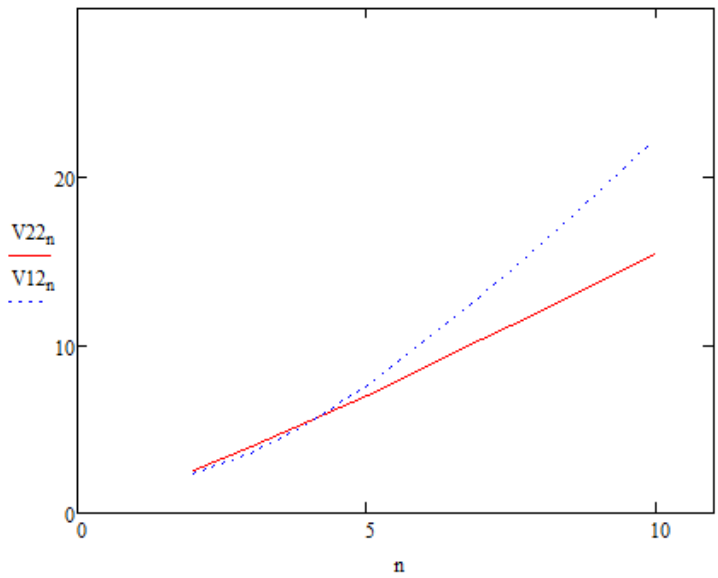

Рисунок 4.4 – Графік залежності часу перебування пакета в LSP-шляху при організації тунелю і без організації тунелю від кількості вузлів при ρ=0,4

На рис. 4.4 помітно ситуацію, схожу з попереднім випадком. Час перебування пакета в мережі передачі даних з організацією тунелю – V1 на початковому етапі трішки менше, ніж час проходження пакета по мережі без організації тунелю – V2. Хоча після проходження третього маршрутизатора відбувається зчеплення пачки пакетів і час їх перебування в тунелі стрімко зростає.

Таким чином, організацію тунелю при навантаженні мережі ρ=0,4 і середньої швидкості обслуговування 22 000 пак/с можна вважати не ефективною, бо результат можна отримати тільки при трьох вузлах і розходження в часі з тунелем та без незначне, приблизно $1*10^{-7} – 2*10^{-7}$с.

Наступним кроком необхідно провести розрахунок ефективності тунелювання при навантаженні мережі ρ=0,5, що представлено на рис. 4.5.

$$K3_n := 1 + n \cdot \frac{\rho 3}{1 - \rho 3}$$

$$V23_n := \sum_{n=1}^{n} \left[m \cdot \frac{1}{\mu 1} \cdot \frac{\left[1 - \left(K_n + 1 \right) \cdot \rho 3^{K_n} + K_n \cdot \rho 3^{K_n + 1} \right]}{\left(1 - \rho 3^{K_n} \right) \cdot (1 - \rho 3)} \right]$$

$$n := 2..N$$

$$V13_n := \ln\left[(n-2)! \cdot \left(\frac{\rho 3}{1 - \rho 3} \right)^n \right] + n \cdot (1 + \gamma)$$

$K3_n =$	$V23_n =$	$V13_n =$
3	3.154	2.595
4	4.731	4.089
5	7.001	5.692
6	9.677	7.387
7	12.64	9.159
8	15.826	10.997
9	19.195	12.888
10	22.718	14.824
11	26.375	16.797

Рисунок 4.5 – Розрахунок ефективності побудови тунелю в мережі MPLS при навантаженні ρ=0,5

Виведення результатів у вигляді графіків залежності часу перебування пакета в LSP-шляху при організації тунелю і без організації тунелю від кількості вузлів при ρ=0,5 вісвітленно на рис.4.6.

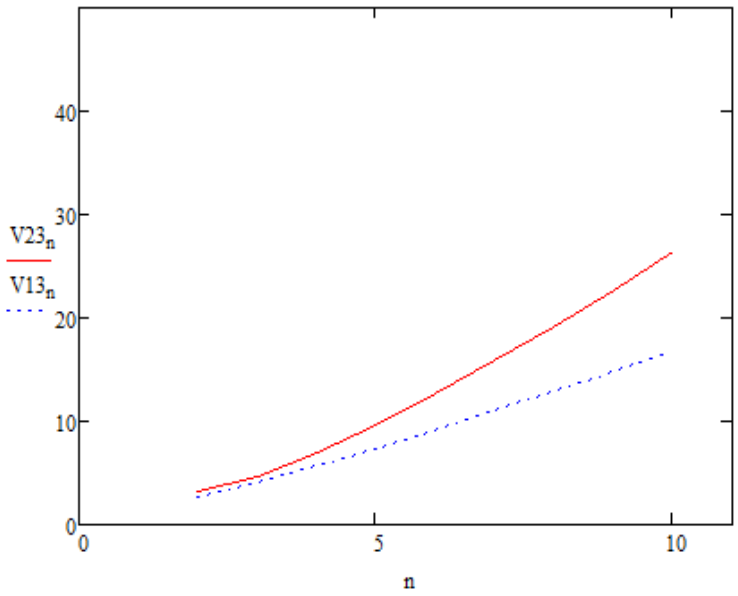

Рисунок 4.6 – Графік залежності часу перебування пакета в LSP-шляху при організації тунелю і без організації тунелю від кількості вузлів при ρ=0,5

На рис. 4.6 помітно, що організація тунелю ефективна на всій протяжності мережі. Хоча на початку маршруту час перебування пакетів в мережі без тунелю та з тунелем відрізняється несуттєво.

Продовження розрахунків ефективності тунелювання в мережі MPLS для завантаження ρ=0,6 представлено на рис. 4.7.

$$K4_n := 1 + n \cdot \frac{\rho 4}{1 - \rho 4}$$

$$V24_n := \sum_{n=1}^{n} \left[m \cdot \frac{1}{\mu 1} \cdot \frac{\left[1 - (K_n + 1) \cdot \rho 4^{K_n} + K_n \cdot \rho 4^{K_n + 1} \right]}{\left(1 - \rho 4^{K_n} \right) \cdot (1 - \rho 4)} \right]$$

$$n := 2..N$$

$$V14_n := \ln\left[(n-2)! \cdot \left(\frac{\rho 4}{1 - \rho 4} \right)^n \right] + n \cdot (1 + \gamma)$$

$K4_n =$	$V24_n =$	$V14_n =$
4	3.965	2.647
5.5	5.947	4.203
7	8.623	5.894
8.5	11.704	7.707
10	15.073	9.629
11.5	18.665	11.648
13	22.439	13.752
14.5	26.367	15.932
16	30.429	18.179

Рисунок 4.7 – Розрахунок ефективності побудови тунелю в мережі MPLS при навантаженні ρ=0,6

Результат розрахунків для ρ=0,6 у вигляді графіків представлено на рис.4.8.

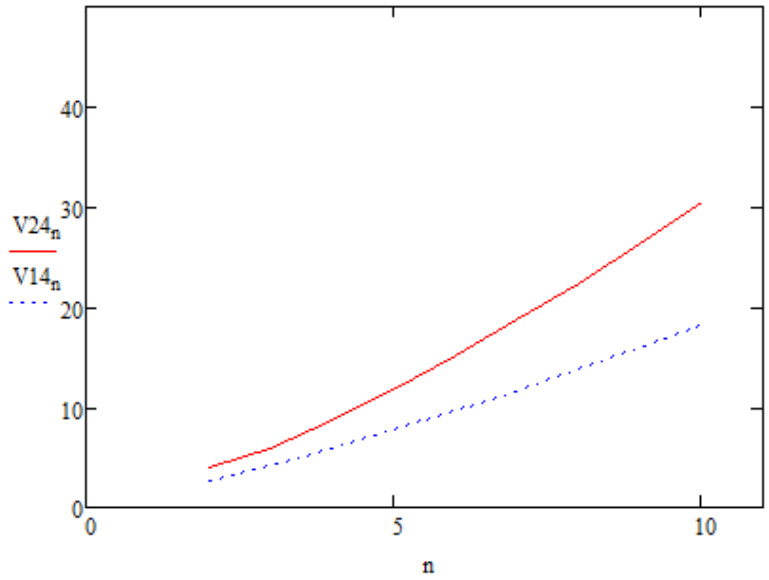

Рисунок 4.8 – Графік залежності V1 та V2 від кількості вузлів при ρ=0,6

На рис. 4.8 відображено результат розрахунків ефективності тунелювання при завантаженні мережі ρ=0,6, де явно зазначено, що побудова MPLS тунелю буде ефективною на всій ділянці даної мережі.

Далі проведено розрахунки для ρ=0,8 та представлено на рис. 4.9.

$$K5_n := 1 + n\cdot\frac{\rho 5}{1-\rho 5}$$

$$V25_n := \sum_{n=1}^{n}\left[m\cdot\frac{1}{\mu 1}\cdot\frac{\left[1-\left(K_n+1\right)\cdot\rho 5^{K_n}+K_n\cdot\rho 5^{K_n+1}\right]}{\left(1-\rho 5^{K_n}\right)\cdot(1-\rho 5)}\right]$$

$$n := 2..N$$

$$V15_n := \ln\left[(n-2)!\cdot\left(\frac{\rho 5}{1-\rho 5}\right)^n\right]+n\cdot(1+\gamma)$$

$K5_n$ =	$V25_n$ =	$V15_n$ =
9	5.927	2.733
13	8.89	4.392
17	12.546	6.236
21	16.608	8.258
25	20.958	10.452
29	25.531	12.81
33	30.286	15.327
37	35.195	17.995
41	40.238	20.808

Рисунок 4.9 – Розрахунок ефективності побудови тунелю в мережі MPLS при навантаженні ρ=0,8

Результат розрахунків для ρ=0,8 у вигляді графіків представлено на рис. 4.10.

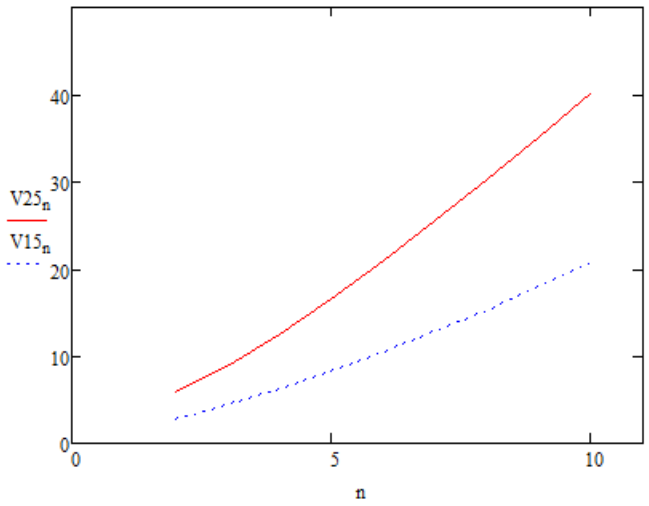

Рисунок 4.10 – Графік залежності V1 та V2 від кількості вузлів при ρ=0,8

З графіків, які представленні на рис. 4.10 помітно, що час перебування пакету в тунелі менший, ніж час перебування пакету в мережі без організації тунелю, середнє значення виграшу часу дорівнює $1{,}6*10^{-5}$с. Таким чином, для отримання виграшу в часі в даному випадку побудова тунелю необхідна.

Останні підрахунки були проведені для майже максимального завантаження, а саме ρ=0,95, що продемонстровано на рис. 4.11.

$$K6_n := 1 + n\cdot\frac{\rho б}{1-\rho б}$$

$$V26_n := \sum_{n=1}^{n}\left[m\cdot\frac{1}{\mu 1}\cdot\frac{\left[1-(K_n+1)\cdot\rho б^{K_n}+K_n\cdot\rho б^{K_n+1}\right]}{(1-\rho б^{K_n})\cdot(1-\rho б)}\right]$$

$$n := 2..N$$

$$V16_n := \ln\left[(n-2)!\cdot\left(\frac{\rho б}{1-\rho б}\right)^n\right] + n\cdot(1+\gamma)$$

$K6_n$ =	$V26_n$ =	$V16_n$ =
39	9.043	2.786
58	13.564	4.508
77	18.779	6.448
96	24.399	8.604
115	30.307	10.973
134	36.438	13.555
153	42.751	16.349
172	49.218	19.351
191	55.819	22.56

Рисунок 4.11 – Розрахунок ефективності побудови тунелю в мережі MPLS при навантаженні ρ=0,8

Результат розрахунків для ρ=0,95 у вигляді графіків представлено на рис. 4.12.

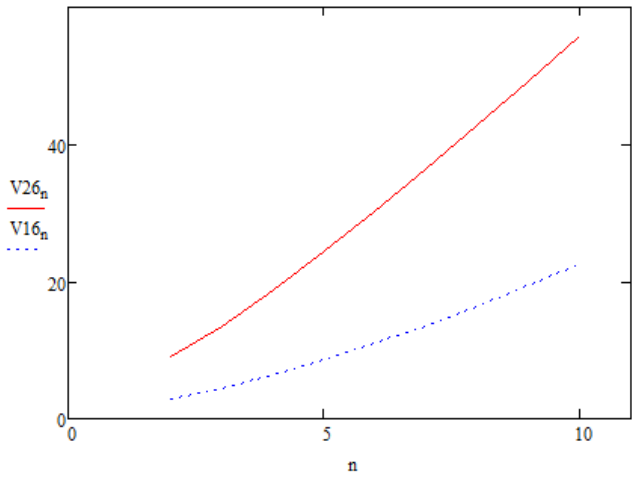

Рисунок 4.12 – Графік залежності V1 та V2 від кількості вузлів при ρ=0,8

На графіках, що представленні на рис. 4.12 помітно беззаперечну необхідність створення тунелю та його ефективність. В даній ситуації виграш часу буде складати в середньому $2,45*10^{-5}$с.

Результати розрахунків, що були проведені в роботі представлені в таблицях 4.1–4.3.

Таблиця 4.1 – Результати розрахунків величини пачки K_n

N	1	2	3	4	5	6	7	8	9	10
ρ=0,3										
$K1_n$	1,429	1,857	2,286	2,714	3,143	3,571	4	4,429	4,857	5,286
ρ=0,4										
$K2_n$	1,667	2,333	3	3,667	4,333	5	5,667	6,333	7	7,667
ρ=0,5										
$K3_n$	2	3	4	5	6	7	8	9	10	11
ρ=0,6										
$K4_n$	2,5	4	5,5	7	8,5	10	11,5	13	14,5	16
ρ=0,8										
$K5_n$	5	9	13	17	21	25	29	33	37	41
ρ=0,95										
$K6_n$	20	39	58	77	96	115	134	153	172	191

Таблиця 4.2 – Результати розрахунків часу перебування пакету в LSP-шляху з організації тунелю (V1)

N	ρ=0,3	ρ=0,4	ρ=0,5	ρ=0,6	ρ=0,8	ρ=0,95
2	1,459	2,343	3,154	3,965	5,927	9,043
3	2,189	3,515	4,731	5,947	8,89	13,564
4	3,612	5,379	7,001	8,623	12,546	18,779
5	5,44	7,649	9,677	11,704	16,608	24,399
6	7,556	10,207	12,64	15,073	20,958	30,307
7	9,895	12,988	15,826	18,665	25,531	36,438
8	12,417	15,952	19,195	22,439	30,286	42,751
9	15,092	19,069	22,718	26,367	35,195	49,218
10	17,902	22,32	26,375	30,429	40,238	55,819

Таблиця 4.3 – Результати розрахунків часу перебування пакету в мережі без організації тунелю (V2)

N	ρ=0,3	ρ=0,4	ρ=0,5	ρ=0,6	ρ=0,8	ρ=0,95
1	1,184	1,206	1,225	1,241	1,267	1,282
2	2,463	2,534	2,595	2,647	2,773	2,786
3	3,812	3,96	4,09	4,203	4,392	4,508
4	5,212	5,466	5,692	5,894	6,236	6,448
5	6,649	7,035	7,387	7,707	8,258	8,604
6	8,112	8,652	9,16	9,629	10,452	10,973
7	9,591	10,308	10,997	11,648	12,811	13,556
8	11,083	11,992	12,888	13,752	15,327	16,349
9	12,582	13,698	14,825	15,932	17,995	19,351
10	14,087	15,42	16,797	18,179	20,808	22,56

Отже, з отриманих результатів можна зробити висновки, що ефективність застосування технології MPLS при різних навантаженнях залежить від кількості вузлів. Так, при навантаженні ρ=0,3 найбільша ефективність досягається при семи вузлах, а при навантаженні ρ=0,4 побудова тунелю має сенс тільки на трьох вузлах на початку мережі, хоча різниця в часі між пакетом мережі та в тунелі на даному відрізку незначна, а після проходження третього маршрутизатора пакет в мережі з організацією тунелю буде оброблятися повільніше, ніж в мережі без тунелю. Це

відбувається через зчеплення пачок повідомлень, що робить істотний вплив на якість обслуговування.

Найбільш ефективне використання технології помітно у навантаженні на мережу ρ=0,6 – 0,95. Але, необхідно зауважити, що на початку мережі час просування пакету в мережі, та в тунелі різниться не суттєво, а найбільшу ефективність застосування тунелювання показує при збільшенні кількості вузлів, в тунелі час обробки зростає плавно, повільніше, про що свідчать графіки в даному розділі.

Також необхідно пам'ятати, технологія MPLS забезпечує широкий діапазон функціональних можливостей і додатків. Вона рідко використовується самостійно, а зазвичай накладається на технології 2-го рівня, і повинна працювати спільно з іншими протоколами в площині управління, такими як протоколи маршрутизації IP.

5 ПОБУДОВА ТА НАЛАШТУВАННЯ ФРАГМЕНТУ MPLS МЕРЕЖІ В СИМУЛЯТОРІ GNS3

5.1 Вибір середовища для відтворення мережі

GNS3 – це графічний симулятор створення мереж, який дозволяє змоделювати віртуальну мережу з маршрутизаторів і віртуальних машин. Працює практично на всіх платформах. На жаль, є один цілком закономірний мінус: система дуже вимоглива до ресурсів обладнання, на якому запущена.

Цікавою особливістю GNS3 є можливість з'єднання проектованої топології з реальною мережею. Це дає просто унікальну можливість перевірити на практиці будь-який проект без використання реального обладнання. Використання WireShark дозволяє провести моніторинг трафіку всередині проектованої топології, що дає додаткову інформацію для розуміння досліджуваних технологій. Після встановлення програми були проведені налаштування, та додані необхідні доступні образи. Вагомою перевагою GNS3 є простота і зручність при створенні проектів.

Однією з поставлених задач у роботі – необхідно було відтворити фрагмент MPLS мережі, встановити налаштування на кожному окремому вузлі. Даний пакет надає таку можливість. Мережа основана на маршрутизаторах Cisco c7200, з додавання Fast Ethernet модулів. Також для виконання поставленої задачі був розглянутий пакет Cisco Packet Tracer Student, який також знаходиться у вільному доступі. Але ознайомившись детальніше, було виявленно, що даний симулятор не підтримує налаштування MPLS мереж. Таким чином, було обрано GNS3.

5.2 Побудова та налаштування MPLS мережі

Необхідно зазначити, що сам по собі чистий MPLS застосовується рідко. Зазвичай основним застосуванням є MPLS-L2VPN, MPLS-L3VPN, MPLS-TE Але однією з основних задач роботи – необхідно було продемонструвати налаштування та використання безпосередньо самої технології, та прокладання LSP-тунелів. Виграш в продуктивності незначний, але різниця є і полягає вона в тому, що в одному випадку треба заглянути в FIB та поміняти деякі поля у заголовках, а в іншому – подивитися таблицю міток, помінявши мітку в заголовку MPLS. Цей факт

був перевірений в симуляторі GNS3 командою ping ip після звичайного налаштування IP-мережі, а також після встановлення на кожному вузлі налаштувань MPLS. Результати представлені на рис. 5.22 та рис. 5.23 відповідно.

Незважаючи на те, що MPLS не прив'язується до типу мережі, на якій він буде працювати, в наш час він живе в симбіозі тільки з IP. Тобто сама мережа будується поверх IP, але переносити при цьому вона може дані багатьох інших протоколів [15].

Перш ніж почати налаштування, необхідно побудувати мережу. В даному випадку існує фрагмент мережі, який включає в себе 10 вузлів – маршрутизаторів (рис. 5.1), які в свою чергу поділяються на R1 – Ingress LSR – точка входу в мережу MPLS, вхідний маршрутизатор, граничний маршрутизатор. R10 – Egress LSR – точка виходу, вихідний вузол, та R2 – R9 (LSR) – транзитні вузли. Всі IP-адреси, які були використані при налаштуванні мережі занесені до таблиці 5.1.

При налаштуванні IP-мережі використовувався протокол OSPF – протокол динамічної маршрутизації, заснований на технології відстеження стану каналу і використовує для знаходження найкоротшого шляху алгоритм Дейкстри.

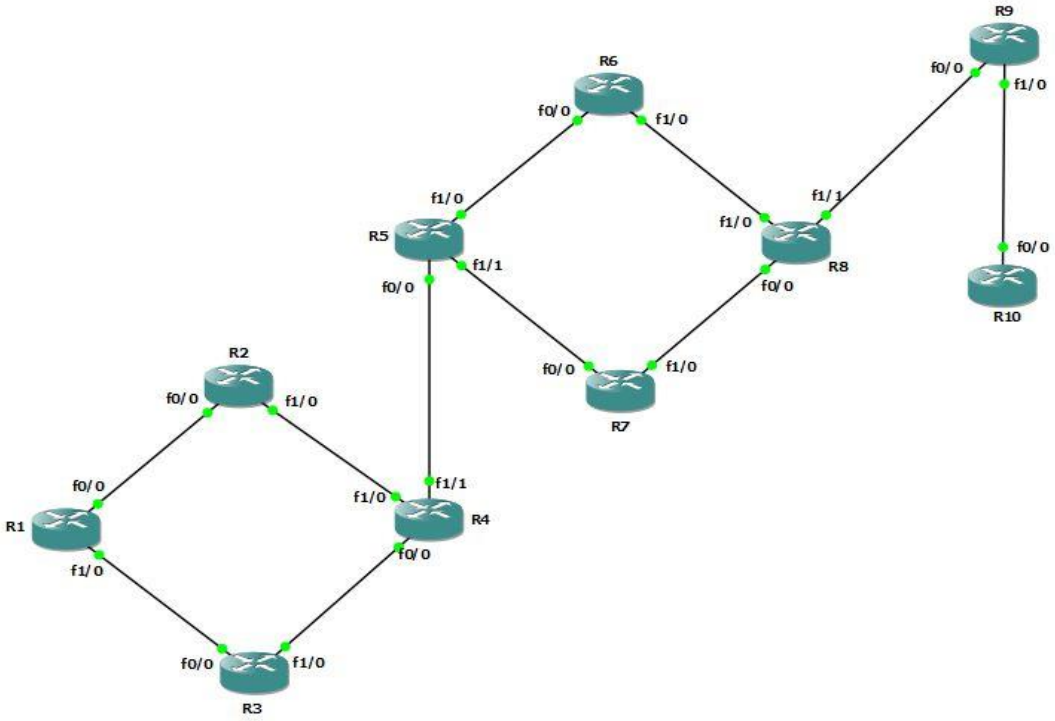

Рисунок 5.1 – Топологія побудованої мережі MPLS

Таблиця 5.1 – IP адреси вузлів обраного фрагмента мережі

	loopback	fa 0/0	fa 1/0	fa 1/1

R1	ip 10.10.10.10	ip 1.1.1.1	ip 2.2.2.1	–
R2	ip 20.20.20.20	ip 1.1.1.2	ip 3.3.3.2	–
R3	ip 30.30.30.30	ip 2.2.2.2	ip 4.4.4.2	–
R4	ip 40.40.40.40	ip 4.4.4.1	ip 3.3.3.1	ip 5.5.5.1
R5	ip 50.50.50.50	ip 5.5.5.2	ip 6.6.6.2	ip 7.7.7.2
R6	ip 60.60.60.60	ip 6.6.6.1	ip 8.8.8.1	–
R7	ip 70.70.70.70	ip 7.7.7.1	ip 9.9.9.1	–
R8	ip 80.80.80.80	ip 9.9.9.2	ip 8.8.8.2	ip 11.11.11.2
R9	ip 90.90.90.90	ip 11.11.11.1	ip 12.12.12.1	–
R10	ip 15.15.15.15	ip 12.12.12.2	–	–

Наступним кроком після побудови топології, слід провести налаштування вузлів. Спершу було проведено налаштування IP-мережі на кожному вузлі, починаючи з першого (рис. 5.2).

```
R1#en
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int loopback 0
R1(config-if)#ip address 10.10.10.10 255.255.255.255
R1(config-if)#exit
R1(config)#int fa 0/0
R1(config-if)#ip address 1.1.1.1 255.255.255.252
R1(config-if)#no sh
R1(config-if)#exit
R1(config)#int fa 1/0
R1(config-if)#ip address 2.2.2.1 255.255.255.252
R1(config-if)#no sh
R1(config-if)#exit
R1(config)#router ospf 1
R1(config-router)#passive-interface default
R1(config-router)#no passive-interface fastEthernet 0/0
R1(config-router)#no passive-interface fastEthernet 1/0
R1(config-router)#network 1.1.1.0 0.0.0.3 area 0
R1(config-router)#network 2.2.2.0 0.0.0.3 area 0
R1(config-router)#network 10.10.10.10 0.0.0.0 area 0
*Dec  4 23:46:01.943: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Dec  4 23:46:02.007: %LINK-3-UPDOWN: Interface FastEthernet1/0, changed state to up
*Dec  4 23:46:02.943: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R1(config-router)#network 10.10.10.10 0.0.0.0 area 0
*Dec  4 23:46:03.007: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed state to up
R1(config-router)#network 10.10.10.10 0.0.0.0 area 0
R1(config-router)#
R1(config-router)#exit
R1(config)#exit
R1#w
*Dec  4 23:46:25.283: %SYS-5-CONFIG_I: Configured from console by console
R1#wr
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
Building configuration...
[OK]
R1#
R1#
*Dec  4 23:47:06.263: %OSPF-5-ADJCHG: Process 1, Nbr 20.20.20.20 on FastEthernet0/0 from LOADING to FULL, Load
ing Done
R1#
```

Рисунок 5.2 – Налаштування першого вузла R1

Після налаштування IP-мережі необхідно поверх неї запустити технологію MPLS. Налаштування MPLS виконується окремо на кожному вузлі, починаючи з першого (рис. 5.3).

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip cef
R1(config)#mpls ip
R1(config)#mpls label protocol ldp
R1(config)#mpls ldp router-id loopback 0
R1(config)#int fa 0/0
R1(config-if)#mpls ip
R1(config-if)#mpls mtu 1512
R1(config-if)#exit
R1(config)#int fa 1/0
R1(config-if)#mpls ip
R1(config-if)#mpls mtu 1512
R1(config-if)#exit
R1(config)#exit
R1#
*Dec  5 00:46:52.307: %SYS-5-CONFIG_I: Configured from console by console
R1#
R1#
R1#
*Dec  5 00:47:44.027: %LDP-5-NBRCHG: LDP Neighbor 20.20.20.20:0 is UP
R1#
*Dec  5 00:48:35.751: %LDP-5-NBRCHG: LDP Neighbor 30.30.30.30:0 is UP
```

Рисунок 5.3 – Налаштування MPLS на першому вузлі

На рис. 5.4 представлено налаштування другого вузла мережі – одного з транзитних маршрутизаторів.

```
R2#en
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#int loopback 0
R2(config-if)#ip address 20.20.20.20 255.255.255.255
R2(config-if)#exit
R2(config)#int fa 0/0
R2(config-if)#ip address 1.1.1.2 255.255.255.252
R2(config-if)#no sh
R2(config-if)#exit
R2(config)#int fa 1/0
R2(config-if)#ip address 3.3.3.2 255.255.255.252
R2(config-if)#no sh
R2(config-if)#exit
R2(config)#router ospf 1
R2(config-router)#network 1.1.1.0 0.0.0.3 area 0
R2(config-router)#network 3.3.3.0 0.0.0.3 area 0
R2(config-router)#network 20.20.20.20 0.0.0.0 area 0
R2(config-router)#
*Dec  4 23:47:00.955: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Dec  4 23:47:00.999: %LINK-3-UPDOWN: Interface FastEthernet1/0, changed state to up
*Dec  4 23:47:01.955: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R2(config-router)#
*Dec  4 23:47:01.999: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed state to up
R2(config-router)#
*Dec  4 23:47:06.907: %OSPF-5-ADJCHG: Process 1, Nbr 10.10.10.10 on FastEthernet0/0 from LOADING to FULL, Load
ing Done
R2(config-router)#exit
R2(config)#exit
R2#
*Dec  4 23:47:25.455: %SYS-5-CONFIG_I: Configured from console by console
R2#wr
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
Building configuration...
[OK]
R2#
```

Рисунок 5.4 – Налаштування другого вузла R2

Далі на другому маршрутизаторі виконується налаштування технології MPLS (рис. 5.5).

```
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#ip cef
R2(config)#mpls ip
R2(config)#mpls label protocol ldp
R2(config)#mpls ldp router-id loopback 0
R2(config)#int fa 0/0
R2(config-if)#mpls ip
R2(config-if)#mpls mtu 1512
R2(config-if)#exit
R2(config)#int fa 1/0
R2(config-if)#mpls ip
R2(config-if)#mpls mtu 1512
R2(config-if)#exit
R2(config)#exit
R2#
*Dec  5 00:47:41.451: %SYS-5-CONFIG_I: Configured from console by console
R2#
*Dec  5 00:47:44.215: %LDP-5-NBRCHG: LDP Neighbor 10.10.10.10:0 is UP
R2#
R2#
*Dec  5 00:49:38.807: %LDP-5-NBRCHG: LDP Neighbor 40.40.40.40:0 is UP
```

Рисунок 5.5 – Налаштування MPLS на другому вузлі

Виконано налаштування третього вузла (рис. 5.6).

```
R3#en
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#int loopback 0
R3(config-if)#ip address 30.30.30.30 255.255.255.255
R3(config-if)#exit
R3(config)#int fa 0/0
R3(config-if)#ip address 2.2.2.2 255.255.255.252
R3(config-if)#no sh
R3(config-if)#exit
R3(config)#int fa 1/0
R3(config-if)#ip address 4.4.4.2 255.255.255.252
R3(config-if)#no sh
R3(config-if)#exit
R3(config)#router ospf 1
R3(config-router)#network 2.2.2.0 0.0.0.3 area 0
R3(config-router)#network 4.4.4.0 0.0.0.3 area 0
R3(config-router)#network 30.30.30.30 0.0.0.0 area 0
*Dec  4 23:50:56.855: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Dec  4 23:50:56.911: %LINK-3-UPDOWN: Interface FastEthernet1/0, changed state to up
*Dec  4 23:50:57.855: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R3(config-router)#network 30.30.30.30 0.0.0.0 area 0
R3(config-router)#
*Dec  4 23:50:57.911: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed state to up
R3(config-router)#U^
*Dec  4 23:51:06.367: %OSPF-5-ADJCHG: Process 1, Nbr 10.10.10.10 on FastEthernet0/0 from LOADING to FULL, Load
ing Done
R3(config-router)#exit
R3(config)#exit
R3#
*Dec  4 23:51:17.959: %SYS-5-CONFIG_I: Configured from console by console
```

Рисунок 5.6 – Налаштування третього вузла R3

Налаштовано MPLS на третьому вузлі (рис. 5.7).

```
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#ip cef
R3(config)#mpls ip
R3(config)#mpls label protocol ldp
R3(config)#mpls ldp router-id loopback 0
R3(config)#int fa 0/0
R3(config-if)#mpls ip
R3(config-if)#mpls mtu 1512
R3(config-if)#exit
R3(config)#int fa 1/0
R3(config-if)#mpls ip
R3(config-if)#mpls mtu 1512
R3(config-if)#exit
R3(config)#exit
R3#
*Dec  5 00:48:34.551: %SYS-5-CONFIG_I: Configured from console by console
*Dec  5 00:48:35.443: %LDP-5-NBRCHG: LDP Neighbor 10.10.10.10:0 is UP
R3#
R3#
*Dec  5 00:49:40.199: %LDP-5-NBRCHG: LDP Neighbor 40.40.40.40:0 is UP
```

Рисунок 5.7 – Налаштування MPLS на третьому вузлі

Виконано налаштування четвертого маршрутизатора (рис. 5.8).

```
R4#en
R4#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R4(config)#int loopback 0
R4(config-if)#ip address 40.40.40.40 255.255.255.255
R4(config-if)#exit
R4(config)#int fa 0/0
R4(config-if)#ip address 4.4.4.1 255.255.255.252
R4(config-if)#no sh
R4(config-if)#exit
R4(config)#int fa 1/0
R4(config-if)#ip address 3.3.3.1 255.255.255.252
R4(config-if)#no sh
R4(config-if)#exit
R4(config)#int fa 1/1
R4(config-if)#ip address 5.5.5.1 255.255.255.252
R4(config-if)#no sh
R4(config-if)#exit
R4(config)#router ospf 1
R4(config-router)#network 3.3.3.0 0.0.0.3 area 0
R4(config-router)#network 4.4.4.0 0.0.0.3 area 0
R4(config-router)#network 5.5.5.0 0.0.0.3 area 0
R4(config-router)#network 40.40.40.40 0.0.0.0 area 0
R4(config-router)#
*Dec  4 23:55:53.531: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Dec  4 23:55:53.587: %LINK-3-UPDOWN: Interface FastEthernet1/0, changed state to up
*Dec  4 23:55:53.651: %LINK-3-UPDOWN: Interface FastEthernet1/1, changed state to up
*Dec  4 23:55:54.531: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R4(config-router)#
*Dec  4 23:55:54.587: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed state to up
*Dec  4 23:55:54.651: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/1, changed state to up
R4(config-router)#
*Dec  4 23:56:00.263: %OSPF-5-ADJCHG: Process 1, Nbr 30.30.30.30 on FastEthernet0/0 from LOADING to FULL, Load
ing Done
R4(config-router)#
*Dec  4 23:56:04.191: %OSPF-5-ADJCHG: Process 1, Nbr 20.20.20.20 on FastEthernet1/0 from LOADING to FULL, Load
ing Done
R4(config-router)#exit
R4(config)#exit
R4#
*Dec  4 23:56:19.279: %SYS-5-CONFIG_I: Configured from console by console
```

Рисунок 5.8 – Налаштування четвертого вузла R4

Налаштовано MPLS на четвертому вузлі (рис. 5.9).

```
R4#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R4(config)#ip cef
R4(config)#mpls ip
R4(config)#mpls label protocol ldp
R4(config)#mpls ldp router-id loopback 0
R4(config)#int fa 0/0
R4(config-if)#mpls ip
R4(config-if)#mpls mtu 1512
R4(config-if)#exit
R4(config)#int fa 1/0
R4(config-if)#mpls ip
R4(config-if)#mpls mtu 1512
R4(config-if)#exit
R4(config)#int fa 1/1
R4(config-if)#mpls ip
R4(config-if)#mpls mtu 1512
R4(config-if)#exit
R4(config)#exit
R4#
*Dec  5 00:49:37.115: %SYS-5-CONFIG_I: Configured from console by console
R4#
*Dec  5 00:49:38.227: %LDP-5-NBRCHG: LDP Neighbor 20.20.20.20:0 is UP
R4#
*Dec  5 00:49:40.159: %LDP-5-NBRCHG: LDP Neighbor 30.30.30.30:0 is UP
R4#E{M'}T
R4#p}
R4#
R4#E{M'}T
R4#p}
R4#
R4#
*Dec  5 01:06:21.675: %LDP-5-NBRCHG: LDP Neighbor 50.50.50.50:0 is UP
```

Рисунок 5.9 – Налаштування MPLS на четвертому вузлі

На рис. 5.10 представлено налаштування п'ятого вузла мережі – одного з транзитних маршрутизаторів.

```
R5#en
R5#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R5(config)#int loopback 0
R5(config-if)#ip address 50.50.50.50 255.255.255.255
R5(config-if)#exit
R5(config)#int fa 0/0
R5(config-if)#ip address 5.5.5.2 255.255.255.252
R5(config-if)#no sh
R5(config-if)#exit
R5(config)#int fa 1/0
R5(config-if)#ip address 6.6.6.2 255.255.255.252
R5(config-if)#no sh
R5(config-if)#exit
R5(config)#int fa 1/1
R5(config-if)#ip address 7.7.7.2 255.255.255.252
R5(config-if)#no sh
R5(config-if)#exit
R5(config)#router ospf 1
R5(config-router)#network 5.5.5.0 0.0.0.3 area 0
R5(config-router)#network 6.6.6.0 0.0.0.3 area 0
R5(config-router)#network 7.7.7.0 0.0.0.3 area 0
R5(config-router)#network 50.50.50.50 0.0.0.0 area 0
R5(config-router)#
*Dec  4 23:58:00.563: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Dec  4 23:58:00.611: %LINK-3-UPDOWN: Interface FastEthernet1/0, changed state to up
*Dec  4 23:58:00.675: %LINK-3-UPDOWN: Interface FastEthernet1/1, changed state to up
*Dec  4 23:58:01.563: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R5(config-router)#
*Dec  4 23:58:01.611: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed state to up
*Dec  4 23:58:01.675: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/1, changed state to up
R5(config-router)#
*Dec  4 23:58:07.687: %OSPF-5-ADJCHG: Process 1, Nbr 40.40.40.40 on FastEthernet0/0 from LOADING to FULL, Loading Done
R5(config-router)#exit
R5(config)#exit
R5#
*Dec  4 23:58:15.451: %SYS-5-CONFIG_I: Configured from console by console
```

Рисунок 5.10 – Налаштування п'ятого вузла R5

Налаштовано MPLS на п'ятому вузлі (рис. 5.11).

```
R5#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R5(config)#ip cef
R5(config)#mpls ip
R5(config)#mpls label protocol ldp
R5(config)#mpls ldp router-id loopback 0
R5(config)#int fa 0/0
R5(config-if)#mpls ip
R5(config-if)#mpls mtu 1512
R5(config-if)#exit
R5(config)#int fa 1/0
R5(config-if)#mpls ip
R5(config-if)#mpls mtu 1512
R5(config-if)#exit
R5(config)#int fa 1/1
R5(config-if)#mpls ip
R5(config-if)#mpls mtu 1512
R5(config-if)#exit
R5(config)#exit
R5#
*Dec  5 01:06:18.999: %SYS-5-CONFIG_I: Configured from console by console
R5#
*Dec  5 01:06:22.215: %LDP-5-NBRCHG: LDP Neighbor 40.40.40.40:0 is UP
R5#
*Dec  5 01:07:40.423: %LDP-5-NBRCHG: LDP Neighbor 60.60.60.60:0 is UP
R5#
*Dec  5 01:08:22.515: %LDP-5-NBRCHG: LDP Neighbor 70.70.70.70:0 is UP
R5#
```

Рисунок 5.11 – Налаштування MPLS на п'ятому вузлі

Виконано налаштування шостого транзитного вузла мережі (рис. 5.12).

```
R6#en
R6#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R6(config)#int loopback 0
R6(config-if)#ip address 60.60.60.60 255.255.255.255
R6(config-if)#exit
R6(config)#int fa 0/0
R6(config-if)#ip address 6.6.6.1 255.255.255.252
R6(config-if)#no sh
R6(config-if)#exit
R6(config)#int fa 1/0
R6(config-if)#ip address 8.8.8.1 255.255.255.252
R6(config-if)#no sh
R6(config-if)#exit
R6(config)#router ospf 1
R6(config-router)#network 6.6.6.0 0.0.0.3 area 0
R6(config-router)#network 8.8.8.0 0.0.0.3 area 0
R6(config-router)#network 60.60.60.60 0.0.0.0 area 0
R6(config-router)#exit
R6(config)#exit
R6#
*Dec  5 00:21:04.171: %SYS-5-CONFIG_I: Configured from console by console
R6#
*Dec  5 00:21:04.663: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Dec  5 00:21:04.723: %LINK-3-UPDOWN: Interface FastEthernet1/0, changed state to up
*Dec  5 00:21:05.663: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R6#
*Dec  5 00:21:05.723: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed state to up
R6#
*Dec  5 00:21:13.611: %OSPF-5-ADJCHG: Process 1, Nbr 80.80.80.80 on FastEthernet1/0 from LOADING to FULL, Load
ing Done
*Dec  5 00:21:13.835: %OSPF-5-ADJCHG: Process 1, Nbr 50.50.50.50 on FastEthernet0/0 from LOADING to FULL, Load
```

Рисунок 5.12 – Налаштування шостого вузла R6

Налаштовано MPLS на шостому маршрутизаторі (рис. 5.13).

```
R6#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R6(config)#ip cef
R6(config)#mpls ip
R6(config)#mpls label protocol ldp
R6(config)#mpls ldp router-id loopback 0
R6(config)#int fa 0/0
R6(config-if)#mpls ip
R6(config-if)#mpls mtu 1512
R6(config-if)#exit
R6(config)#int fa 1/0
R6(config-if)#mpls ip
R6(config-if)#mpls mtu 1512
R6(config-if)#exit
R6(config)#exit
R6#
*Dec  5 01:07:38.279: %SYS-5-CONFIG_I: Configured from console by console
R6#
*Dec  5 01:07:39.923: %LDP-5-NBRCHG: LDP Neighbor 50.50.50.50:0 is UP
R6#
*Dec  5 01:09:31.683: %LDP-5-NBRCHG: LDP Neighbor 80.80.80.80:0 is UP
```

Рисунок 5.13 – Налаштування MPLS на шостому вузлі

На рис. 5.14 представлено налаштування сьомого вузла мережі – одного з транзитних маршрутизаторів.

```
R7#en
R7#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R7(config)#int loopback 0
R7(config-if)#ip address 70.70.70.70 255.255.255.255
R7(config-if)#exit
R7(config)#int fa 0/0
R7(config-if)#ip address 7.7.7.1 255.255.255.252
R7(config-if)#no sh
R7(config-if)#exit
R7(config)#int fa 1/0
R7(config-if)#ip address 9.9.9.1 255.255.255.252
R7(config-if)#no sh
R7(config-if)#exit
R7(config)#router ospf 1
R7(config-router)#network 7.7.7.0 0.0.0.3 area 0
R7(config-router)#network 9.9.9.0 0.0.0.3 area 0
R7(config-router)#network 70.70.70.70 0.0.0.0 area 0
R7(config-router)#exit
R7(config)#exit
R7#
*Dec  5 00:27:51.643: %SYS-5-CONFIG_I: Configured from console by console
R7#
*Dec  5 00:27:51.951: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Dec  5 00:27:52.019: %LINK-3-UPDOWN: Interface FastEthernet1/0, changed state to up
*Dec  5 00:27:52.951: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R7#
*Dec  5 00:27:53.019: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed state to up
R7#
*Dec  5 00:28:00.887: %OSPF-5-ADJCHG: Process 1, Nbr 80.80.80.80 on FastEthernet1/0 from LOADING to FULL, Loading Done
R7#
R7#
*Dec  5 00:28:03.723: %OSPF-5-ADJCHG: Process 1, Nbr 50.50.50.50 on FastEthernet0/0 from LOADING to FULL, Loading Done
```

Рисунок 5.14 – Налаштування сьомого вузла R7

Далі на сьомому маршрутизаторі налаштовано технологію MPLS (рис. 5.15).

```
R7#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R7(config)#ip cef
R7(config)#mpls ip
R7(config)#mpls label protocol ldp
R7(config)#mpls ldp router-id loopback 0
R7(config)#int fa 0/0
R7(config-if)#mpls ip
R7(config-if)#mpls mtu 1512
R7(config-if)#exit
R7(config)#int fa 1/0
R7(config-if)#mpls ip
R7(config-if)#mpls mtu 1512
R7(config-if)#exit
R7(config)#exit
R7#wr
*Dec  5 01:08:17.543: %SYS-5-CONFIG_I: Configured from console by console
R7#wr
Building configuration...
[OK]
R7#
*Dec  5 01:08:21.275: %LDP-5-NBRCHG: LDP Neighbor 50.50.50.50:0 is UP
R7#
```

Рисунок 5.15 – Налаштування MPLS на сьомому вузлі

Виконано налаштування восьмого вузла – R8 (рис. 5.16).

```
R8#en
R8#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R8(config)#int loopback 0
R8(config-if)#ip address 80.80.80.80 255.255.255.255
R8(config-if)#exit
R8(config)#int fa 0/0
R8(config-if)#ip address 9.9.9.2 255.255.255.252
R8(config-if)#no sh
R8(config-if)#exit
R8(config)#int fa 1/0
R8(config-if)#ip address 8.8.8.2 255.255.255.252
R8(config-if)#no sh
R8(config-if)#exit
R8(config)#int fa 1/1
R8(config-if)#ip address 11.11.11.2 255.255.255.252
R8(config-if)#no sh
R8(config-if)#exit
R8(config)#router ospf 1
R8(config-router)#network 9.9.9.0 0.0.0.3 area 0
R8(config-router)#network 8.8.8.0 0.0.0.3 area 0
R8(config-router)#network 11.11.11.0 0.0.0.3 area 0
R8(config-router)#network 80.80.80.80 0.0.0.0 area 0
R8(config-router)#
*Dec  5 00:05:50.307: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Dec  5 00:05:50.359: %LINK-3-UPDOWN: Interface FastEthernet1/0, changed state to up
*Dec  5 00:05:50.431: %LINK-3-UPDOWN: Interface FastEthernet1/1, changed state to up
*Dec  5 00:05:51.307: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R8(config-router)#
*Dec  5 00:05:51.359: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed state to up
*Dec  5 00:05:51.431: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/1, changed state to up
R8(config-router)#
*Dec  5 00:05:56.495: %OSPF-5-ADJCHG: Process 1, Nbr 70.70.70.70 on FastEthernet0/0 from LOADING to FULL, Load
ing Done
R8(config-router)#exit
*Dec  5 00:06:04.231: %OSPF-5-ADJCHG: Process 1, Nbr 60.60.60.60 on FastEthernet1/0 from LOADING to FULL, Load
ing Done
R8(config-router)#exit
R8(config)#exit
R8#
*Dec  5 00:06:09.315: %SYS-5-CONFIG_I: Configured from console by console
```

Рисунок 5.16 – Налаштування восьмого вузла R8

Налаштування технології MPLS на восьмому вузлі (рис. 5.17).

```
R8#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R8(config)#ip cef
R8(config)#mpls ip
R8(config)#mpls label protocol ldp
R8(config)#mpls ldp router-id loopback 0
R8(config)#int fa 0/0
R8(config-if)#mpls ip
R8(config-if)#mpls mtu 1512
R8(config-if)#exit
R8(config)#int fa 1/0
R8(config-if)#mpls ip
R8(config-if)#mpls mtu 1512
R8(config-if)#exit
R8(config)#int fa 1/1
R8(config-if)#mpls ip
R8(config-if)#mpls mtu 1512
R8(config-if)#exit
R8(config)#exit
R8#
*Dec  5 01:09:28.851: %SYS-5-CONFIG_I: Configured from console by console
R8#
*Dec  5 01:09:29.919: %LDP-5-NBRCHG: LDP Neighbor 70.70.70.70:0 is UP
R8#
*Dec  5 01:09:31.631: %LDP-5-NBRCHG: LDP Neighbor 60.60.60.60:0 is UP
R8#
*Dec  5 01:10:11.891: %LDP-5-NBRCHG: LDP Neighbor 90.90.90.90:0 is UP
```

Рисунок 5.17 – Налаштування MPLS на восьмому вузлі

На рис. 5.18 представлено налаштування дев'ятого вузла обраного фрагмента мережі – передостаннього маршрутизатора.

```
R9#en
R9#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R9(config)#int loopback 0
R9(config-if)#ip address 90.90.90.90 255.255.255.255
R9(config-if)#exit
R9(config)#int fa 0/0
R9(config-if)#ip address 11.11.11.1 255.255.255.252
R9(config-if)#no sh
R9(config-if)#exit
R9(config)#int fa 1/0
R9(config-if)#ip address 12.12.12.1 255.255.255.252
R9(config-if)#no sh
R9(config-if)#exit
R9(config)#router ospf 1
R9(config-router)#network 11.11.11.0 0.0.0.3 area 0
R9(config-router)#network 12.12.12.0 0.0.0.3 area 0
R9(config-router)#network 90.90.90.90 0.0.0.0 area 0
R9(config-router)#exit
R9(config)#exit
R9#
*Dec  5 00:30:07.007: %SYS-5-CONFIG_I: Configured from console by console
R9#
*Dec  5 00:30:07.567: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Dec  5 00:30:07.567: %LINK-3-UPDOWN: Interface FastEthernet1/0, changed state to up
*Dec  5 00:30:08.567: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
*Dec  5 00:30:08.567: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed state to up
R9#
*Dec  5 00:30:14.647: %OSPF-5-ADJCHG: Process 1, Nbr 80.80.80.80 on FastEthernet0/0 from LOADING to FULL, Loading Done
```

Рисунок 5.18 – Налаштування дев'ятого вузла R9

Налаштовано MPLS на дев'ятому маршрутизаторі (рис. 5.19).

```
R9#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R9(config)#ip cef
R9(config)#mpls ip
R9(config)#mpls label protocol ldp
R9(config)#mpls ldp router-id loopback 0
R9(config)#int fa 0/0
R9(config-if)#mpls ip
R9(config-if)#mpls mtu 1512
R9(config-if)#exit
R9(config)#int fa 1/0
R9(config-if)#mpls ip
R9(config-if)#mpls mtu 1512
R9(config-if)#exit
R9(config)#exit
R9#
*Dec  5 01:10:09.043: %SYS-5-CONFIG_I: Configured from console by console
R9#
*Dec  5 01:10:11.575: %LDP-5-NBRCHG: LDP Neighbor 80.80.80.80:0 is UP
R9#
*Dec  5 01:10:37.259: %LDP-5-NBRCHG: LDP Neighbor 15.15.15.15:0 is UP
```

Рисунок 5.19 – Налаштування MPLS на дев'ятому вузлі

Останнім кроком налаштування обраного фрагменту мережі є встановлення налаштувань на кінцевий маршрутизатор R10 (рис. 5.20)

```
R10#en
R10#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R10(config)#int loopback 0
R10(config-if)#ip address 15.15.15.15 255.255.255.255
R10(config-if)#exit
R10(config)#int fa 0/0
R10(config-if)#ip address 12.12.12.2 255.255.255.252
R10(config-if)#no sh
R10(config-if)#exit
R10(config)#router ospf 1
R10(config-router)#passive-interface default
R10(config-router)#no passive-interface fastEthernet 0/0
R10(config-router)#network 12.12.12.0 0.0.0.3 area 0
R10(config-router)#network 15.15.15.15 0.0.0.0 area 0
R10(config-router)#exit
R10(config)#exit
R10#
*Dec  5 00:31:46.311: %SYS-5-CONFIG_I: Configured from console by console
R10#
*Dec  5 00:31:47.159: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Dec  5 00:31:48.159: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R10#
*Dec  5 00:31:51.919: %OSPF-5-ADJCHG: Process 1, Nbr 90.90.90.90 on FastEthernet0/0 from LOADING to FULL, Loading Done
```

Рисунок 5.20 – Налаштування десятого вузла R10

Далі на десятому вузлі налаштовано технологію MPLS (рис. 5.21).

```
R10#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R10(config)#ip cef
R10(config)#mpls ip
R10(config)#mpls label protocol ldp
R10(config)#mpls ldp router-id loopback 0
R10(config)#int fa 0/0
R10(config-if)#mpls ip
R10(config-if)#mpls mtu 1512
R10(config-if)#exit
R10(config)#exit
R10#
*Dec  5 01:10:34.355: %SYS-5-CONFIG_I: Configured from console by console
R10#
*Dec  5 01:10:37.899: %LDP-5-NBRCHG: LDP Neighbor 90.90.90.90:0 is UP
```

Рисунок 5.21 – Налаштування MPLS на десятому вузлі

Необхідно зазначити основні команди, що були використані для налаштування MPLS мережі: ip cef – ввімкнути Cisco Express Forwarding, технологія швидкої комутації пакетів на 3-му рівні компанії Cisco [16]; mpls ip – ввімкнути глобально процес комутації по мітках (MPLS); mpls label protocol ldp – обрати протокол, по якому будуть обмінюватися мітками LSR між собою; mpls ldp router-id loopback 0 – визначити, який інтерфейс (IP-адреса) береться в якості ID роутера в процесі MPLS [17]; mpls ip – ввімкнути MPLS на інтерфейсі; mpls mtu 1512 – збільшити розмір mtu для уникнення фрагментації (розбивки) фреймів (стандартний розмір 1500).

Після закінчення налаштування всіх маршрутизаторів фрагмента мережі необхідно перевірити її працездатність. В консолі першого початкового вузла R1 введено команду ping ip та адресу порту маршрутизатора R10. Тобто виконується перевірка з'єднання початкового та кінцевого маршрутизатора. Виконавши команду, помітно, що пакети передаюсть без втрат, що свідчить про правильність налаштування IP-мережі Також команда ping ip показує час прийому-передачі пакету – мінімальний, середній, максимальний (рис 5.22).

```
R1#ping ip 12.12.12.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 12.12.12.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1448/1602/1708 ms
```

Рисунок 5.22 – Перевірка налаштування командою ping ip

При налаштуванні MPLS на вузлах помітно, що після активації даної технології відразу позначаються сусідні маршрутизатори, на яких вже були

проведені налаштування. Також, при необхідності перевірити сусідів конкретного вузла за проколом ldp можна командою sh mpls ldp nighbor (рис. 5.24).

```
R1#sh mpls ldp neighbor
    Peer LDP Ident: 20.20.20.20:0; Local LDP Ident 10.10.10.10:0
        TCP connection: 20.20.20.20.13210 - 10.10.10.10.646
        State: Oper; Msgs sent/rcvd: 90/91; Downstream
        Up time: 00:58:19
        LDP discovery sources:
          FastEthernet0/0, Src IP addr: 1.1.1.2
        Addresses bound to peer LDP Ident:
          1.1.1.2         3.3.3.2         20.20.20.20
    Peer LDP Ident: 30.30.30.30:0; Local LDP Ident 10.10.10.10:0
        TCP connection: 30.30.30.30.29955 - 10.10.10.10.646
        State: Oper; Msgs sent/rcvd: 89/89; Downstream
        Up time: 00:57:27
        LDP discovery sources:
          FastEthernet1/0, Src IP addr: 2.2.2.2
        Addresses bound to peer LDP Ident:
          2.2.2.2         4.4.4.2         30.30.30.30
```

Рисунок 5.24 – Приклад виведення сусідніх вузлів на одному з маршрутизаторів

Тепер за допомогою команди show mpls forwarding-table можна подивитися, які мітки призначено для кожного FEC – Forwarding Equivalence Class (рис. 5.25). FEC – це класи трафіку. У найпростішому випадку ідентифікатором класу є адресний префікс призначення, також можна сказати, що це IP-адреса або підмережа призначення.

Наприклад, є потоки трафіку від різних клієнтів і різних додатків, які йдуть всі на одну адресу – всі ці потоки належать одному класу – одному FEC – використовують один LSP.

Якщо взяти інші потоки від інших клієнтів і додатків на іншу адресу призначення – це буде відповідно інший клас і інший LSP.

За допомогою команди show mpls forwarding-table з додаванням FEC вузла призначення показано LSP-тунель від початку до кінцевої точки фрагмента мережі (рис. 5.26). LSP – Label Switched Path – шлях перемикання міток. Це односпрямований канал від Ingress LSR до Egress LSR, тобто шлях, по якому фактично пройде пакет через MPLS-мережа. Іншими словами – це послідовність LSR.

```
R1#sh mpls forwarding-table
Local  Outgoing    Prefix           Bytes tag  Outgoing   Next Hop
tag    tag or VC   or Tunnel Id     switched   interface
16     16          50.50.50.50/32   0          Fa0/0      1.1.1.2
       17          50.50.50.50/32   0          Fa1/0      2.2.2.2
17     18          70.70.70.70/32   0          Fa0/0      1.1.1.2
       18          70.70.70.70/32   0          Fa1/0      2.2.2.2
18     Pop tag     3.3.3.0/30       0          Fa0/0      1.1.1.2
19     Pop tag     4.4.4.0/30       0          Fa1/0      2.2.2.2
20     20          80.80.80.80/32   0          Fa0/0      1.1.1.2
       20          80.80.80.80/32   0          Fa1/0      2.2.2.2
21     Pop tag     20.20.20.20/32   0          Fa0/0      1.1.1.2
22     21          5.5.5.0/30       0          Fa0/0      1.1.1.2
       22          5.5.5.0/30       0          Fa1/0      2.2.2.2
23     22          6.6.6.0/30       0          Fa0/0      1.1.1.2
       23          6.6.6.0/30       0          Fa1/0      2.2.2.2
24     23          7.7.7.0/30       0          Fa0/0      1.1.1.2
       24          7.7.7.0/30       0          Fa1/0      2.2.2.2
25     24          8.8.8.0/30       0          Fa0/0      1.1.1.2
       25          8.8.8.0/30       0          Fa1/0      2.2.2.2
26     25          9.9.9.0/30       0          Fa0/0      1.1.1.2
       26          9.9.9.0/30       0          Fa1/0      2.2.2.2
27     26          40.40.40.40/32   0          Fa0/0      1.1.1.2
       27          40.40.40.40/32   0          Fa1/0      2.2.2.2
28     28          11.11.11.0/30    0          Fa0/0      1.1.1.2
       29          11.11.11.0/30    0          Fa1/0      2.2.2.2
29     29          12.12.12.0/30    0          Fa0/0      1.1.1.2
       30          12.12.12.0/30    0          Fa1/0      2.2.2.2
30     30          90.90.90.90/32   0          Fa0/0      1.1.1.2
       31          90.90.90.90/32   0          Fa1/0      2.2.2.2
31     31          60.60.60.60/32   0          Fa0/0      1.1.1.2
       32          60.60.60.60/32   0          Fa1/0      2.2.2.2
32     Pop tag     30.30.30.30/32   0          Fa1/0      2.2.2.2
33     33          15.15.15.15/32   0          Fa0/0      1.1.1.2
       33          15.15.15.15/32   0          Fa1/0      2.2.2.2
```

Рисунок 5.25 – Таблиця міток

Важливо розуміти, що LSP насправді односпрямований. Це означає, що, по-перше, трафік по ньому передається тільки в одному напрямку, по-друге, якщо існує шлях в одну сторону, не обов'язково існує назад, по-третє, повертається не обов'язково тим самим шляхом, яким прийшов до точки. Все ж таки слід зазначити, що це схоже трохи на IP-маршрутизацію. Незважаючи на те, що існує шлях від точки А до точки Б, таблиця маршрутизації знає тільки наступний вузол, куди треба відправляти трафік. Але різниця в тому, що LSR не приймає рішення, що до кожного пакета на основі адреси призначення – шлях визначений заздалегідь.

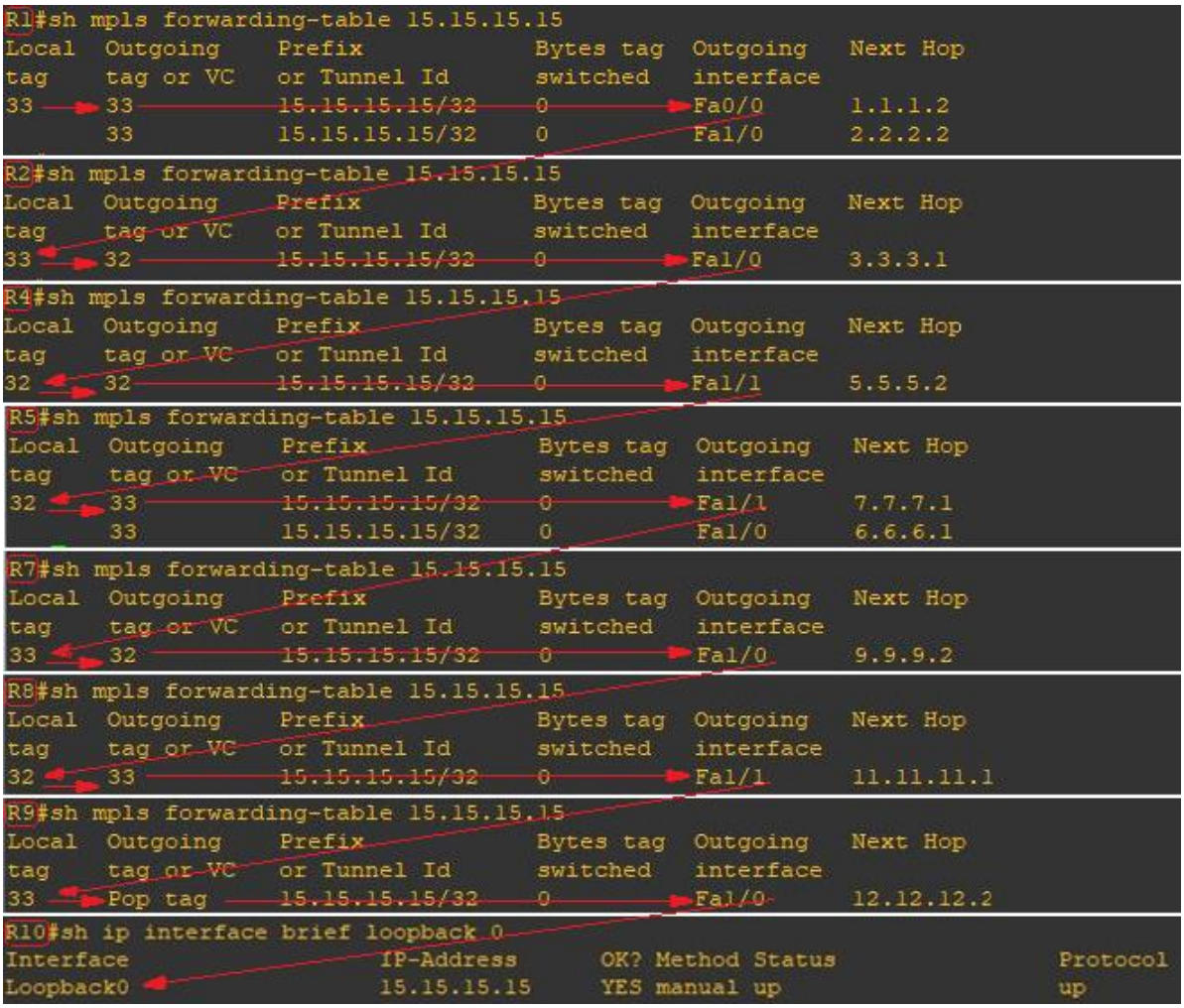

Рисунок 5.26 – LSP тунель

Отже, в даному розділі було побудовано та налаштовано фрагмент мережі, який включає в себе 10 вузлів – маршрутизаторів. Які в свою чергу поділяються на R1 – Ingress LSR – точка входу в мережу MPLS, вхідний маршрутизатор, граничний маршрутизатор. R10 – Egress LSR – точка виходу, вихідний вузол, та R2 – R9 (LSR) – транзитні вузли. Кожен маршрутизатор був окремо налаштований. Спочатку введені налаштування для організації IP-мережі, після чого проведено налаштування MPLS технології.

Також було продемонстровано команди, що дозволяють переглянути призначення MPLS міток для кожного маршрутизатора. Представлено знаходження сусідніх вузлів та показано один з побудованих LSP-тунелів.

В даному випадку технологія MPLS дозволяє істотно підвищити швидкість транспортування пакетів від відправника до отримувача через маршрутизовані мережі, за рахунок кешування маршруту за принципом роботи технології CEF – Cisco Express Forwarding. А також за допомогою MPLS значно підвищилась

захищеність інформації, що передається в пакетах мережею. Бо даний механізм не слідкує за вмістом пакету, а зчитує тільки додатковий транспортний заголовок яким наділений кожен пакет.

Швидкість обробки пакетів маршрутизатором збільшується за рахунок зменшення кількості оброблюваної маршрутної інформації, відбувається її приміщення в пам'ять кешу маршрутизатора і переходу на другий рівень моделі OSI. При застосуванні технології MPLS, маршрутизатор не звіряється з таблицею маршрутизації, не вираховує IP-адресу next-hop, а обробляє і перенаправляє пакети згідно з номером мітки, що надана кожному пакету. Дана позначка розміщується в заголовку пакета між MAC-адресою і IP-адресою. Величина мітки дорівнює 32 бітам або 12 байтам.

Після включення MPLS, маршрутизатор відразу привласнює унікальні мітки у вигляді номера всіх мереж, що містяться в його таблиці маршрутизації таблицю маршрутизації можна подивитися командою show ip route, і поміщає їх в таблицю LIB – Label Information Base, в якій містяться мітки для існуючих в таблиці маршрутизації мереж.

Далі вузлам необхідно обмінятися своїми мітками за допомогою протоколу LDP. Виконати подібно це до того, як обмінюються маршрутами по протоколом OSPF, після чого результати обміну заносяться в таблицю LFIB – Label Forwarding Information Base, яка визначає маршрут по мітках. В процесі роботи протоколу LDP, маршрутизатор не складає повну топологію мережі, він всього лише заносить в свою пам'ять мітку і номер інтерфейсу, через який доступна Ваша мережа.

Найпростіший функціонал MPLS налаштовується в режимі конфігурації интерфеса командою mpls ip. LDP включається за допомогою команди mpls label protocol ldp. Вище було згадано, що розмір мітки в заголовку пакета дорівнює 12 байтам, тому щоб уникнути фрагментації пакетів, необхідно збільшити його розмір задавши значення командою mpls mtu 1512 (стандартний розмір 1500) також в режимі конфігурації інтерфейсу.

5.3 Налаштування MPLS L2VPN

MPLS L2VPN – це набір технологій, транспортом для яких виступає MPLS LSP. Саме він зараз отримав найбільш широке поширення в мережах провайдерів.

Головна причина чому обрано саме MPLS L2VPN полягає безумовно, в здатності маршрутизаторів, що передають MPLS-пакети абстрагуватися від їх вмісту, але при цьому розрізняти трафік різних сервісів. Наприклад, передаючи E1-кадр, він приходить на граничний маршрутизатор MPLS-мережі провайдера, відразу ж інкапсулюється в MPLS і вже ніхто по дорозі навіть не запідозрить, що там всередині – важливо тільки вчасно замінити мітку. А на інший порт приходить Ethernet-кадр і за тим самим LSP він може пройти по мережі, тільки з іншого міткою VPN. А крім того така технологія дозволяє будувати канали з урахуванням вимог трафіку до параметрів мережі.

Після налаштування технології MPLS на кожному маршрутизаторі мережі необхідно впровадити налаштування для вузлів між якими буде налаштоване VPN з'єднання. В даному випадку це вузли R1 та R10.

MPLS L2VPN налаштовано на першому, відправному маршрутизаторі R1 (рис.5.28) та на кінцевому маршрутизаторі-отримувачі R10 (рис.5.27)

```
R10#en
R10#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R10(config)#ip cef
R10(config)#mpls ip
R10(config)#mpls label protocol ldp
R10(config)#mpls ldp router-id loopback 0
R10(config)#int loopback 0
R10(config-if)#ip address 15.15.15.15 255.255.255.255
R10(config-if)#exit
R10(config)#int fa 0/0
R10(config-if)#ip address 12.12.12.2 255.255.255.252
R10(config-if)#no sh
R10(config-if)#mtu 1512
% Interface FastEthernet0/0 does not support user settable mtu.
R10(config-if)#mpls ip
R10(config-if)#mpls mtu 1512
R10(config-if)#exit
R10(config)#router ospf 1
R10(config-router)#passive-interface default
R10(config-router)#no passive-interface fastEthernet 0/0
R10(config-router)#network 15.15.15.15 0.0.0.0 area 0
R10(config-router)#network 12.12.12.0 0.0.0.3 area 0
R10(config-router)#exit
R10(config)#int fa 0/0.20
R10(config-subif)#encapsulation dot1Q 20
R10(config-subif)#xconnect 10.10.10.10 9999 encapsulation mpls
R10(config-subif)#exit
R10(config)#exit
R10#exit
```

Рисунок 5.27 – Налаштування MPLS L2VPN на маршрутизаторі R10

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip cef
R1(config)#mpls ip
R1(config)#mpls label protocol ldp
R1(config)#mpls ldp router-id loopback 0
R1(config)#int loopback 0
R1(config-if)#ip address 10.10.10.10 255.255.255.255
R1(config-if)#exit
R1(config)#int fa 0/0
R1(config-if)#ip address 1.1.1.1 255.255.255.252
R1(config-if)#no sh
R1(config-if)#mtu 1512
% Interface FastEthernet0/0 does not support user settable mtu.
R1(config-if)#mpls ip
R1(config-if)#mpls mtu 1512
R1(config-if)#exit
R1(config)#int fa 1/0
R1(config-if)#ip address 2.2.2.1 255.255.255.252
R1(config-if)#no sh
R1(config-if)#mtu 1512
% Interface FastEthernet1/0 does not support user settable mtu.
R1(config-if)#mpls ip
R1(config-if)#mpls mtu 1512
R1(config-if)#exit
R1(config)#router ospf 1
R1(config-router)#passive-interface default
R1(config-router)#no passive-interface fastEthernet 0/0
R1(config-router)#no passive-interface fastEthernet 1/0
R1(config-router)#network 10.10.10.10 0.0.0.0 area 0
R1(config-router)#network 1.1.1.0 0.0.0.3 area 0
R1(config-router)#network 2.2.2.0 0.0.0.3 area 0
R1(config-router)#exit
R1(config)#int fa 0/0.10
R1(config-subif)#encapsulation dot1Q 10
R1(config-subif)#xconnect 15.15.15.15 9999 encapsulation mpls
R1(config-subif)#exit
R1(config)#int fa 1/0.10
R1(config-subif)#encapsulation dot1Q 10
R1(config-subif)#xconnect 15.15.15.15 9999 encapsulation mpls
Pseudowire, VCID 9999, PeerID 15.15.15.15, already in use
R1(config-subif)#exit
R1(config)#exit
```

Рисунок 5.28 – Налаштування MPLS L2VPN на маршрутизаторі R1

Перевірка налаштування командою ping від R1до R10 (рис. 5.29)

```
R1#ping ip 12.12.12.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 12.12.12.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 112/168/212 ms
```

Рисунок 5.29 – Перевірка налаштування командою ping ip

Отже, після налаштування технології MPLS, а зокрема MPLS L2VPN, можна зробити висновок, що час витрачений на проходження пакету значно зменшився. Цей факт свідчить про те, що VPN налагоджено успішно, і побудова даного тунелю дає вагомий виграш у часі.

5.4 Дослідження характеристик роботи побудованої моделі VPN-мережі

Дослідження і тестування розробленої мережі, схема якої представлена на рис. 5.1 проводилися в симуляторі GNS 3.

Метою є визначення проходження пакетів по мережі, а також перевірка працездатності мережі, якості обслуговування. Для дослідження було обрано команду ping, з її допомогою можна відправляти пакети різного розміру, а також позначати їх необхідними бітами в заголовку пакета.

Для перевірки каналу в мережу відправлялися пакети розміром: 100 байт, 5000 байт, 15000 байт, 18000 байт.

Дослідження VPN тунелю проходило в кілька етапів: дослідження проходження пакетів по мережі від вхідного маршрутизатора R1 до на кінцевого маршрутизатора-отримувача R10; дослідження впливу пошкодження одного з кабелів провайдера, а саме обриву одного зі шляху в, на проходження пакетів між відправником та отримувачем; дослідження проходження пакетів в мережі при завантаженості однієї з ділянок мережі.

Вимірювання необхідно провести в три етапи. Перший етап – залежність часу проходження пакету від його розміру. Необхідно виконати дослідження всього маршруту від R1 до R10. Використано команду ping застосувавши пакети різного розміру, вона має вигляд ping size 5000 repeat 100, результати внесено до таблиці 5.2:

Таблиця 5.2 – Залежність часу проходження пакету від його розміру

Розмір пакета (байт)	Мінімальній час (мс)	Середній час (мс)	Максимальний час (мс)
100	224	283	301
5000	406	432	473
15000	531	575	598
18000	608	654	732

З отриманих результатів побудовано графіки залежностей часу проходження пакету мережею та повернення запиту від розміру цього пакету (рис. 5.30).

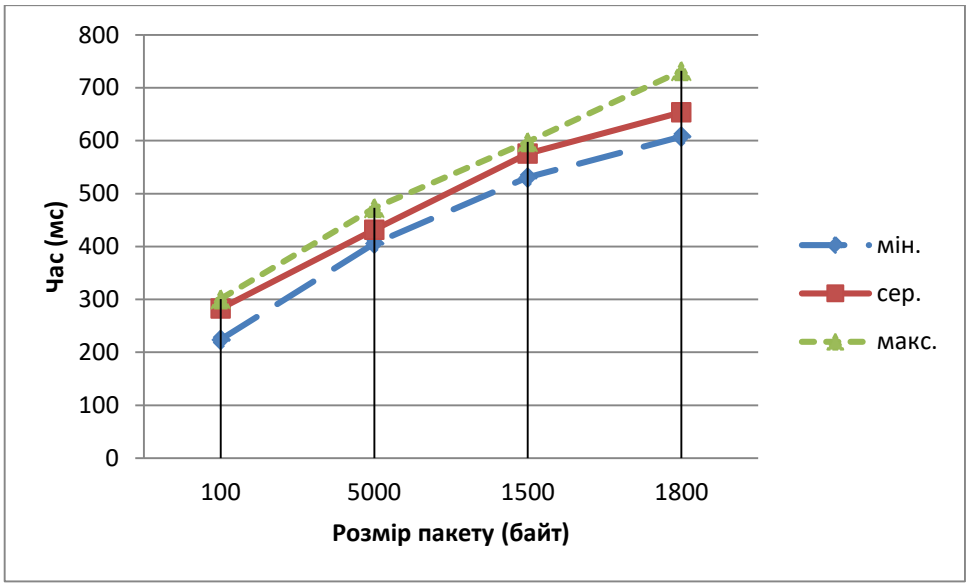

Рисунок 5.30 – Графіки залежність часу проходження пакету від його розміру

З графіків помітно, що при збільшенні розміру пакету час його транспортування в тунелі збільшується не суттєво, що не можна сказати про ситуацію з відсутністю тунелювання.

На другому етапі досліджень припускається, що стався обрив кабелю на ділянці R1-R3. Для цього на побудованій топології видалено з'єднання між даними двома маршрутизаторами і повторюються дії виконані на першому етапі, використовується команда у вигляді ping size 5000 repeat 100 з застосуванням різних розмірів пакетів. Також, необхідно зауважити, що спочатку перші 10 секунд ping не проходив, оскільки маршрутизатори реагували на зміни в мережі. Отримані дані внесено до таблиці 5.3.

Таблиця 5.3 – Залежність часу проходження пакету від його розміру, при обриві з'єднання на ділянці R1 та R3

Розмір пакета	Мінімальній час (мс)	Середній час (мс)	Максимальний час (мс)
100	291	304	323
5000	334	408	421
15000	403	448	523
18000	648	786	835

З отриманих результатів побудовано графіки залежностей часу проходження пакету мережею та повернення запиту від розміру цього пакету, при обриві з'єднання на ділянці R1 та R3 (рис. 5.31).

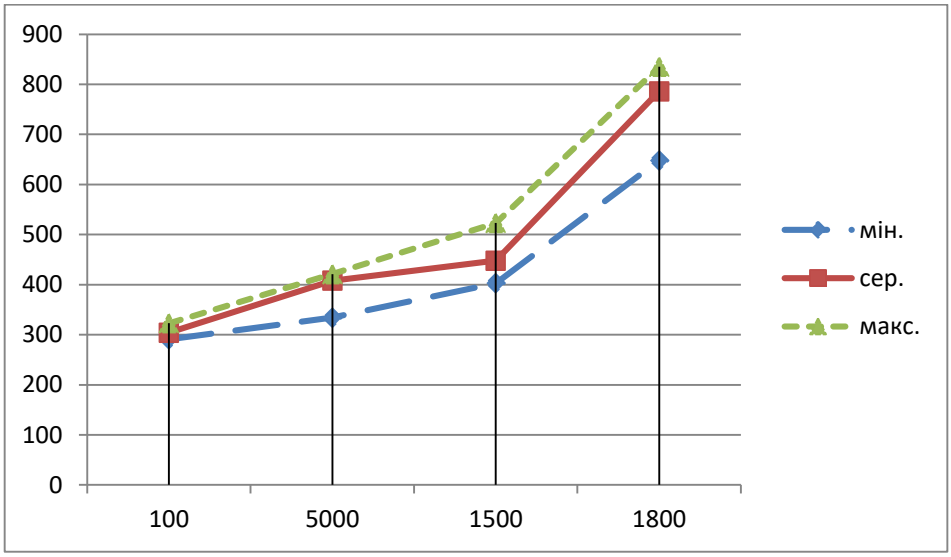

Рисунок 5.31 – Графіки залежність часу проходження пакету від його розміру, при обриві з'єднання на ділянці R1 та R3

З графіків помітно, що зростання часу спостерігається біль значним при максимальній довжині пакету. На початку час зростає більш плавно. Але слід зауважити, що на перших секундах пакет не відправляється одразу, бо відбувається пристосування мережі і знаходження маршрутизаторами нових сусідів.

На третьому етапі необхідно перевірити проходження пакету по тунелю при навантаженій мережі. Результати занесені до таблиці 5.4

Таблиця 5.4 – Залежність часу проходження пакету від його розміру при навантаженій мережі

Розмір пакета	Мінімальній час (мс)	Середній час (мс)	Максимальний час (мс)
100	311	351	367
5000	371	407	458
15000	513	524	561
18000	741	756	804

З отриманих результатів побудовано графіки залежностей часу проходження пакету завантаженою мережею та повернення запиту від розміру цього пакету

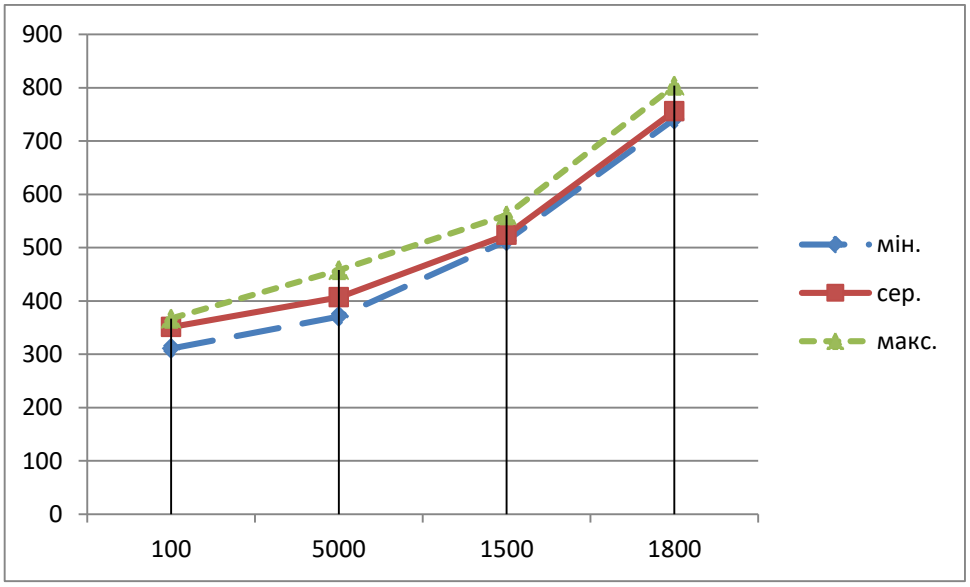

Рисунок 5.32 – Графіки залежність часу проходження пакету від його розміру при навантаженій мережі

На третьому етапі результати були отримані при проходженні пакету по тунелю при навантаженій мережі. Для цього була використана команда ping size 18000 repeat 1000 з застосуванням різних розмірів пакетів. З графіків помітно, що час зростає біль плавно ніж в ситуації з обривом одного зі з'єднань.

Отже, можна зробити висновок, що середня затримка в мережі не може залежати тільки від числа маршрутизаторів на шляху. Це значення можна розглядати тільки як один з факторів, що впливає на тимчасову затримку в мережі.

Таким чином, на всіх трьох етапах помітно однозначні переваги прокладання тунелю, а саме налаштування технології MPLS L2VPN. В результаті чого, отримано значну перевагу в часі при передачі пакетів, незалежно від їх розміру; швидке пристосування при обриві однієї з ділянок мережі; зовсім незначні втрати в часі при навантаженні мережі.

ВИСНОВКИ

Мета роботи полягала в розробці, перевірці та обґрунтуванні алгоритму для визначення доцільності та ефективності побудови тунелю в мережі MPLS. Створення фрагменту мережі та налаштування MPLS на кожному вузлі.

Опираючись на це, було проаналізовано алгоритм ефективності створення тунелю в мережі та проведено розрахунки в середовищі Mathcad. Продемонстровано, що ефективність застосування технології MPLS при різних навантаженнях залежить від кількості вузлів. Доведено, що при навантаженні, починаючи з $\rho=0,6$ на початку мережі час просування пакету в мережі та в тунелі різниться не суттєво, а найбільшу ефективність застосування тунелювання показує при збільшенні кількості вузлів, в тунелі час обробки зростає плавно та повільніше.

Проведено аналіз тунелювання MPLS, також особливостей даної технології. MPLS дозволяє пересилати дані за допомогою міток, що прикріплюються до кожного пакету. Внутрішні вузли ядра мережі, підтримують MPLS, не потребують аналізу вмісту кожного пакету. Так, не розглядається IP-адреса одержувача, що дає можливість MPLS надати ефективний механізм інкапсуляції для приватного трафіку, що передається по магістралі оператора.

Було проаналізовано застосування технології MPLS, проведено розрахунок швидкості передачі корисного навантаження в мережі. Технологія MPLS забезпечує широкий діапазон функціональних можливостей і додатків. Вона рідко використовується самостійно, а зазвичай, накладається на технології 2-го рівня, і повинна працювати спільно з іншими протоколами в площині управління, такими як протоколи маршрутизації IP.

Виконано побудову та налаштування мережі в симуляторі GNS3. Налаштовано IP-мережу на основі протоколу динамічної маршрутизації OSPF, повех якої застосовані налаштування MPLS мережі. Продемонстровано команди, що дозволяють переглянути призначення MPLS міток для кожного маршрутизатора. Представлено знаходження сусідніх вузлів та показано один з побудованих LSP-тунелів.

Обрано технологію створення VPN-тунелів. Налаштовано технологію MPLS L2VPN на мережі. Саме MPLS L2VPN на сьогоднішній день має найбільш широке поширення в мережах провайдерів.

Проведено три етапи досліджень в мережі з організованими VPN з'єднаннями. Перший етап – залежність часу проходження пакету від його розміру. Доведено, що при пересуванні пакета по тунелю залежність часу транспортування від його розміру не суттєва. Це досягається завдяки тому, що в технології MPLS маршрутизація базується не на зчитуванні адреси призначення, як в IP-мережі, а на мітках, які вставляються на початок кожного пакету даних. Також, цей метод дає змогу убезпечити приватну інформацію, що передається пакетами, бо в такому випадку зазирати до пакету за адресою непотрібно. На другому етапі досліджень імітовано обрив кабелю на одній з ділянок. Показано, що в даній ситуації час збільшуються при максимальному розмірі пакету, бо залишаться менше шляхів для транспортування. На третьому етапі перевірено проходження пакету по тунелю при навантаженій мережі. В даному випадку при збільшенні розміру пакету, час зростає плавно та несуттєво.

ПЕРЕЛІК ПОСИЛАННЯ

1. Muthukrishnan, K. A Core MPLS IP VPN Architecture / K. Muthukrishnan, A. Malis. // September 2013. – 348 p.

2. Гольдштейн, А. Б. Технология и протоколы MPLS / А. Б. Гольдштейн, Б. С. Гольдштейн // СПб. : BHV – 2005.

3. The Notion of overbooking and Its Application to IP/MPLS Traffic Engineering [Електронний ресурс] / Cheng C. Chen, Internet Traffic Engineering Working Group. – Режим доступу: http://www.ietf.org/proceedings/52/I-D/draft-cchen-te-overbooking-01.txt.

4. Rosen, E. BGP/MPLS VPNs / E. Rosen, Y. Rekhter // March 2012. – 215 p.

5. Токар Л. О., Білоусова К. Е, и др. «Разработка модели опорной сети на основе технологии long term evolushion.» // Восточно-Европейский журнал передовых технологий – 2017.

6. Ведмедеря М.А. Необхідність впровадження протоколу MPLS в інфокомунікаційних мережах // Харків, ХНУРЕ, Матеріали XXII міждународного молодіжного форуму «Радіоелектроніка та молодь у XXI столітті». Том 4 –2018. – с. 30 – 31.

7. Ведмедеря М.А. Розвиток транспортних мереж пакетної передачі даних // Харків, ХНУРЕ, Матеріали XXII міждународного молодіжного форуму «Радіоелектроніка та молодь у XXI столітті». Том 4 –2018. – с. 12 – 13.

8. Воробієнко П.П., Нікітюк Л.А., та ін. Телекомунікаційні та інформаційні мережі – Київ: САММІТ-Книга –2010.

9. Олвейн В. Структура и реализация современной технологии MPLS. – Москва «Вильямс», 2009. – 480 с.

10. Захватов М. Построение виртуальных частные сетей (VPN) на базе технологии MPLS. – М.: Cisco Systems, 2011. – 52 с.

11. Ведмедеря М.А. Впровадження технології MPLS в інфокомунікаційних мережах // Харків, ХПІ, Матеріали п'ятої міжнародної ноуково-технічної конференції студентів, магістрів та аспірантів. – 2018. – с.18.

12. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы / В. Олифер, Н. Олифер // Учебник для вузов. Четвертое издание. – СПБ.: Питер, 2010 – 944с.

13. Гейн Л. Основы MPLS. – Индианаполис: Cisco Press, 2007. – 651 с.

14. Гольдштейн А.Б., Гольдштейн Б.С Технология и протоколы MPLS. – СПб.: БХВ – Санкт-Петербург, 2005. – 304 с

15. Rosen E., Viswanathan A., Callon R. Multiprotocol Label Switching Architecture / E. Rosen, A. Viswanathan, R. Callon // Cisco Systems, Inc., Force10 Networks, Inc. – January 2001, 61p.

16.Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update [Електронний ресурс] / White Paper, February 3, 2016. – Режим доступа: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.html

17. Тодд Леммл, Кевин Хейлз. – Настройка коммутаторов Cisco. / Тодд Леммл, Кевин Хейлз // Москва, «ЛОРИ» – 2012 г.

ДОДАТКИ

Захист тимчасового каналу передачі даних у відкритій мережі загального користування

- Магістерська робота: Дмитро РИМАРЧУК
- Спеціальність 125 «Кібербезпека та захист інформації»
- Керівник: Юрій ПЕПА, к.т.н., доцент
- Фокус: MPLS, LSP-тунелі, QoS, GNS3, Mathcad

Актуальність дослідження

- Зростає потреба корпоративних клієнтів у VPN-з’єднаннях і гарантованій якості обслуговування.
- Традиційні транспортні системи та звичайна IP-маршрутизація не завжди забезпечують гнучкість і масштабованість.
- Технологія MPLS дає змогу будувати тунелі, ізолювати потоки та ефективніше керувати трафіком у відкритих мережах.

Мета, об’єкт і предмет роботи

- Мета: аналіз, перевірка та обґрунтування алгоритму визначення доцільності й ефективності побудови тунелю в мережі MPLS.
- Об’єкт дослідження: мережа на основі технології MPLS.
- Предмет дослідження: алгоритм ефективності тунелювання MPLS.
- Методи дослідження: аналіз, формалізація, розрахунки, порівняння та моделювання.

Основні завдання дослідження

- Проаналізувати особливості MPLS та протоколи розподілу міток.
- Дослідити застосування технології MPLS і побудувати модель мережі.
- Обґрунтувати математичну модель ефективності побудови тунелю.
- Виконати розрахунки у Mathcad та змоделювати мережу в GNS3.
- Перевірити роботу MPLS L2VPN і оцінити характеристики роботи мережі.

Структура магістерської роботи

- Розділ 1 — аналіз тунелів MPLS та особливостей технології.
- Розділ 2 — аналіз застосування технології MPLS.
- Розділ 3 — алгоритм та математична модель ефективності побудови тунелю.
- Розділ 4 — розрахунок ефективності тунелювання в середовищі Mathcad.
- Розділ 5 — побудова та налаштування фрагменту MPLS-мережі в симуляторі GNS3.

Технологія MPLS

- MPLS — багатопротокольна комутація за мітками (Multi Protocol Label Switching).
- Передавання пакетів здійснюється LSP-шляхом за мітками, а не лише за IP-адресами.
- Внутрішні вузли ядра мережі не потребують аналізу вмісту кожного пакета.
- Технологія зручна для побудови VPN, інкапсуляції приватного трафіку та забезпечення QoS.

Протоколи розподілу міток і ключові елементи

- У мережах MPLS застосовуються LDP та RSVP-TE для розподілу міток і керування тунелями.
- Ключові елементи мережі: ingress LSR, egress LSR, LER, LSR.
- Формуються FEC-класи та LSP-тунелі для організації маршруту проходження пакетів.
- Мітка MPLS спрощує та пришвидшує процес комутації в ядрі мережі.

Переваги й безпека MPLS-тунелювання

- MPLS забезпечує логічне відокремлення приватного трафіку в магістралі оператора.
- Підтримуються QoS та Traffic Engineering для керування напрямом і пріоритетами трафіку.
- Технологія характеризується масштабованістю, гнучкістю та зручністю модернізації мережі.
- Автоматичне перенаправлення LSP-тунелів підвищує стійкість мережі до відмов.

Застосування технології та модель мережі

- MPLS застосовується в транспортних, корпоративних і провайдерських мережах.
- У роботі побудовано модель мережі з десяти вузлів.
- Базову IP-мережу налаштовано на основі протоколу динамічної маршрутизації OSPF.
- Поверх цієї мережі реалізовано MPLS і VPN-тунелі для транспортування даних.

Математична модель ефективності тунелювання

- У роботі порівнюються час перебування пакета в тунелі V1(N) і в мережі V2(N).
- Ефект тунелювання оцінюється залежно від кількості вузлів N та навантаження ρ.
- Алгоритм дає змогу визначити доцільність побудови тунелю в мережі MPLS.
- Розрахунки та перевірка моделі виконані в середовищі Mathcad.

Результати розрахунків у Mathcad

- Показано, що ефективність застосування MPLS зростає зі збільшенням кількості вузлів.
- При навантаженні, починаючи з ρ = 0,6, на початку мережі різниця часу стає незначною.
- У тунелі час обробки пакета зростає плавніше та повільніше, ніж у звичайній мережі.
- Тунелювання є найбільш доцільним для багатовузлових мереж і підвищених навантажень.

Побудова та налаштування мережі в GNS3

- Створено та налаштовано фрагмент MPLS-мережі в симуляторі GNS3.
- Продемонстровано призначення MPLS-міток, таблиці сусідства та маршрути LSP.
- Перевірено працездатність мережі на базі OSPF з подальшим накладанням MPLS.
- Моделювання підтвердило коректність налаштованого фрагменту мережі.

Налаштування MPLS L2VPN

- Для організації VPN-з’єднань обрано технологію MPLS L2VPN.
- MPLS L2VPN налаштовано поверх побудованої мережі та перевірено в роботі.
- Технологія широко застосовується в мережах провайдерів.
- Рішення забезпечує транспортування приватного трафіку у відкритій мережі загального користування.

Експериментальні дослідження

- Досліджено залежність часу проходження пакета від його розміру.
- Імітовано обрив кабелю на одній із ділянок мережі та оцінено наслідки.
- Перевірено проходження пакета по тунелю в умовах навантаженої мережі.
- Встановлено, що в тунелі вплив розміру пакета на час транспортування є несуттєвим.

Практичні рекомендації

- Доцільно застосовувати MPLS у мережах із підвищеними вимогами до QoS та масштабованості.
- Для організації VPN-з’єднань у провайдерських мережах рекомендовано використовувати MPLS L2VPN.
- Для верифікації конфігурацій і перевірки сценаріїв ефективно застосовувати GNS3 та Mathcad.
- Необхідно контролювати навантаження, таблиці міток і резервування маршрутів.

Висновки

- Проаналізовано MPLS-тунелювання, його переваги та області застосування.
- Обґрунтовано алгоритм оцінювання ефективності побудови тунелю в мережі MPLS.
- Виконано розрахунки в Mathcad і моделювання мережі в середовищі GNS3.
- Підтверджено, що MPLS підвищує ефективність передавання даних у багатовузлових мережах і є придатною основою для VPN.