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

Інститут телекомунікаційних систем

Кафедра інформаційно-комунікаційних технологій та систем

«На правах рукопису»
УДК 621.391

«До захисту допущено»
ВО завідувача кафедри
_____ Аліна МОШИНСЬКА
«___»_____20__ р.

Магістерська дисертація

на здобуття ступеня магістра

зі спеціальності 172 Телекомунікації та радіотехніка

на тему: «Дослідження механізмів керування трафіком у мережах NGN на основі MPLS**»**

Виконав (-ла):
студент (-ка) ІІ курсу, групи ТС-11мп
Паршин Антон Юрійович _____

Керівник:
Доцент кафедри ІКТС к.т.н., доцент
Гаттуров В.К. _____

Рецензент:
Доцент кафедри СК-3 ІСЗЗІ
КПІ ім. Ігоря Сікорського, к.т.н.
Мазор С.Ю. _____

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.
Студент (-ка) _____

Київ – 2022 року

Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

Інститут телекомунікаційних систем

Кафедра інформаційно-комунікаційних технологій та систем

Рівень вищої освіти – другий (магістерський) за освітньо-професійною програмою

Спеціальність (освітня програма) – 172 «Телекомунікації та радіотехніка» («Системи та мережі електронних комунікацій»)

ЗАТВЕРДЖУЮ

ВО завідувача кафедри

_____ Аліна МОШИНСЬКа

«___»_____20__ р.

ЗАВДАННЯ
на магістерську дисертацію студенту

Паршину Антону Юрійовичу

1. Тема дисертації «Дослідження механізмів керування трафіком у мережах NGN на основі MPLS», науковий керівник дисертації Гаттуров Віктор Кавич, к.т.н, доцент, затверджені наказом по університету від «___»_____ 20__ р. №_____

2. Термін подання студентом дисертації 06 грудня 2022

3. Об’єкт дослідження механізми управління трафіком мереж наступного покоління з ядром на основі IP/MPLS

4. Предмет дослідження комплекс питань пов’язаних з забезпечення необхідної якості обслуговування за рахунок оптимального використання мережевих ресурсів мережі наступного покоління

5. Перелік завдань, які потрібно розробити

- Розглянути Технологію багатопротокольної коммутації за мітками у мережах наступного покоління.
- Розглянути концепцію управління трафіком в MPLS.
- Розглянути реалізацію концепції DiffServ в MPLS.
- Моделювання мережі на основі IP/MPLS та вирішення задачі управління трафіком у цій мережі.

6. Орієнтовний перелік графічного (ілюстративного) матеріалу

Слайд №1 Актуальність, мета, об'єкт та предмет дослідження магістерської дисертації

Слайд №2 Завдання магістерської дисертації

Слайд №3 Управління Трафіком (Traffic Engineering) у MPLS

Слайд №4 Топологія модульованої мережі

Слайд №5 Отримані для моделювання з використанням MPLS-TE

Слайд №6 Отримані для моделювання з використанням MPLS-TE та Diffserv

Слайд №7 Висновки

7. Дата видачі завдання .10.2021 р.

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Строк виконання етапів магістерської дисертації	Примітка
1	Технологія багатопротокольної коммутації за мітками у мережах наступного покоління. Передумови переходу до мереж наступного покоління. Мережі наступного покоління	01.11.2021 - 15.01.2022	
2	Керування трафіком з використанням IP/MPLS. Керування трафіком в мережах наступного покоління. Історія виникнення та відмінності MPLS. Елементи архітектури. Елементи мереж mpls. Стек міток та їх інкапсуляція. Тунелювання в mpls. Управління трафіком (traffic engineering) в MPLS. Концепція te в mpls. Атрибути te-тунелю та маршрутизація на основі обмежень. Сигнальні протоколи CR-LDP та RSVP-TE. Реалізація diffserv з MPLS. Class of type – ct. Обчислення шляху. Сигналізація тракту.	16.01.2022 – 29.05.2022	
3	Моделювання мережі наступного покоління на основі IP/MPLS. Імітаційний експеримент з	29.05.2022-16.09.2022	

	використанням ospf. Імітаційний експеримент з використанням MPLS – TE. Імітаційний експеримент використанням MPLS-TE і diffserv.		
4	Оформлення результатів.	16.09.2022 – 15.10.2022	
5	Чистовий варіант дипломної роботи, плакати	До 06.12.2022	

Студент _____ Антон ПАРШИН
(підпис) (ініціали, прізвище)

Науковий керівник дисертації _____ Віктор ГАТТУРОВ
(підпис) (ініціали, прізвище)

РЕФЕРАТ

Актуальність полягає у тому однією з головних проблем, що виникають при переході від спеціалізованих мереж до єдиної мультисервісної комунікаційної мережі, є забезпечення необхідної якості обслуговування різних сервісів і додатків. Розробка механізмів забезпечення якості послуг у мультисервісних мережах є однією з центральних проблем. У зв'язку з цим все більше уваги приділяється засобам керування трафіком, реалізованим на мережевому рівні мереж наступного покоління. Вище названими причинами обумовлена актуальність теми дослідження механізмів керування трафіком у мережах NGN на основі MPLS.

Метою роботи є пошук шляхів підвищення продуктивності мереж NGN за допомогою більш ефективного розподілу ресурсів пропускної спроможності за допомогою багатопротокольної комутації за мітками. Вирішення задачі управління трафіком в мережі NGN.

Об’єктом дослідження є механізми управління трафіком мереж наступного покоління з ядром на основі IP/MPLS .

Предметом дослідження є комплекс питань пов’язаних з забезпечення необхідної якості обслуговування за рахунок оптимального використання мережевих ресурсів мережі наступного покоління.

В дані роботі розглядаються особливості механізмів управління трафіком сучасних мультисервісних мережах побудованих на основі технології багатопротокольної комутації за мітками.

В роботі проведено моделювання мультисервісної мережі та вирішення задачі управління для цієї мережі.

Ключові слова: мережа наступного покоління, мультисервісна мережа, багатопротокольна комутація за мітками, mpls-te, якість ослуговування

ABSTRACT

The relevance of the field is that one of the main problems arises from the transition from specialized fences to a single multiservice community network is to ensure the maintenance of the necessary maintenance services. The purpose of the work is to find ways to increase the productivity of NGN networks by means of more efficient allocation of bandwidth resources under various topology. Solving the problem of traffic management in the NGN network. The development of mechanisms to ensure the quality of services in multiservice networks is one of the central problems. In this regard, more and more attention is paid to traffic management tools implemented at the network level of next generation networks. The above reasons are due to the relevance of the research topic of traffic management mechanisms in NGN networks based on MPLS.

The aim of the work is to find ways to increase the productivity of NGN networks by more efficient allocation of bandwidth resources across different topologies. Solving the problem of traffic management in the NGN network.

The object of the study is the traffic engineering mechanisms of a next generation networks with a core based on IP / MPLS.

The subject of the study is a set of issues related to ensuring the required quality of service through the optimal use of network resources of the next generation network.

These work examines the peculiarities of traffic management mechanisms of modern multiservice networks built on the basis of multi-protocol switching technology by tags.

The simulation of the multiservice network and solving the management problem for this network are carried out.

Keywords: next-generation network, multi-service networks, multiprotocol label switching, mpls-te, quality of service

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ І ТЕРМІНІВ 9
ВСТУП 12
1 ТЕХНОЛОГІЯ БАГАТОПРОТОКОЛЬНОЇ КОММУТАЦІЇ ЗА МІТКАМИ У МЕРЕЖАХ НАСТУПНОГО ПОКОЛІННЯ 14
1.1 Передумови переходу до мереж наступного покоління 14
1.2 Мережі наступного покоління 15
1.3 Висновки по розділу 1 16
2 КЕРУВАННЯ ТРАФІКОМ З ВИКОРИСТАННЯМ IP/MPLS 17
2.1 Керування трафіком в мережах наступного покоління 17
2.2 Історія виникнення та відмінності MPLS 18
2.3 Елементи архітектури 19
2.3.1 Елементи мереж MPLS 19
2.3.2 Структура міток 20
2.3.3 Стек міток та їх інкапсуляція 21
2.4 Тунелювання в MPLS 23
2.5 Управління Трафіком (Traffic Engineering) в MPLS 27
2.5.1 Концепція TE в MPLS 27
2.5.2 Атрибути TE-тунелю та маршрутизація на основі обмежень 29
2.5.3 Сигнальні протоколи CR-LDP та RSVP-TE 32
2.6 Реалізація DiffServ з MPLS 38
2.6.1 DiffServ 38
2.6.2 Class of Type – CT 40
2.6.3 Обчислення шляху 41
2.6.4 Сигналізація тракту 42
2.7 Підсумок MPLS-TE 44
2.8 Висновки до розділу 2 45

3 МОДЕЛЮВАННЯ МЕРЕЖІ НАСТУПНОГО ПОКОЛІННЯ НА ОСНОВІ IP/MPLS 46
3.1 Вступ до моделювання та топологія мережі 46
3.2 Імітаційний експеримент з використанням OSPF 49
3.2.1 Пропускна здатність 49
3.2.2 Затримки в черзі 54
3.2.3 Висновки по експерименту 56
3.3 Імітаційний експеримент з використанням MPLS –TE 57
3.3.1 Пропускна здатність 59
3.3.2 Затримки в черзі 67
3.3.3 Висновок по експерименту 69
3.4 Імітаційний експеримент використанням MPLS-TE і Diffserv 71
3.4.1 Конфінурація MPLS-TE та підтримка QoS 71
3.4.2 Затримка WFQ і використання буфера 74
3.4.3 Затримка потоку 76
3.4.4 Пропускна здатність 77
3.5 Висновки до розділу 3 80
ВИСНОВКИ 82
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 88

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

AF	Assured Forwarding, Гарантована передача
ATM	Asynchronous Transfer Mode, Асинхронний режим передавання
BC	Bandwidth Constraint, Обмеження смуги пропускання
BE	Best Effort, Кращі зусилля
BGP	Border Gateway Protocol, Протокол Граничного Шлюзу
CR-LDP	Constraint-based Routing Label Distribution Protocol, Протокол розподілу міток маршрутизації на основі обмежень
CSR	Cell Switching Router, Маршрутизатор стільникового зв'язку
CT	Class of Type, Тип класу
DiffServ	Differentiated Service, Диференційоване обслуговування
DS1	Digital Signal at first level, Цифровий сигнал першого рівня
DSCP	Differentiated Services Code Point, Точка коду диференційованих послуг
ECN	Explicit Congestion Notification, Явне сповіщення про перевантаження
EF	Expedited Forwarding, Прискорена передача
ERO	Explicit Route Object, Явний об'єкт маршруту
FDDI	Fiber Distributed Data Interface, Розподілений волоконний інтерфейс даних
FEC	Forwarding Equivalency Class, Клас еквівалентності пересилання
FIFO	First-In First-Out, Перший прийшов перший вийшов
GII	Global Information Infrastructure, Глобальна Інформаційна Інфраструктура
IETF	Internet Engineering Task Force, Спеціальна комісія інтернет-розробок
IGP	Interior Gateway Protocol, Протокол внутрішнього шлюзу
IntServ	Integrated Service, Інтегрований сервіс

IP	Internet Protocol, Міжмережевий протокол
IPSec	Internet Protocol Security, Безпека Інтернет-протоколу
IPX	Internetwork Packet Exchange, Мережевий обмін пакетам
ISDN	Integrated Services Digital Network, Цифрова Мережа з Інтегрованими Послугами
IS-IS	Intermediate System to Intermediate System, Проміжна система до проміжної системи
L2TP	Layer 2 Tunneling Protocol, Протокол тунелювання другого рівня
LDP	Label Distribution Protocol, Протокол розподілу міток
LER	Edge Label Switching Router, Граничний маршрутизатор комутації по мітках
LIB	Label Information Base, Інформаційна база міток
LIFO	Last-In First-Out, Останній увійшов, перший вийшов
LSP	Label Switched Path, Віртуальний комутований по мітках шлях
LSR	Label Switching Router, Маршрутизатор комутації по мітках
MAM	Maximum Allocation Model, Модель максимального розподілу
MPLS	Multiprotocol Label Switching, Багатопротокольна Комутація по Мітках
MTU	Maximum Transmission Unit, Максимальна одиниця передачі
NetBEUI	NetBIOS Extended User Interface, Розширений інтерфейс користувача дейтаграммної передачі NetBIOS
NGN	Next Generation Network, Мережа Наступного Покоління
NHRP	Next Hop Resolution Protocol, Протокол вибору наступного переходу
OSPF	Open Shortest Path First, Відкритий – перший найкоротший шлях
PHB	Per-Hop Behavior, Поведінка за стрибок
PPP	Point-to-Point Protocol, Протокол точка-точка.
PPTP	Point-to-Point Tunneling Protocol, Протокол тунелювання точка-точка

QoS	Quality of service, Якість обслуговування
RDM	Russian Dolls Model, Модель російської ляльки
RRO	Record Route Object, Об'єкт запису маршруту
RSVP	Resource Reservation Protocol, Протокол резервування мережевих ресурсів
RSVP-TE	Resource Reservation Protocol Traffic Engineering, Протокол резервування мережевих ресурсів для керування трафіком
SCP	Service Control Point, Вузол управління послугами
SDH	Synchronous Digital Hierarchy, Синхронна Цифрова Ієрархія
SPF	Sortest Path First, Перший найкоротший шлях
SSP	Service Switching Point, Вузол комутації послуг
TC	Traffic class, Клас трафіку
TCP	Transmission Control Protocol, Протокол керування передаванням
TE	Traffic Engineering, Управління Трафіком
TOS	Type of Service, Тип послуги
TTL	Time To Live, Час життя
UDP	User Datagram Protocol, Протокол датаграм користувача
WFQ	Weighted Fair Queuing, Зважена справедлива черга
АТС	Автоматична телефонна станція
ІМ	Інтелектуальна мережа
МсМ	Мультисервісна мережа
ТКМ	Телекомунікаційна мережа

ВСТУП

Стрімкий розвиток технологій та все більше розповсюдження ір-мереж значно вплинув на те, які послуги прагнуть отримувати споживачі та на продуктивність цих послуг, якими вони хочуть користуватися. У постачальників послуг виникла потреба у мережі здатній об'єднувати різноманітні технології для передачі різнотипного типу трафіку, таким рішення стала концепція мереж наступного покоління. Виникла вимога розвивати, керувати та вдосконалювати інфраструктуру мережі з точки зору продуктивності. Ядром такої мережі як правило мережа IP /MPLS. Цим обумовлен інтерес постачальників послуг до механізмів управління трафіком на основі багатопротокольної комутації по мітка.

Основною ціллю управління трафіком є досягнення певної продуктивності у великих IP-мережах. Висока якість обслуговування, ефективність і максимально можливе використання мережевих ресурсів усе це є рушійною силою, що обумовлює потреби і бажання розробки механізмів управління трафіку. Управління трафіком вимагає точного контролю над функціями маршрутизації в мережі. Обчислення та встановлення шляху пересилання від одного вузла до іншого є життєво важливим для досягнення бажаного потоку трафіку. Як правило, цілі продуктивності можуть бути орієнтовані на трафік і/або ресурси. Продуктивність, орієнтована на трафік, зазвичай пов’язана з QoS у мережі, що стосується втрати пакетів та затримки. Продуктивність, орієнтована на ресурси, пов’язана з ефективним використанням мережевих активів. Ефективний розподіл ресурсів необхідний для досягнення мети продуктивності в мережі. Контроль перевснтажень є ще однією важливою метою організації управління трафіком. Перевантаження зазвичай виникає за таких обставин, коли мережевих ресурсів недостатньо або недостатньо для обробки отриманого навантаження. Іншою причиною появи перевантаження є неефективний розподіл ресурсіа мережі, що призводить до надмірного використання підмножини ресурсів, в той час як інші залишаються недостатньо використаними.

До цілей управління трафіком також можно віднести забезпечення є надійної робота мережі та диференційованих послуг, де потоки трафіку з різними вимогами до послуг змагаються за ресурси мережі. Тому QoS важливий для тих, хто підписався на певну угоду про рівень обслуговування (SLA). Тому є необхідним контролювати трафік, щоб певні потоки трафіку могли бути маршрутизовані таким чином, щоб було надано необхідний QoS. Коли керовані потоки трафіку мають різні вимоги до QoS, можна призначити певні потоки певному шляху. Оскільки кілька потоків часто проходять один і той же шлях до певного місця призначення, агрегація потоків трафіку може зменшити кількість необхідних розподілів ресурсів, резервуючи ресурс для кожного з агрегованих потоків трафіку. Це дає можливість проектувати агреговані потоки трафіку, одночасно підтримуючи QoS для кожного з них з мінімальними витратами для резервування ресурсів уздовж певного шляху.

Щоб окреслити продуктивність, досягнуту механізмами управління трафіком, спочатку було розглануто конепцію мереж наступного покоління. Після чого розглядаємо управління трафіком за технологію багатопротокольної комутації за мітками та концепцію диференційованих. Підкреслюючи їхню функціональність і те, як вони можуть взаємодіяти для підтримки якості обслуговування під час проектування трафіку.

Після опису самих технологій переходимо до імітаційних мереж, щоб виміряти їх продуктивність. Для цього спочатку розглянемо мережу налаштовану на запуск протоколу маршрутизації за найкоротшим шляхом OSPF. Щоб виміряти спалахи продуктивності, генеруємо трафік TCP і UDP, задля вимірювання його обробки в умовах сильно завантаженої мережі. Потім ту саму мережу з її трафіком, проте налаштовуємо багатопротокольну комутацію по мітках, щоб спроектувати потоки за окремими шляхами. Порівнюємо результати, зібрані з обох мереж. Пізніше розглядається можливість проектування трафіку, в той же час беручи до уваги аспекти QoS. В якому лише порівнюємо підтримку QoS, надану потокам, що керуються через комутований по мітках шлях.

1 ТЕХНОЛОГІЯ БАГАТОПРОТОКОЛЬНОЇ КОММУТАЦІЇ ЗА МІТКАМИ У МЕРЕЖАХ НАСТУПНОГО ПОКОЛІННЯ

1.1 Передумови переходу до мереж наступного покоління

Сучасний етап розвитку світової цивілізації характеризується переходом від індустріального до інформаційного суспільства, що передбачає нові форми соціальної й економічної діяльності, базовані на широкому використанні інформаційних і телекомунікаційних технологій. Результатом еволюції телекомунікаційної індустрії став перехід від телекомунікаційної мережі до Глобальної інформаційної інфраструктури. Глобальна Інформаційна Інфраструктура (Global Information Infrastructure, GII) є технологічною основою інформаційного суспільства яка повинна забезпечити можливість вільного та бездискримінаційного доступу до інформаційних ресурсів кожному жителю планети.

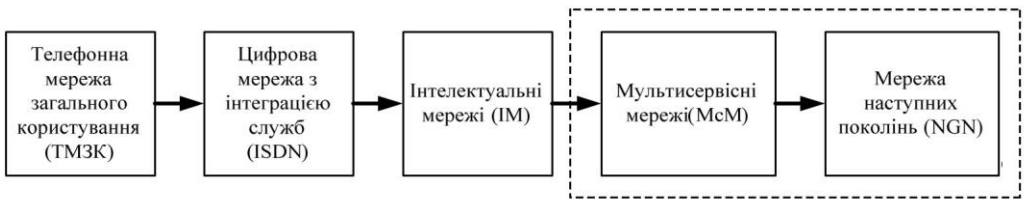

Рисунок 1.1 – Етапи еволюції телекомунікаційних мереж

Довгий час варіант організації телекомунікаційної мережі опирався на поняттях первинної та вторинної мереж[1]. Первинна мережа складалася з сукупності каналів та трактів передавання, створених обладнанням вузлів та ліній передавання, що з’єднували ці вузли. Первинна мережа надавала канали в експлуатацію вторинним мережам. Вторинна мережа складалася з каналів зв’язку первинної мережі, обладнання комутації та розподілу з метою організації зв’язку між абонентськими пристроями користувачів.

Наступним етапом еволюції ТКМ була розробка концепції цифрової мережі з інтегрованими службами (ISDN), що передбачала надання численних послуг на базі цифрових каналів з швидкостями від 64 до 2048 кбіт/с [1].

Подальше збільшення кількості послуг ТКМ виконувалося шляхом запровадження послуг інтелектуальної мережі (ІМ). Архітектура ІМ дозволяла розширити функціональність ТКМ шляхом її доповнення системою комутації послуг (SSP) та пунктів управління послугами (SCP) [1].

Недоліком попередніх етапів еволюції ТКМ було те що вони будувалися на базі аналогових та цифрових систем передачі з комутацією каналів. Ще одним їх суттєвим недоліком була невисока ефективність використання пропускної здатності систем передавання та відсутність достатньої гнучкості у виборі типів цифрових каналів для надання послуг. При розробці мультисервісних мереж ці недоліки були враховані.

1.2 Мережі наступного покоління

Розвиток IP-телефонії, мобільних мереж зв'язку, просування ринку послуг, для реалізації яких потрібні різні значення параметрів якості обслуговування, все це призвело до необхідності створення нових технологій доступу та початку такого процесу як конвергенція мереж.

Для реалізації цього було запропоновано концепцію єдиної мультисервісної мережі загального користування NGN, якою передбачається передача трафіку різного типу. Таке рішення дозволяє відмовитися від дублюючих один одного мереж, зменшити вартість обслуговування мережі, та дозволить впроваджувати нові послуги, забезпечуючи виконання їх специфічних вимог до швидкості та якості передачі.

Під мультисервісною мережею (МсМ) мається на увазі пакетна мережа, що здатна передавати голос, відеозображення та дані в рамках єдиної інфраструктури. Її концепція включає в себе такі аспекти:

- конвергенція загрузки мережі, яка визначає передавання різнотипного трафіку за допомогою єдиного формату представлення даних (пакети);
- конвергенція протоколів, що передбачає перехід від великої кількості різнотипних протоколів до одного загального (наприклад, IP);

- фізична конвергенція, що передбачає використання єдиної мережної інфраструктури для передавання різних типів трафіку;
- конвергенція пристроїв, яка приводить до інтеграції в одному корпусі обладнання комутації (Ethernet та ATM) і маршрутизації IP. В додаток до цього, пристрої можуть виконувати функції по обробці даних та підтримувати пакетну телефонію.

Основним завдання мереж наступного покоління (NGN) є передача будь-якого типу інформації від будь-якого користувача до іншого користувача, незалежно від того, де користувачі розташовані; при цьому для кожного типу інформації висуваються свої вимоги до смуги пропускання, часу доставки, допустимого рівня втрат та ступеня захищеності. Особливість мереж NGN є диференціація між послугами та транспортними технологіями. Що дозволяє розглядати мережу у вигляді логічно розділеної на рівні сутності. Кожен рівень якої може розвиватися незалежно, не впливаючи на інші рівні. Міжрівнева взаємодія в такій мережі виконується на основі відкритих інтерфейсів.

1.3 Висновки по розділу 1

Створення мережі наступного покоління відображає еволюційний розвиток існуючих телекомунікаційних мереж за рахунок злиття мереж та технологій. Завдяки цьому забезпечується широкий набір послуг, починаючи з класичних послуг телефонії та закінчуючи різними послугами передачі даних або їх комбінацією. Для реалізації мереж наступного покоління необхідна транспортна технологія здатна керувати трафіком різнотипних мереж та забезпечувати якість обслуговування послуг що надаються цими мережами. Такою технологією є технологія багатопротокольної комутації по мітках.

2 КЕРУВАННЯ ТРАФІКОМ З ВИКОРИСТАННЯМ IP/MPLS

2.1 Керування трафіком в мережах наступного покоління

Незалежно від кількості користувачів мережі NGN необхідно вирішення завдань пов’язаних з управління трафіком. Через одночасне існування різнотипних потоків трафіку які потребують безумовного дотримання одних параметрів передачі, і допускають деякі поступки іншим. У періоди виникнення перевантажень мережа може для одного потоку зменшити смугу пропускання, вже для іншого збільшити час доставки, а для третього, знехтувати цілісністю даних, що передаються і усе це з забезпеченням необхідної якості обслуговування.

Для забезпечення цього мережам наступного покоління необхідно мати більш складну систему управління, в порівнянні з системами управління традиційних мереж, яка має забезпечувати одночасне надання безлічі різноманітних мережевих послуг та передачу через мережу різнотипного трафіку.

Для ефективного управління трафіком необхідно мати у своєму розпорядженні відповідні апаратні та програмні засоби, що дозволяють швидко і гнучко надавати користувачеві будь-яку послугу.

Наразі оператори переходять від безлічі накладених мереж, що вимагають окремого управління і техобслуговування, до однієї мережі, ядром якої, як правило, є мережа IP/MPLS. Це обумовлюється наступними причинами:

- Використання технології IP/MPLS в середовищі Ethernet дозволяє підвищити масштабованість і якість обслуговування до рівня, необхідного транспортним мережам, а специфікація MPLS RSVP-TE Fast Reroute забезпечує відновлення трактів у межах 50 мс. Завдяки чому Ethernet мережі набувають характеристики та надійність SDH або ATM;
- кількість додатків, що використовують протокол IP, буде збільшуватися, відповідно доля трафіку IP буде збільшуватися, це призводить до пропорційної

збільшення вартості реалізації на основі технології ATM через пов'язані з додатковими накладними витратами смуги пропускання при передачі IP-трафіку.

2.2 Історія виникнення та відмінності MPLS

Значний вплив на історію MPLS внесла існуюча на той час проблема забезпечення сумісності протоколів IP і ATM. Спроби вирішення проблеми маршрутизації пакетів IP по мережах ATM робилися ще в кінці 1980 років, але більш активна робота розпочалася на початку 1990 років. Цією проблемою зайнялися відразу кілька робочих груп у складі комітету IETF.

Вирішення проблеми створення віртуального каналу ATM до IP-пристрою іншої LIS, взяла на себе робоча група ROLC в складі IETF. Вона запропонувала протокол Next Hop Resolution Protocol (NHRP). Протокол NHRP дозволяє IP-пристрою однієї логічної підмережі IP дізнатися ATM-адресу іншого IP-пристрою, з яким йому потрібно встановити зв'язок, за допомогою спеціального сервера наступного пересилання і організувати віртуальний канал зв'язку з цим пристроєм.

У 1994 р компанією Toshiba був анонсований маршрутизатор комутації комірок CSR (Cell Switching Router). Проте компанії Ipsilon завдяки більш повним технічним специфікаціям IP Switching і наявності готового продукту IP switch часто приписується честь створення першої справжньої формалізованої концепції MPLS-подібної комутації по міткам у IP мережах, що отримала значно більше визнання, ніж технологія CSR. Пізніше випуском власних аналогічних продуктів зайнялися багато інших компаній, серед яких слід зазначити Cisco Systems (Tag Switch), IBM (IP-Switch, заснована на агрегованих маршрутах) та Cascade (IP-навігатор). Усі продукти засновані на методі коли для знаходження маршрутів між кінцевими вузлами використовується стандартний протокол маршрутизації, при надходженні пакетів у мережу їм призначаються відповідні маршрути і все ж для переміщення цих пакетів по маршрутам застосовуються ATM-комутатори. На той час ATM-комутатори були значно швидше за IP-

маршрутизатори, тому мета полягала в підвищенні продуктивності, переміщуючи якомога більшу частину трафіку вниз, на рівень ATM. У 1997 р. було зібрано робочу групу MPLS для розробки загального стандартизованого підходу. До випуску першого набору пропозицій з'явилися маршрутизатори, що не поступалися швидкістю комутаторам ATM, що позбавило від необхідності підтримки в одній мережі одночасно технології IP і ATM. Попри це архітектура MPLS відіграє особливу роль, знижуючи обсяг необхідної обробки індивідуального пакета на кожному маршрутизаторі IP-мережі, що ще більше збільшує продуктивність маршрутизаторів.

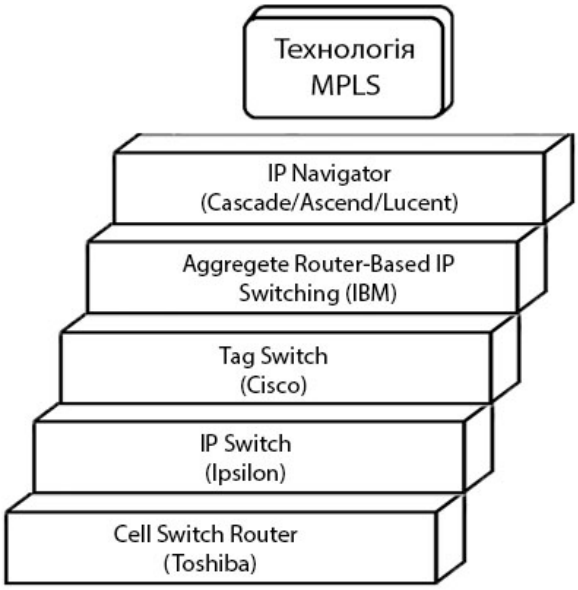

Рисунок 2.1 – Етапи розвитку MPLS

2.3 Елементи архітектури

2.3.1 Елементи мереж MPLS

Мережі MPLS складаються з граничних (Label Edge Router, LER), та транзитних (Label Switched Router, LSR) маршрутизаторів (рис 2.2).

LER на вході в MPLS-мережу додає мітку MPLS до пакета даних, окрім того він аналізує IP-заголовок і встановлює, до якого класу еквівалентного обслуговування

(Forwarding Equivalency Class, FEC) при виборі адреси наступної передачі пакета він належить. FEC - клас пакетів мережевого рівня, які отримують від мережі однакове обслуговування як при виборі шляху просування пакета, так і з точки зору доступу до ресурсів. LER на виході з MPLS-мережі видаляє мітку MPLS з пакета даних і направляє його адресату на підставі своєї маршрутної IP-таблиці.

LSR в свою чергу виконує маршрутизацію пакетів даних, базуючись тільки на значенні мітки. Мітки між LSR розподіляються за допомогою протоколе розподілу міток (Label Distribution Protocol, LDP). Для того, щоб отримати повну картину MPLS-мережі, LSR постійно обмінюються мітками і інформацією про кожний сусідній вузол, використовуючи стандартну процедуру.

Пакети, що належать до одного FEC і проходять шлях від вхідного LER до вихідного LER транзитні маршрутизатори LSR, утворюють віртуальний комутований по мітках шлях (Label Switched Path, LSP). Встановлене з'єднання є симплексним. Для організації полудуплексного з'єднання повинні бути встановлені два LSP.

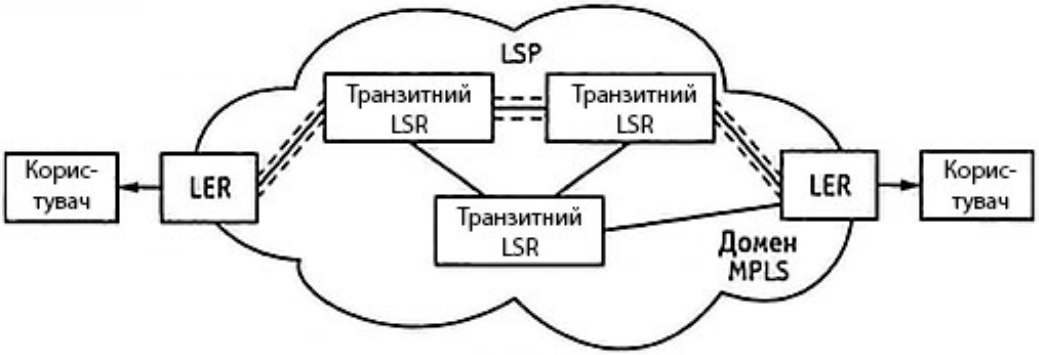

Рисунок 2.2 – Елементи мережі MPLS

2.3.2 Структура міток

Мітка - це короткий 32-бітний ідентифікатор фіксованої довжини, що використовується на локальній ділянці мережі. Він призначений для визначення класу еквівалентного обслуговування пакета при його пересиланні по мережі.

Рисунок 2.3 – Структура заголовку мітки MPLS

Поле Label (Мітка) – має величину 20 біт і містить власне значення мітки. Необхідна для визначення відповідного шляху комутації по мітках.

Поле TC (Traffic class, клас трафіку) – має величину 3 біти, використовується для реалізації механізмів якості обслуговування (QoS), містить пріоритет пакета, подібного полю DSCP в IP.

Поле S (Bottom of Stack, дно стека) – має величину 1 біт У біт S записується 1, якщо це остання мітка і «0», якщо стек містить більше однієї мітки.

Поле TTL (Time To Live) – має величину 9 бітів, використовується для запобігання нескінченного блукання пакета по мережі в разі петлі. При передачі IP-пакета через мережу MPLS поле TTL зменшується на одиницю на кожній ділянці маршруту, і коли значення лічильника досягає нуля, пакет відкидається або передається для обробки помилок

2.3.3 Стек міток та їх інкапсуляція

Ключовим для технології MPLS поняття є стек міток. Можливість мати в пакеті не одну мітку, а кілька. у вигляді стека дозволяє створювати ієрархію міток у MPLS мережах.

Розрізняють верхні та нижні мітки. Верхня мітка обробляється першою на шляху проходження пакету в той час нижня мітка обробляється останньою на шляху проходження пакету. При цьому результат комутації задає лише верхня мітка стека, нижні ж передаються прозоро до операції вилучення верхньої.

MPLS може виконати зі стеком наступні операції:

- Додавати мітку до стека;
- Видаляти мітку зі стека;
- Замінювати мітку

Операція push operation використовується для додавання мітки до стеку, а операція pop operation використовується для видалення мітки зі стеку.

Функціональні можливості стека MPLS дозволяють об'єднувати декілька LSP в один. До стеку міток кожного з цих LSP зверху додається загальна мітка, в результаті чого утворюється агрегований тракт MPLS. У точці закінчення такого тракту відбувається його розгалуження на індивідуальні складові LSP. Так можуть об'єднатися тракти, які мають загальну частину маршруту.

Інкапсуляція в MPLS виконується згідно правила LIFO (last-in, first-out), тобто мітка у верхній частині стека, отримана останньою, і тільки вона обробляється при пересиланні пакета [3]. Варто зауважити, обробка завжди базується на верхній мітці, без урахування можливості того, що деяка кількість інших міток могла бути «над нею» в минулому, або що певна кількість інших міток може бути під нею зараз.

Рисунок 2.4 – Чотирьохрівневий стек міток

При використанні протоколів комутації на рівні ланки даних, таких як ATM і Frame Relay, верхня MPLS-мітка вписується в поле ідентифікаторів цих протоколів [3]. У випадку, коли MPLS забезпечує пересилку IP-пакетів мережевого рівня і коли технологія рівня ланки даних не підтримує власне поле міток то MPLS-заголовок повинен інкапсулюватися між заголовками рівня ланки даних і мережевого рівня.

Механізм інкапсуляції переносить один або більше протоколів верхніх рівнів всередині корисного навантаження дейтаграми інкапсулюючого протоколу[3]. По суті, вводиться новий заголовок, який робить з інкапсульованого заголовка і поля даних нове поле даних. Мітка MPLS може бути поміщена в існуючий формат заголовка рівня 2, у випадку ATM або FR, або вписана в спеціальний заголовок MPLS, як у випадку Ethernet або PPP. В будь якому випадку будь-які додаткові мітки знаходяться між верхньою міткою стека і IP-заголовком рівня 3. Загальний принцип інкапсуляції заголовка MPLS зображено на рис 2.5.

Рисунок 2.5 – Загальний принцип інкапсуляції заголовка MPLS

2.4 Тунелювання в MPLS

Організація тунелів виконується у більшості сучасних протоколів. Її організація базується на інкапсуляції пакетів, що направляються тунелем, у пакети, що йдуть

основним віртуальним каналом, і мають ту саму адресу призначення, що й пакети, що інкапсулюються в них.

Для технології MPLS розглядатимуться тунелі, що організовуються не шляхом інкапсуляції пакетів, а за допомогою засобів комутації за мітками.

Такий тунель має назву LSP-тунель, і представляє з себе послідовність маршрутизаторів, у якій перший маршрутизатор є кінцевим вхідним пунктом тунелю, в той час як останній є його вихідним кінцевим пунктом. LSP-тунель створюється всередині LSP. Він зазвичай буває коротшим за LSP в якому він створений, і тому часто початок та кінець тунелю не збігається з початком та кінцем LSP.

В межах одного LSP може бути створено кілька LSP-тунелів одного рівня з різними вхідними та вихідними кінцевими пунктами. Всередині будь-якого з цих LSP-тунелів можна створювати LSP-тунелі вже наступного рівня. Таким чином забезпечується ієрархічність структури MPLS [6].

Якщо в одному LSP зливається кілька потоків (кожен потік - зі своїм FEC і зі своєю міткою), то цей LSP не замінює мітки, пов'язані з названими потоками, а залишає їх, поміщаючи зверху мітку нового FEC, який відповідає об'єднаному потоку пакетів, що утворюється внаслідок злиття.

Під LSP рівня m розуміється LSP, який утворений послідовністю маршрутизаторів LSRвх, LSR(n-1), LSRвих з наступними властивостями:

- глибина стека m дорівнює кількості розміщених вхідним маршрутизатором LSRвх міток у стеку міток пакета;
- при всіх i (1<i<n) пакет, що надходить до LSRi, має стек міток глибини m;
- у процесі транспортування пакета від LSRвх до LSRn 1 глибина його стека міток ніколи не буває меншою за m;
- за всіх i (1<i<n) LSRi передає пакет LSRi+1 засобами MPLS.

Тобто під маршрутом LSP рівня m мається на увазі послідовність маршрутизаторів. Початком цієї послідовності є вхідний маршрутизатор LSR, що розміщує в пакет мітку рівня m [6]. Ця послідовність містить проміжні LSR,які

приймають рішення про пересилання пакета на основі мітки рівня m. Послідовність закінчується вихідним LSR, який приймає рішення про пересилання на основі мітки рівня m - k, де k>0, або на основі стандартних процедур пересилання.

Усе це так саме відноситься і до LSP-туннелів рівня m з тією ж різнецею, що вхідний, проміжні та вихідний LSR є такими не для всього LSP, а лише для LSP-тунелю[6]. Тобто кінцеві пункти LSP-тунелю та LSP, у якому був організований тунель, можуть не збігатися. На рисунку 2.5 наведено схему туннелювання в IP/MPLS.

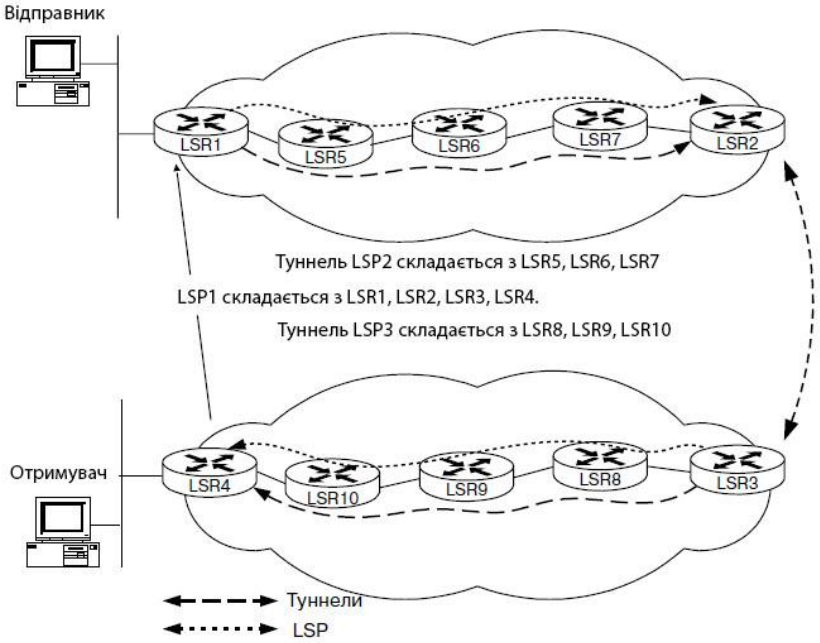

Рисунок 2.5 – Схема тунелювання в IP/MPLS

На даній схемі Граничні маршрутизатори LSR1, LSR2, LSR3 та LSR4 створюють комутований тракт LSP1. Маршрутизатор LSR1 має інформацію, що наступним пунктом призначення для нього є LSR2. В той час як, для LSR2 — LSR3, а LSR3 — LSR4. З допомогою протоколу LDP граничні LSR будуть отримувати та зберігати мітки від вихідного LSR4 до вхідного LSR1.

Для передачі від LER1 до LER2 даних, їм необхідно пройти через транзитні маршрутизатори LSR. Для цього, між LER1 та LER2 створюється окремий шлях LSP2,

який охоплює LSR5, LSR6 та LSR7. По суті, він є тунелем між цими двома LER. Мітки на цьому шляху відрізняються від міток, які LER створили для LSP1. Це справедливо і для LER3 і LER4, так само як і для LSR, що знаходяться між ними. І тому на останньому сегменті створюється шлях LSP3. Для досягнення даного результату при передачі пакета через два мережеві сегменти використовується концепція стека міток. Оскільки пакет повинен слідувати через LSP1, LSP2 і LSP3, він одночасно переноситиме дві окремі мітки. Для першого сегменту - мітка для LSP1 та LSP2, для другого - мітка для LSP1 та LSP3.

Коли пакет залишає першу мережу і приймається граничним маршрутизатором LER2, той видаляє мітку LSP2 і замінює її на мітку LSP3, замінюючи при цьому мітку LSP1 всередині пакета на мітку наступної пересилки. LER4 видаляє обидві мітки перед надсиланням пакета адресату.

Відмінною рисою тунелів MPLS є їх можливіть передавати дані будь-якого протоколу вищого рівня такі як комірки ATM, IP, IPX [6]. Це обумовлено тим вміст пакетів напротязі усього шляху пакета є незмінним, а змінюються лише мітки. В той час наприклад, тунелі IPSec здатні на передачу даних лише протоколу IP.

Безпека у MPLS забезпечується за рахунок заборони, приймати пакети, забезпечені мітками, від неперевірених джерел. Задля додаткового підвищення безпеки передачі даних доцільним є використання стандартних засобів автентифікації та шифрування [6]..

Застосування міток MPLS дозволяє реалізувати прискорене просування пакетів мережі провайдера. Транспорт MPLS не зчитує заголовки пакетів, що транспортуються, тому адресація, що використовується в цих пакетах, може мати приватний характер. Вміст пакетів не зчитується при передачі IP пакетів за протоколами IPSec, PPTP, L2TP. Однак, на відміну від MPLS, традиційні протоколи тунелювання для транспортування IP-пакетів використовують традиційну IP-маршрутизацію.

При виборі шляху проходження пакета в MPLS враховуються різні параметри, що впливають на вибір маршруту. Спільна робота технології багатопротокольної комутації

та механізмів управління трафіком дозволяє кожному тунелю LSP надати необхідний рівень якості обслуговування з допомогою процедури резервування ресурсів кожному маршрутизаторі вздовж шляху прямування пакета [6].. Крім цього, з'являється можливість відстежувати дійсний маршрут, що проходить через сформований тунель, можливість діагностики та адміністративного контролю тунелів LSP.

2.5 Управління Трафіком (Traffic Engineering) в MPLS

2.5.1 Концепція TE в MPLS

Під терміном Traffic Engineering розуміють методи та механізми збалансованого завантаження всіх ресурсів мережі за рахунок раціонального вибору шляху проходження трафіку через мережу. Механізм управління трафіком надає можливість встановлювати явний шлях, яким будуть передаватися потоки даних.

Традиційна маршрутизація у IP-мережах базується на обчисленні найкоротшого шляху, що має найменшу сумарну метрику мережного рівня. Цей шлях може бути оптимальним, оскільки він залежить від інформації статичної метрики каналу. У цьому випадку при виборі шляху не враховуються вільні мережеві ресурси, поточне завантаження каналів, а також вимоги до обслуговування трафіку. Таким чином, якщо найкоротший шлях вже перевантажений, то пакети все одно будуть посилатися цим шляхом, внаслідок чого буде спостерігатися картина завантаженості одних каналів зв'язку і простоювання інших. Слід зазначити, що за наявності в мережі кількох рівноцінних альтернативних маршрутів трафік ділиться між ними, і навантаження на маршрутизатори і канали зв'язку розподіляється більш збалансовано. Але, якщо маршрути є повністю рівноцінними, розподіл трафіку між ними не відбувається.

На рисунку 2.7 зображено приклад, що ілюструє цю проблему маршрутизації за принципом SPF (Sortest Path First).

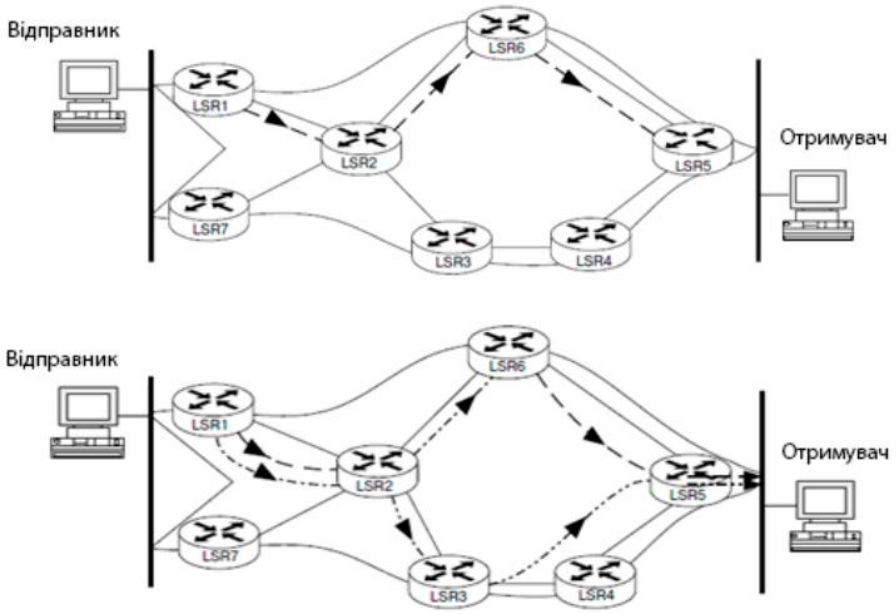

Рисунок 2.7 – традиційний та рівномірний розподілі трафіку

При першому варіанті трафік від маршрутизатора LSR2 до LSR5 згідно алгоритму OSPF йде через маршрутизатор LSR6. Таким чином, маршрут LSR2-LSR6-LSR5 перевантажений, а ресурс маршруту LSR2-LSR3-LSR4-LSR5 використовується неефективно. З вирішенням цієї проблеми може допомогти використання механізмів TE, що вкажуть два різні шляхи від LSR1 до LSR5.

При другому варіанті використання механізмів TE дозволяє краще використовувати мережеві ресурси за рахунок того що частина трафіку буде переведена з більш завантаженої ділянки мережі на менш завантажену. За рахунок більш ефективного використання смуги пропускання, ще й досягається більш висока якість обслуговування трафіку, оскільки зменшується ймовірність перевантаження в мережі. Також для послуг для яких необхідно виконання заданих норм якості обслуговування QoS, TE дозволяє забезпечувати належний QoS шляхом призначення явно визначених маршрутів.

Характеристики пов’язані з управлінням трафіком, можуть бути орієнтовані або на трафік або на ресурси [6]. Завдання TE включають аспекти поліпшення показників

QoS інформаційних потоків, а центральною функцією ТЕ є оптимальне управління пропускною здатністю.

Трафік-інженер, під яким мається на увазі не людина а деякий абстрактний елемент управління, формулює політику управління, контролює стан мережі, використовуючи систему моніторингу, визначає характеристики трафіку і робить керуючі дії, щоб перевести мережу в стан, що узгоджується з політикою управління[6]. Усе це може виконуватися або за допомогою операцій, які здійснюються у відгуку на поточний стан мережі, або завчасно, на основі прогнозування змін стану мережі задля запобігання виникненню небажаних станів.

Завдання управління трафіком вирішувалися у галузі зв'язку завжди, по при це підхід до їх вирішення був принципово іншим. Як приклад до управління трафіком можна віднести розрахунки які проводилися при проектуванні АТС на основі теорії телетрафіку, а також вимірювання характеристик навантаження та якості обслуговування в процесі експлуатації з подальшою реконфігурацією сполучних ліній.

2.5.2 Атрибути ТЕ-тунелю та маршрутизація на основі обмежень

В області керування трафіком стосовно MPLS використовується термін traffic trunk, яким позначають об'єднання потоків трафіку, що належать одному класу і проходять по одному LSP. Іншими словами, traffic trunk – це об'єднаний потік трафіку, що віднесений до одного FEC.

ТЕ-тунель має певні атрибути, що описують вимоги транка трафіку, від яких залежить вибір політики адміністратора.

- Traffic parameter attributes (Атрибути параметрів трафіку)
- Generic Path selection and maintenance attributes (Атрибути вибору та обслуговування загального шляху)
- Priority attribute (Атрибут пріоритету)
- Preemption attribute (Атрибут випередження)

- Resilience attribute (Атрибут стійкості)
- Policing attribute

Атрибути параметрів трафіку можна використовувати для фіксації характеристик потоків трафіку (FEC), які будуть транспортуватися через канал трафіку. До таких характеристики відносяться пікові швидкості, середні швидкості, допустимий розмір пакету і т.д [10]. З точки зору проектування трафіку, параметри трафіку є важливими, через те що вони вказують на вимоги до ресурсів магістралі трафіку. Це корисно для розподілу ресурсів і уникнення перевантажень через випереджувальні політики.

Атрибути вибору та обслуговування загального шляху визначають правила вибору маршрутів для LSP, а також правила роботи з маршрутами, які вже існують. До них відносяться:

Administratively Specified Explicit Paths (Адміністративно специфіковані маршрути) конфігуруються оператором. Такі маршрути можуть визначатися повністю або частково і бути обов'язковим для використання, або лише бажаними [16]. Шлях є повністю визначеним, якщо вказано всі необхідні переходи між кінцевими точками.

Hierarchy of Preference Rules For Multi-Paths (Ієрархія переваг для набору маршрутів) адміністративно специфікує ієрархію в наборі можливих маршрутів для даного LSP [16].

Resource Class Affinity Attributes використовуються для специфікації класу ресурсів, які слід явно включити в LSP або виключити з нього. Це атрибути політики, які можуть використовуватися з метою введення додаткових обмежень на маршрути для LSP [16].

Adaptivity Attribute (Атрибут адаптивність) являє собою двійкову змінну, що визначає, як слід реагувати на зміну стану мережі: дозволити або припинити адаптивну оптимізацію.

Load Distribution Across Parallel Traffic Trunks (Розподіл навантаження в паралельних транках). Коли об'єднаний трафік між узлами є таким, один транк не зможе

його пропустити, і єдиним рішенням є поділ трафіку на кілька потоків, то ці атрибути вказують долі трафіку, що проходить через кожен з паралельних трактів [16] .

Priority attribute (Атрибут пріоритету) визначає відносну важливість потоку трафіку. Пріоритети використовуються в разі відмов для того, щоб визначити порядок, в якому вибираються з наявного списку маршрути для відповідного LSP, а також у реалізаціях, що допускають пріоритетне обслуговування.

Атрибут Preemption (Атрибут випередження) визначає можливіть одного потоку трафіку замістити інший потік трафіку у тракті, і задає умови пріоритетного розміщення.

Resilience attribute (Атрибут стійкості) визначає поведінку тракту в разі виникнення помилок. Базовий атрибут Resilience вказує на процедуру відновлення, яка повинна бути запущена для даного тракту при виникненні відмови. Розширений атрибут Resilience містить детальну специфікацію дій у разі відмови.

Атрибут Policing визначає дії, які слід передбачити, коли які-то параметри тракту виходять за допустимі межі [16]. Атрибути Policing показують, чи потрібно обмежити тракт за смугою пропускання, помітити його або просто пересилати його трафік без будь-яких дій.

Атрибути ресурсів є частиною параметрів стану топології, які використовуються для обмеження маршрутизації каналів трафіку через певні ресурси [16].

Maximum allocation multiplier (Максимальний множник розподілу) є адміністративно заданим атрибутом, який визначає долю ресурсу, доступну тракту. Цей атрибут використовується, в основному, для розподілу смуг пропускання. Однак він може бути застосований також для резервування ресурсів LSR.

Атрибути Resource Class (Класс ресурсу) можна розглядати як приписані ресурси кольору, такі, що набір ресурсів з одним кольором належить одному класу. Атрибути класу можуть бути використані для:

- Застосування однакових політик для набору ресурсів, які не обов’язково знаходяться в одній топологічній області.

- Специфікації відносного переваги для набору ресурсів, пов’язаних з положенням маршруту, за яким транспортується потік даних.
- Обмеження розміщення каналів передачі даних для заданої підмножини ресурсів.
- реалізація політики обмеження локальності трафіку.

Атрибути, пов’язані з каналами передачі даних і ресурсами мережі, а також параметри, пов’язані з маршрутизацією, у сукупності є набором керуючих змінних, які можуть бути модифіковані в результаті дій адміністратора, або автоматичних агентів, для того, щоб привести набір у необхідний стан.

Маршрутизація на основі обмежень використовує як вхідні дані атрибути, пов'язані з потоками трафіку, атрибути, пов'язані з ресурсами, а також іншу інформацію, що характеризує поточну топологію мережі, та дає можливість резервувати на запит ресурси для управління трафіком.

ЇЇ призначенням є максимальне скорочення обсягу робіт, що пов'язані із ручною конфігурацією та ступіню участі адміністратора у реалізації політики управління трафіком.

2.5.3 Сигнальні протоколи CR-LDP та RSVP-TE

Протокол CR-LDP є розширенням базового протоколу LDP, і на відміну від нього що дотримується лише таблиць маршрутизації IP, здатен підтримувати явну маршрутизацію з урахуванням QoS.

Використовуючи CR-LDP в якості протоколу для розповсюдження міток, запит на отримання мітки дотримується явно заданого маршрута, при цьому відпадає необхідніть у використанні таблиць маршрутизації оскільки повідомлення передається за маршрутом, заданим у спеціальному полі ERO повідомлення Path. Відомості про динамічне резервування пропускної спроможності повинні включатися в широкомовну

інформацію протоколів IGP, OSPF, IS-IS або в оголошення про стан каналів, CR-LDP не підтримує динамічного обчислення явно заданих маршрутів.

З допомогою цієї інформації CR-LDP може займає та резервувати пропускну здатність. Величина доступної пропускної спроможності змінюється відповідно до запитів, після чого нове значення пропускної спроможності розсилається іншим маршрутизаторам за допомогою протоколів OSPF або IS-IS, та виконується обчислення нового маршруту організації LSP.

Протокол RSVP-TE, розширення протоколу RSVP, використовується як протокол сигналізації TE-тунелю. Його використання дозволяє оптимізувати мережу під конкретні завдання шляхом створення тунелів RSVP-TE.

В протокол були введені додаткові можливості необхідні для створення явно заданого LSP, а метод прив'язки міток до RSVP-потоків та функція явної маршрутизації.

Використання RSVP обумовленно забезпеченням можливості маршрутизаторів LSR, які виконують класифікацію пакетів шляхом аналізу їх міток, розпізнавати пакети потоків для яких було виконано резервування ресурсів. Ці пакети розглядається як ще один клас FEC.

Протокол RSVP-TE додає до сигнальних повідомленнь RSVP, розширення що забезпечують підтримку механізмів управління трафіком. Управління трафіком забезпечується шляхом використання тунелів, в той час як для передачі даних явним шляхом застосовуються локальні мітки. Передача пакетів відбувається з урахуванням класів трафіку, на відміну від таких протоколів маршрутизації як OSPF, IS-IS у яких пакети передаються на основі топології. Тобто маршрутизація на основі резервування може бути реалізована завдяки визначення класів трафіку та вимог до створення явного маршруту.

Повідомлення Resv для забезпечення можливості прив’язки мітки до потоку було розширено об’єктом Label. Для передаті повідомлення Resv нового потоку RSVP, LSR призначає мітку зі свого пулу вільних міток в об'єкті LABEL повідомлення Resv та створює запис у своїй таблиці LIB (Label Information Base) після чого передає саме

повідомлення. Оскільки повідомлення. Resv передаються від одержувача до відправника, тому це є різновид призначення позначок знизу.

Маршрутизатор отримуючи повідомлення Resv, записує мітку цього потоку вже у своїй базі LIB як вихідну, і вже для неї назначає вихідну мітку та пересилає її вище до наступного LSR. Таким чином, LSP створюється по шляху поширення повідомлення. Завдяки тому що у об’єкті LABEL повідомлення Resv вказуються мітки, коженому LSR не доставить складності зв'язати відповідні ресурси QoS із відповідним трактом LSP.

Проте протокол RSVP з додатковим об'єктом LABEL, здатен організовувати LSP лише вздовж маршруту, який попердньо обчислюється з допомогою схеми традиційної маршрутизації IP пакетів. Це обумовлено тим, що шлях яким прямує повідомлення Path звичайного протоколу RSVP керується на осноснові пункту призначення, в той час як повідомлення Path прямує маршрутом визначним шляхом LSP. Для визначення наступного маршрутизатора, до якого необхідно передати повідомлення Path, маршрутизатор використовує адресу одержувача з заголовку IP-пакета, та свою таблицю маршрутизації, що формується на основі таких протоколів як OSPF, IS-IS або BGP [6].

При такій організації пересилання повідомленням Path явно заданим маршрутом не має можливості керувати його передачою.

Протокол RSVP-TE має об'єкт Explicit Route Object (ERO), який дозволяє визначати явно заданий маршрут. Повідомлення ERO входить до повідомлення Path, та містить у собі інформацію про послідовність маршрутизаторі, що являє собою явно заданий маршрут. Відповіддю на передачу повідомлення ERO є передача даним маршрутом повідомлення Resv, завдяки чому відбувається встановлення шляху LSP та резервуються ресурси мережі [6].

З відмінностей протоколу CR-LDP та протоколу RSVP-TE найбільш помітною є транспортний протокол, що використовується для передачі запитів міток. Протокол CR-LDP використовує орієнтовані на з'єднання TCP-сеанс для передачі протокольних повідомлень, а для виявлення однорангових маршрутизаторів протокол UDP. Протокол RSVP на томість використований на орінтований на з’єднання протокол IP.

Використання транспорту TCP протоколом CR-LDP має дві негативні риси. Першою є зменшення швидкості перечі інформації між маршрутизаторам через механізм запобігання перевантаження протоколу TCP.

Другою є те, що якщо між двома LSR є тільки одне TCP-з'єднання то виникає ситуація при якій критично важливе повідомлення не може прийти першим за менш важливе, що було відправлено першим. Це обумолено тим, що TCP примусово затосовує дисципліну Перший прийшов перший вийшов (First-In First-Out, FIFO). Ще одним важливим недоліком є те, що при втраті пакету, усі повідомлення, що йдуть після нього повинні очікувати поки не буде проведено повторну передачу пакету.

Забезпечення безпеки протоколу CR-LDP як наслідок організовується на основі протоколу TCP. Це робить використання протоколу CR-LDP вразливим з боку атак ціллю яких є порушення обслуговування TCP-сеансів, що матите значний негативний вплив на функціонування протоколу CR-LDP.

В той час у протоколі RSVP-TE одержувачем повідомлення Path є не проміжні LSR, а вихідний, що не дозволяє використовувати IPSec (Internet Protocol Security, серія стандартів забезпечення автентифікації та захисту переданих протоколом IP), бо проміжні LSR не будуть здатні отримати доступ до необхідної інформації повідомлення Path. Проте протокол RSVP-TE має свої механізми автентифікації користувачів, що не дозволяють несанкціонованого резервування ресурсів.

Орієнтовані на з'єднання протоколи вимагають зберігання даних про стани з'єднань на проміжних та кінцевих LSR. Вимоги при використанні протоколу RSVP-TE багато в чому схожі у всій мережі, це обумовлено тим що у кожному LSR інформація про стан повинна як зберігатися так і періодично оновлюватись

Використання протоколу CR-LDP, вимагає зберігання більш подібної інформації, але лише на вхідному та вихідному LSR. До цієї інформації входить інформація про стан, включаючи параметри трафіку та дані про явно задані маршрути.

Резервування ресурсів у протоколі CR-LDP та протоколі RSVP-TE виконується на різних стадіях створення LSP. При використанні протоколу CR-LDP у повідомленні

запиту мітки Label Request переноситься повна інформація про параметри трафіку. Це до дозволяє узгоджувати параметри трафіку під час створення LSP та дає можливість керувати трафіком кожному маршрутизатору мережі MPLS. В той час у зворотному напрямку з використанням повідомлення призначення мітки Label Mapping передаються кінцеві значення параметрів. Задяки чому забезпечується контроль доступу та резервування ресурсів в реальному часі у кожному LSR. Використання такого підходу дозволяє не створювати LSP за маршрутом, у якого наразі відсутні необхідні ресурси [6].

При використанні протоколу RSVP-TE параметри трафіку передаються у Tspec (наборы специфікацій потоку даних відправника) в повідомленні Path. Аналізуючи повідомлення Tspec, в якому описані дані, що передаватимуться по LSP, транзитні LSR можуть прийняти рішення про маршрутизацію. Проте перед цим спочатку повідомлення Path повинно дійти до вихідного LSR у якому специфікація потоку даних Tspec перетвориться на специфікація потоку даних Flowspec, яку буде надіслано відправнику у звортньому напрямі у повідомлені Resv. У специфікації потоку Flowspec передаються деталі резервування ресурсів, що необхідні для створення LSP. Тобто, до того моменту доки повідомлення Resv не повернеться пройденим маршрутом до відправника, резервування ресурсів не буде виконано. Через це може статися ситуація, що на даному маршруті вже не буде вистачати ресурсів,і не вдасться створити LSP.

Протоколи CR-LDP та RSVP-TE для розповсюдженя міток, наскрізного запиту і відповіді на цей запит використовують потоки службових повідомлень [6]. У протоколі RSVP передбачено періодичне оновлення стану кожного LSP між суміжними вузлами завдяки чому можно автоматично враховувати зміни у дереві маршрутизації. У якості транспортного засібу він використовує IP-дейтаграми, через що сусідні вузли можуть припинити обслуговування, в ситуації коли керуюче повідомлення буде втрачено.

Тому періодична регенерація стану LSP дозволяє гарантвати, що LSP буде необхідним чином синхронізований між двома суміжними вузлами.

В той же час у протоколі CR-LDP використовується у якості транспортного засобу протокол TCP, що знімає необхідність у періодичній регенерації LSP між двома суміжними вузлами. Для підтвердження того що вузли залишаються активними він використовує повідомлення Hello, а повідомлення KeepAlive для моніторингу TCP-з'єднань. Обмін цими двума повідомлення ведеться не для безлічі LSP, TCP з'єднання а лише для вузла, через що у порівняння з RSVP він менше перевнтажує мережу.

У таблиці 2.1 наведено загальне порівняння протоколів CR-LDP, RSVP-TE.

Таблиця 2.1 – Порівняння протоколів CR-LDP, RSVP-TE

	CR-LDP	***RSVP-TE***
Використуємий протокол	TCP	Исходный IP
Надійність операторського класу	Ні	Так
Підтримка трафіку "багато точок - точка"	Так	Так
Підтримка мовної розсилки	Ні	Ні
Підтримка злиття LSP	Так	Так
Явна маршрутизація	З суворими і не суворими ділянками маршруту	З суворими і не суворими ділянками маршруту
Ремаршрутизація LSP	Так	Так, шляхом запису маршруту
Витіснення потоків у LSP	Так, на основі приорітету	Так, на основі приорітету
Засоби безпеки	Так	Так
Захист LSP	Так	Так
Стан LSP	Жорстке	Нежорстке
Регенерація стану LSP	Не потребується	Періодична, по ділянках
Резервування спільно використовуваних ресурсів	Ні	Так
Обмін параметрами трафіку	Так	Так
Управління трафіком	У прямому напрямку	У зворотньому напрямку
Авторизація користувачів	Неявная	Явная
Індикація протоколу рівня 3	Ні	Так
Обмеження залежно від класу ресурсу	Так	Ні

2.6 Реалізація DiffServ з MPLS

2.6.1 DiffServ

Як вже згадувалося сучасні мережі передачі даних несуть безліч різних типів послуг, включаючи голос, відео, потокову музику, веб-сторінки та електронну пошту. Багато запропонованих механізмів QoS, які дозволяли цим службам співіснувати, були складними і не могли масштабуватися для задоволення вимог загальнодоступного Інтернету.

Першими спробами забезпечити QoS в IP-мережах базувалися на моделі потоку за додатками (IntServ), у якій окремі програми запитували гарантії якості обслуговування безпосередньо від мережі [16]. Протокол сигналізації RSVP використовувався для розповсюдження запитів до вузлів у мережі, і стан потрібно було підтримувати для кожного потоку на кожному стрибку на шляху. З мільйонами потоків, що проходять через IP-мережі, цей підхід виявився не маштабованим і надто складним, і була розроблена більш груба модель у формі DiffServ.

Суть підходу DiffServ до вирішення проблеми QoS є у тому щоб розподілити трафік на невелики кількіть класів і розподіляти мережеві ресурси на основі кожного класу. Клас позначається в полі 6-бітної кодової точки DiffServ (DSCP) пакету, для робиться для того щоб можно було обійтися без протокола сигналізації.

Щоб уникнути потреби в протоколі сигналізації, клас позначається безпосередньо на пакеті в полі 6-бітної кодової точки DiffServ (DSCP). Поле DSCP є частиною поля оригінального байту типу служби (Type of Service, ToS) у заголовку IP [16]. Цей байт поля ToS, був розділений на поле DSCP, яке має величину 6-біті та поле явного повідомлення про перевантаження (ECN), з величною 2-біти. На рисунку 2.8 зображено як було перевизначено поле ToS.

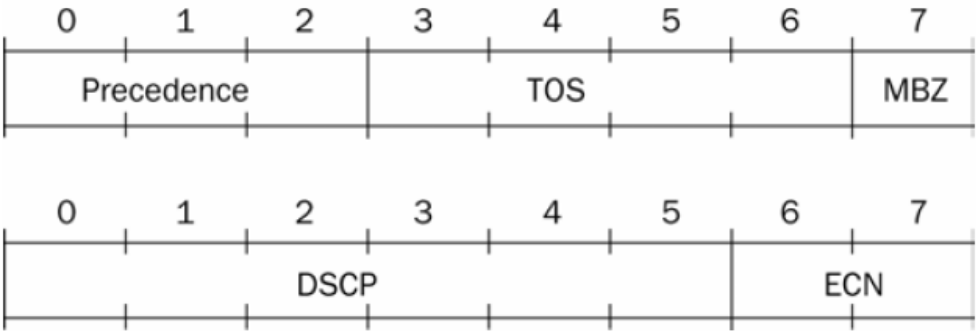

Рисунок 2.8 – ToS and DSCP + ECN

DSCP використовується для визначення рівня якості обслуговування пакета на певного вузлі мережі. Цей рівень якості мережі має назву per-hop behavior (PHB). PHB визначає порядок пердачі та ймовірність відкидання пакетів при перевищені ліміту черги. Окрім цього він визначає частоту обслуговування та ресурси виділені для кожної черги. Було визначено 14 класів PHB:

Перший клас має назву Best Effort (BE, Кращі зусилля). Трафік не отримує особливої обробки.

Другий клас має назву Expedited Forwarding (EF, Прискорене пересилання). Трафік супроводжується мінімальними затримками та низькими втратами.

Інші дванадцять класів PHB мають назву Assured Forwarding (AF, гарантоване пересилання. Ці класи прийнято іменувати наступним чином AFXY, де X це номер черги, а Y це почерговість відкидання. Прийнято використовувати чотири різні черги з трьома рівнями почерговості відкидання в кожній, це і дає дванадцять окремих класів AF PHB. Ці класи використовують для трафіку, що потребує гарантії швидкості, але не вимагає обмежень на затримку або тремтіння.

По при те, що прийнято використовуванти вище названі значення коду DSCP проте постачальники дозволяють операторам мереж перевизначати відповідність між DSCP та PHB, а також визначати нестандартні режими PHB [16].

Набір вузлів що підтримують DiffServ з однаковим набором визначених PHB, відображеннями DSCP-PHB та політикою надання послуг прийнято називати домен DiffServ. На границі такого домену трафік маркуються кодами DSCP, що вказують на бажаний рівень обслуговування PHB. Завдяки чому мережа з DiffServ здатна забезпечувати різну обробку трафіку у вузлах, та дозволяє виконувати різниі вимог QoS різних потоків. Недоліком цього підходу є не можливість гаратнувати необхідну якість обслуговування якщо шлях немає необхідну кількість ресурсів, проте він дозволяє не використовувати сигналізацію для кожного потоку трафіку та є маштабованим.

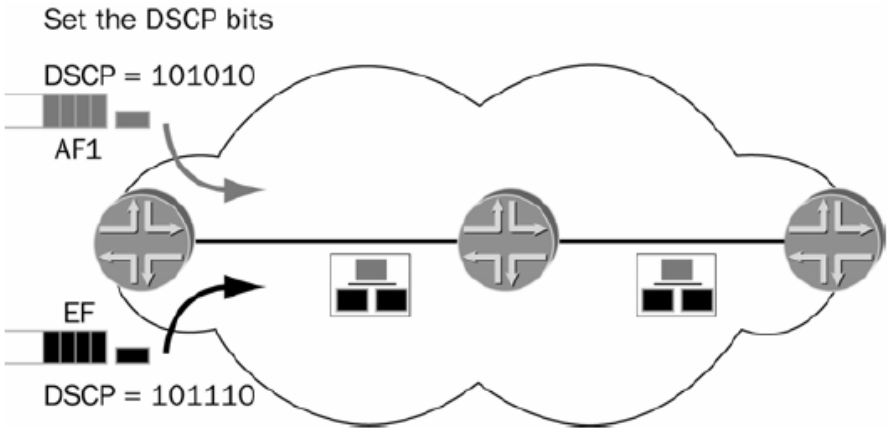

Рисунок 2.9 – Домен DiffServ

В загальному випадку DiffServ дозволяє забезпечити диференційовану обробку переадресації трафіку, таким чином забезпечуючи QoS для різних потоків трафіку. Окрім цього це є масштабоване рішення, що не потребує передачі сигнілізації і підтримки стану в ядрі. Однак не може гарантувати QoS, якщо шлях, за яким йде трафік, не має достатніх ресурсів для задоволення вимог QoS.

2.6.2 Class of Type – CT

Базовою вимогою DiffServ-TE є можливість окремо резервувати смугу пропускання для трафіку кожного класу. Для цього вводиться поняття клас типу CT

(Class of Type), під яким мається на увазі сукупність обмежень по смузі пропускання ланки даних. За допомогою CT здійснюється маршрутизація з урахуванням обмежень смуги пропускання звена та керування доступом. Передбачається до восьми CT, що позначаються CT(0-7) при цьому для трафіку з негарантованим обслуговування відповідає клас CT0. Тракти LSP які, гарантують смугу пропускання для певного CT, позначаються DiffServ-TE LSP. Відповідному LSP дозволено передавати трафік тільки певного CT і використовувати при цьому однакові або різні пріоритети витіснення трактів потоків.

2.6.3 Обчислення шляху

Маршрути в MPLS-TE розраховуються за алгоритмом CSPF (найкоротший шлях вибирається першим з урахуванням обмежень) по смугах пропускання ланок. Технологія DiffServ-TE додає в якості обмежуючої умови доступну смугу пропускання для кожному класу CT, що застосовуватися до LSP який створюється.

Для цього визначено ще TE клас, що є комбінацію CT та пріоритету. DiffServ-TE як і у випадку з класами CT підтримує максимум вісім TE-класів, від TE0 до TE7, які можуть вибиратися з 64 можливих комбінацій CT та пріоритету. Вибір цих восьми класів показано на рисунку 2.10.

Протоколи IGP переносять повідомлення про смугу пропускання, доступну для кожного TE-класу. Для того, щоб CSPF міг виконати достовірний розрахунок, CT та рівні пріоритету, вибрані для LSP, повинні відповідати одному з вибраних TE-класів [16].

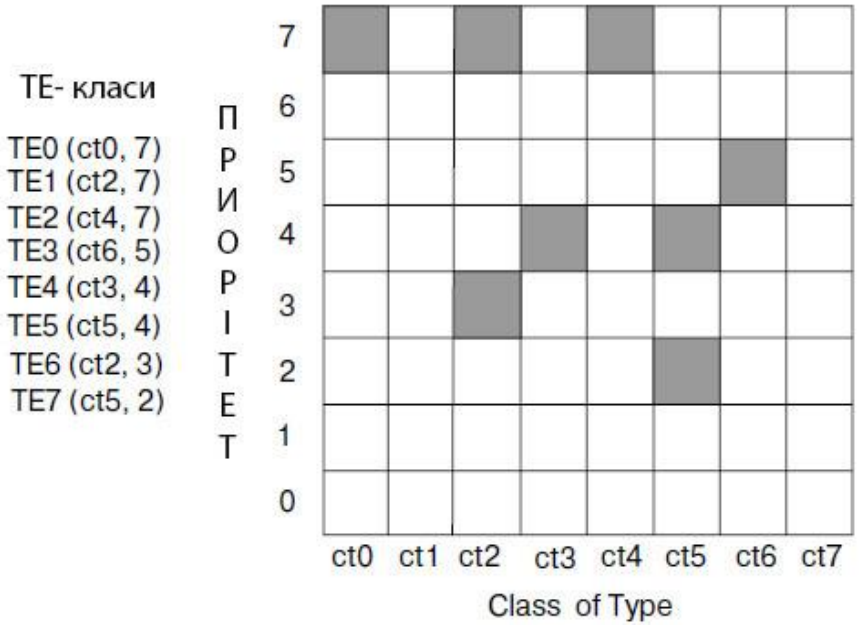

Рисунок 2.10 – Вибір восьми TE-класів з 64 можливих комбінацій

2.6.4 Сигналізація тракту

Результати розрахунку тракту повідомляються всім маршрутизаторам, через які проходять маршрути, що використовуються цим трактом, а потім у кожному маршрутизаторі виконується контроль доступу та облік смуги пропускання

Розширення протоколу RSVP-TE, дозволяють створювати тракти з резервуванням смуги пропускання кожному CT. Інформація про CT для LSP передається у вже згаданого Class of Type (CT) у складі повідомлення Path протоколу RSVP. Можливість поступового розгортання DiffServ-TE у мережі забезпечується тим, що:

• Об'єкт CT присутній лише у повідомленнях для трактів LSP від CT1 до CT7 включно у випадках коли об'єкт CT відсутній, то передбачається CT0.

• LSP, який отримує повідомлення Path з об'єктом CT і не розпізнає його, відмовляє в організації тракту.

Виконання цих правил гарантує, що LSP з резервуванням для кожного CT можна організувати тільки через LSP з підтримукою DiffServ-TE.

Важливим аспектом розрахунку доступної лінії пропускання є призначення лінії пропускання для різних CT. Частка пропускної спроможності ланки, яку може займати даний CT, називається обмеженням смуги пропускання BC (bandwidth constraint) [16].

Однією з моделей обмежень смуги пропускання є модель максимального призначення MAM (Maximum Allocation Model) в якій у відповідність одному BC ставиться один CT. В цій моделі пропускання здатність ланки просто розподіляється між різними CT, при цьому немає можливості розподілити смуги пропускання, що не використовується. Через що замість, передачі інших CT пропускна здатність може витрачатися даремно.

Інша модель призначення смуги пропускання, має назву RDM (Russian Dolls Model, Модель російської ляльки), яка покращує ефективність смуги пропускання порівняно з моделлю MAM, дозволяє CT спільно використовувати смугу пропускання. У цій моделі CT0 трафік із найкращим зусиллям, CT7 трафік із найсуворішими вимогами до QoS. Частка спільного використання різниться між двома крайнощами від 0 до 7. З одного боку BC0, що надає всю пропускну здатність каналу зв’язку, а з іншого боку BC7 котрий надає фіксований відсоток пропускної здатності каналу, зарезервований лише для трафіку від CT7.

Перевага RDM порівняно з MAM полягає в тому, що він забезпечує ефективне використання пропускної здатності шляхом спільного використання.

Недоліком моделі RDM у порівнянні з моделлю MAM є те, що відсутня розв'язка різних CT, і тому повинен використовуватися механізм пріоритетного витіснення для того, щоб відповідному CT у будь-якому випадку гарантувалася його частка пропускної здатності.

Таблиця 2.2 – Порівняння моделей MAM та RDM

MAM	RDM
Одному ВС ставиться у відповідність один CT; модель проста для розуміння та управління	Одному ВС ставиться у відповідність один або кілька CT, модель менш зрозуміла на інтуїтивному рівні
Забезпечує розв'язку різних CT та гарантує смугу пропускання різним CT без необхідності використовувати механізм пріоритетного витіснення	Відсутня розв'язка різних CT; щоб гарантувати смуги пропускання різним CT, потрібно використовувати механізм пріоритетного витіснення
Пропускна здатність може використовуватися неефективно	Ефективне використання пропускної спроможності
Корисна у тих мережах, де виключено пріоритетне витіснення	Не рекомендується в мережах, де виключено пріоритетне витіснення

2.7 Підсумок MPLS-TE

Механізм MPLS-TE здійснюється шляхом встановлення LSP, які можуть передавати трафік через бажаний шлях. Пакети класифікуються під час входу до вхідного маршрутизатора на межі мережі з підтримкою MPLS. Під час класифікації їм призначається заголовок MPLS за їхнім класом FEC, що допомагає їм працювати в мережі. Коли трафік проектується, налаштована специфікація потоку керує характеристиками трафіку та запитуваним класом обслуговування. Ці специфікації потоку визначають тип класу, кількість дозволеного трафіку та інші деталі трафіку, накладеного на вхідний маршрутизатор, який проектується через LSP.

Traffic engineering – це процес організації потоків трафіку в мережі таким чином, щоб можна було уникнути перевантажень, спричинених нерівномірним використанням мережі. Управління трафіком доповнює диференційовані послуги. Підводячи підсумок, MPLS встановлює маршрут для потока й водночас регулює обсяг трафіку, дозволеного в мережу, визначає наступний крок для пакета, тоді як диференційовані служби вказуватимуть обробку пакета, який очікує, щоб зробити наступний крок.

2.8 Висновки до розділу 2

Технологія багатопротокольної комутації по мітках MPLS (Multiprotocol Label Switching) позиціонується як спосіб побудови високошвидкісних IP-магістралей, але область її застосування не обмежується протоколом IP, а поширюється на трафік будь-якого мережевого протоколу, що маршрутизується.

Усі функції класифікації пакетів за різними FEC, а також реалізацію таких додаткових сервісів, як фільтрація, явна маршрутизація, вирівнювання навантаження та управління графіком, беруть на себе граничні маршрутизації. В результаті чого інтенсивним обчисленням займається гранична область, в той час як ядро займається високопродуктивною комутацією. Це дозволяє оптимізувати конфігурацію MPLS пристроїв залежно від їх розташування в мережі. Тобто, головною особливість MPLSє відокремлення процесу комутації пакета від аналізу IP-адрес у його заголовку.

Кожен із класів FEC обробляється окремо від інших - не тільки тому, що для нього будується свій шлях LSP, а й у сенсі доступу до загальних ресурсів таких як смуга пропускання каналу та буферного простор. В результаті технологія MPLS дозволяє дуже ефективно підтримувати необхідну якість обслуговування, не порушуючи гарантій, що надаються користувачеві. Застосування в LSR механізмів управління буферизацією та чергами, як наприклад зважена справедлива черга WFQ (Weighted fair queuing), дає можливість оператору мережі MPLS контролювати розподіл ресурсів та ізолювати трафік окремих користувачів.

Використання концепції інжирингу трафіка та дифференційованих послуг дозволяють забезпечувати необхідну якість обслуговування

3 МОДЕЛЮВАННЯ МЕРЕЖІ НАСТУПНОГО ПОКОЛІННЯ НА ОСНОВІ IP/MPLS

3.1 Вступ до моделювання та топологія мережі

Метою моделювання дослідження функціональних можливостей багатопротокольної комутації міток (MPLS) в якості інструменту управління трафіком та підтримки QoS для подальшого її використання в мережах наступного покоління. Аналіз вимірюваннь, пов’язаних із затримкою в черзі, пропускною здатністю та іншими проблемами, пов’язаними з трафіком. Потім перейдемо до тонкого налаштування мережі MPLS-TE, щоб також врахувати підтримку QoS під час агрегування потоків через один шлях комутації міток. Поєднавши диференційовані послуги з архітектурою MPLS для підтримки вимог QoS.

Для початку був проведен експеримент із мережею, налаштованою на запуск протоколу маршрутизації за найкоротшим шляхом OSPF. Це було необхідним для того, щоб виділити деякі з принципів маршрутизації найкоротшого шляху. Було вирішено не детально описувати результати з OSPF через те, що ця дисертація зосереджена на темі управління трафіком.

У якості інструменту моделювання використовувалося програмне забезпечення OPNET, а саме OPNET modeler 14.5. Причиною його вибору було те, що воно надає комплексне середовище розробки, що підтримує моделювання та імітацію мереж зв’язку. Окрім цього, вона містить утиліти збору та аналізу даних та дозволяє точно представити велику кількість близько розташованих подій у великій мережі.

Для експеременту була використана проста топологія мережі. Це було обумовленно тривалістю моделювання. Топологію мережі використану для експерименту не можна назвати реалістичною робочою мережею. Проте на меті було створення мережевого середовища, яке могло б представляти частину загальної топології мережі Інтернет-провайдера. Були використані маршрутизатори доступу на межі мережі, де трафік передавався або отримувався від сайтів. Основні

маршрутизатори були налаштовані на обробку трафіку від граничних маршрутизаторів. Між усіма мережевими пристроями використовувалося з'єднання DS1, тобто максимальну пропускну здатність було встановлено на рівні 1,544,000 біт/с. Сайти (sites) фактично це робочі станції та сервери, які передають або/і приймають дані. Було вирішено назвати їх сайтами, тому що вони могли б поводитися як власне мережеве середовище, підключене до граничного маршрутизатора постачальника послуг.

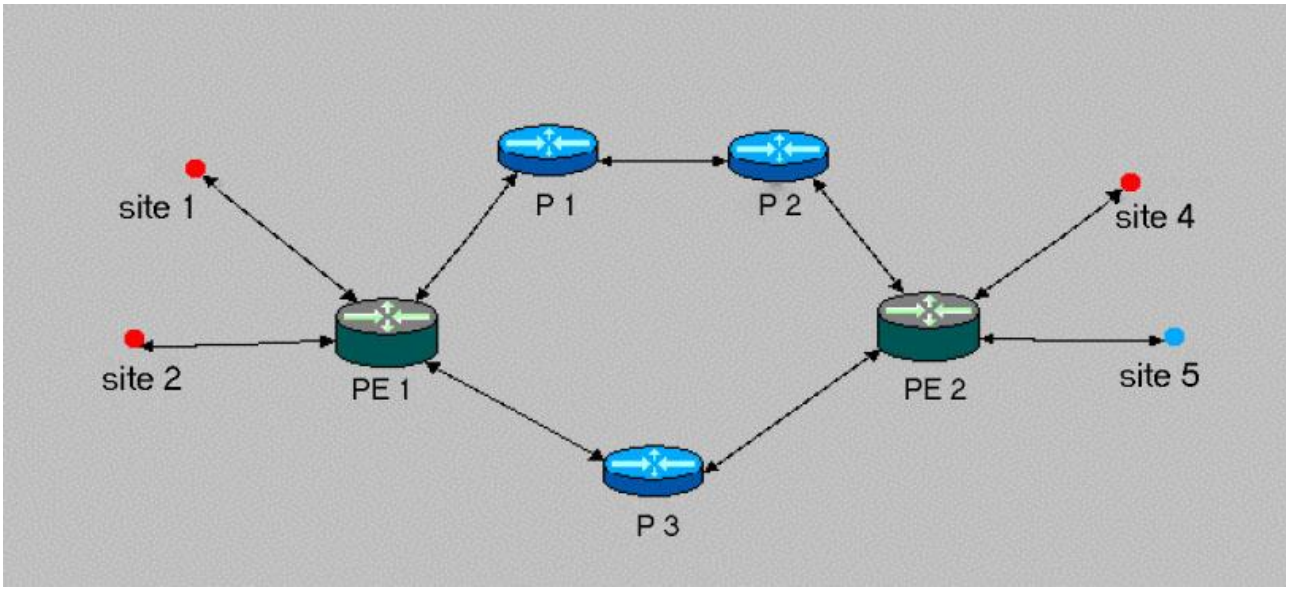

Рисунок 3.1 – Загальна топологія мережі

Через те що найбільша доля трафіку, що передається інтернетом, використовують як транспортний протокол TCP або UDP. Тому для генерації трафіку у експеременті були налаштовані додатки, що генерують трафік саме цих протоколів. Це було зробленно для того щоб виміряти обробку цих типів трафіку, при використанні OSPF, MPLS-TE та MPLS-TE з підтримкою QoS.

Генерування трафіку було запущено через дві хвилини. Це було зроблено для того, щоб маршрутизатори мали достатньо часу для обміну інформацією про топологію та створення своїх таблиць маршрутизації. Хоча і для такого невеликого мережевого середовища це було і не потрібно. На другій хвилині був запущений додаток для передачі файлів, що змусило TCP транспортувати свої пакети через мережу.

Інтенсивність TCP трафіку була встановлена на рівні 1,5 Мбайт/с файлів, що завантажуються на сервер. Це дає нам інтенсивність 1,500,000 біт/с. Наступний додаток, що передає свої пакети за протоколом передачі UDP було налаштовано розпочати генерацію на одну секунду пізніше. Таких додатків було створено п’ять із точно такою ж конфігурацією, які так само почергово запускаються через одну секунду. Це зроблено для того, щоб щоразу збільшувати ту саму інтенсивність трафіку UDP, та виміряти його вплив на трафік TCP. Для пакетів UDP було встановлено розмір 37500 байт/с. Це дає нам інтенсивність трафіку 300,000 біт/с, помножену на п’ять додатків, що досягли інтенсивності трафіку 1,500,000 біт/с.

Максимальна одиниця передачі (MTU, Maximum Transmission Unit) була встановлена для значення Ethernet v2 1500 байт. MTU визначає пакет IP-дейтаграми, що можна передати у кадрі. Тому, коли хост надсилає IP-дейтаграму, він може вибрати будь-який розмір, який захоче. Розумним вибором є MTU мережі, до якої безпосередньо підключений хост. Тоді фрагментація буде необхідною, лише якщо шлях до пункта призначення включає мережу з меншим MTU. Проте, якщо транспортний протокол, який розташований поверх IP, надає IP-пакет, більший за локальний MTU, тоді вихідний хост повинен фрагментувати його. Пакети, надіслані з програми передачі файлів, були встановлені на 1,5 Мбайт. Проте інтерфейси на маршрутизаторах і робочих станціях були налаштувані так, щоб сегментувати файл у значеннях Ethernet. Це обмумовлено тим, що завантаження необроблених IP-пакетів подібного розміру було б не реалістичним. Максимальний розмір повідомлення TCP призначений автоматично, тобто використовуватиметься значення IP.

Зсилаючись на рисунок 3.1 Site 1 має зв’язуватися з Site 5 використовуючи додаток передачі файлів, тобто на другій хвилині він розпочинає генерувати інтенсивність трафіку TCP. Site 2 використовує додаток для відеоконференцій перадаючи трафік на Site 4, тобто розпочинає генерувати UDP-трафік секундою пізніше як і було зазначено раніше. У Таблиці 3.1 вказана інтенсивність трафіку, що була встановлена для використання в усіх експерементах.

Таблиця 3.1 – Конфігурація трафіку для експерементів

Site	Протокол	Початок	Кінець	Інтенсивність трафіку
Site 1	TCP	120сек	126сек	1,500,000 біт/с
Site 2	UDP	121сек	126сек	300,000 біт/с
Site 2	UDP	122сек	126сек	300,000 біт/с
Site 2	UDP	123сек	126сек	300,000 біт/с
Site 2	UDP	124сек	126сек	300,000 біт/с
Site 2	UDP	125сек	126сек	300,000 біт/с

3.2 Імітаційний експеримент з використанням OSPF

Перший сценарій було створено, щоб висвітлити деякі принципи маршрутизації за найкоротшим шляхом. Проаналізувати проблеми пропускної спроможності та затримки в черзі, коли потоки трафіку конкурують за обмежені ресурси в умовах перевантаження.

У цьому сценарії не надаються жодні гарантії якості обслуговування жодному з типів трафіку. Тобто, будь-який трафік, що надходить у мережу, не отримуватиме жодної підтримки якості обслуговування. Значення поля типу сервісу пакетів було встановлено на (0) для класу пріоритету, що відповідає BE (Best Effort) класу обслуговування. Усі маршрутизатори у даному експеременті були налаштовані на використання лише Open Shortest Path First (OSPF) як протоколу маршрутизації.

3.2.1 Пропускна здатність

Site1 було налаштовано на генерацію TCP-трафіку з другої хвилини, він становив 1,500,000 біт/с. Опираючись на рисунок 3.2. можно побачити, що це значення було досягнуто. Через секунду Site 2 почав генерувати UDP-трафік розміром 300,000 біт/с, і з кожною секундою його інтенсивність продовжила збільшувалася на 300,000 біт/с. Через те, що обидва трафіки використовували свої канали до вхідного маршрутизатора, було

зафіксували, що інтенсивність трафіку UDP в даному випадку мала величезний вплив на інтенсивність трафіку TCP. Ці ефекти реєструвалися між сайтами та вхідним маршрутизатором PE1 кожного разу, коли інтенсивність UDP-трафіку збільшувалася. На малюнку 3.2 показано, що пропускна здатність TCP починає падати, коли трафік UDP починає генерувати трафік. Це змушує пропускну здатність TCP впасти нижче 750,000 біт/с з вихідних 1,500,000 біт/с протягом періоду цього моделювання. Трафік UDP не зважає на перевантаження в мережі, продовжуючи передачу свого трафіку незалежно від того, чи встигають пакети прибути до призначеного пункту призначення. Трафік UDP починає споживати ресурси та стабілізується не раніше, ніж досягне максимальної інтенсивності трафіку в 1,500,000 біт/с.

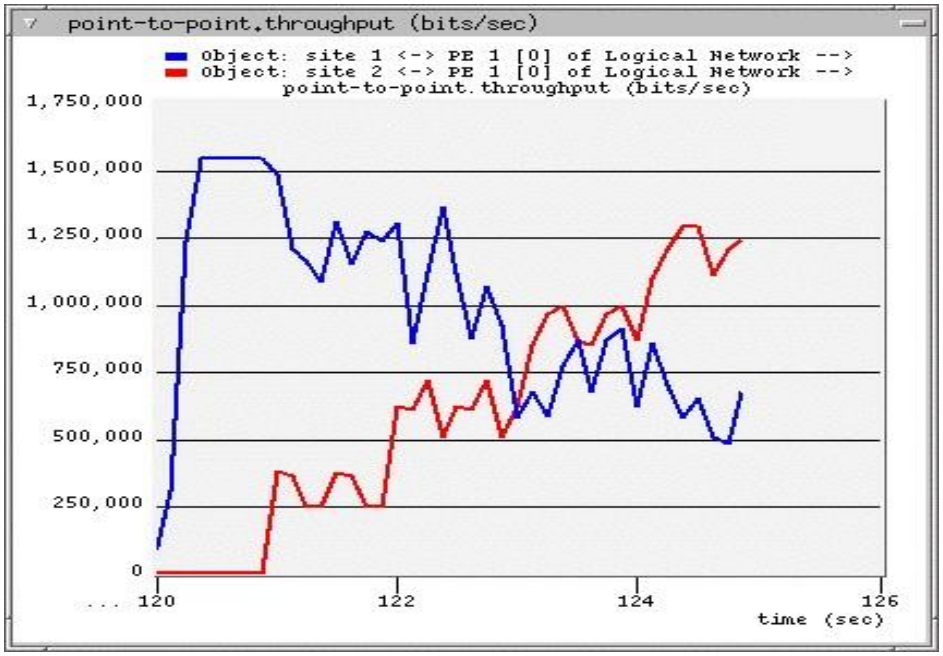

Рисунок 3.2 – Пропускна здатність TCP і UDP в біт/с

На рис. 3.2 показано кількість пакетів, надісланих від клієнтів до сервера. Спостерігаючи за результатом можна бачити, що кожен раз, коли UDP-трафік збільшує свою інтенсивність; інтенсивність трафіку TCP тим же чином знижує свою інтенсивність. Однак відразу після таких випадків зафіксовано деяке зростання. Причиною збільшення інтенсивності, після кожного зменшення, пов’язані з можливістю

швидкої повторної передачі в реалізації TCP RENO. Оскільки TCP реєструє, що після зменшення інтенсивності йому вдається отримати підтвердження для деяких переданих ним пакетів, його негайною реакцією є почати передачу додаткових пакетів знову. Також було зареєстровано деяке зменшення кількості пакетів, надісланих із сайту генерації UDP. Вважалося що UDP-трафік не зменшить інтенсивність трафіку в умовах перевантаження. Однак ці зменшення вважаються дуже незначними і відбуваються щоразу протягом менше секунди. Кожного разу, коли відбуваються такі зменшення, можно спостерігати деяке збільшення від генератора TCP. Все це відбувається за лічені секунди. Отримані результати пізніше будуть порівняні з результатами наступних експерементів щоб визначити переваги продуктивності наступних механізмів керування трафіком.

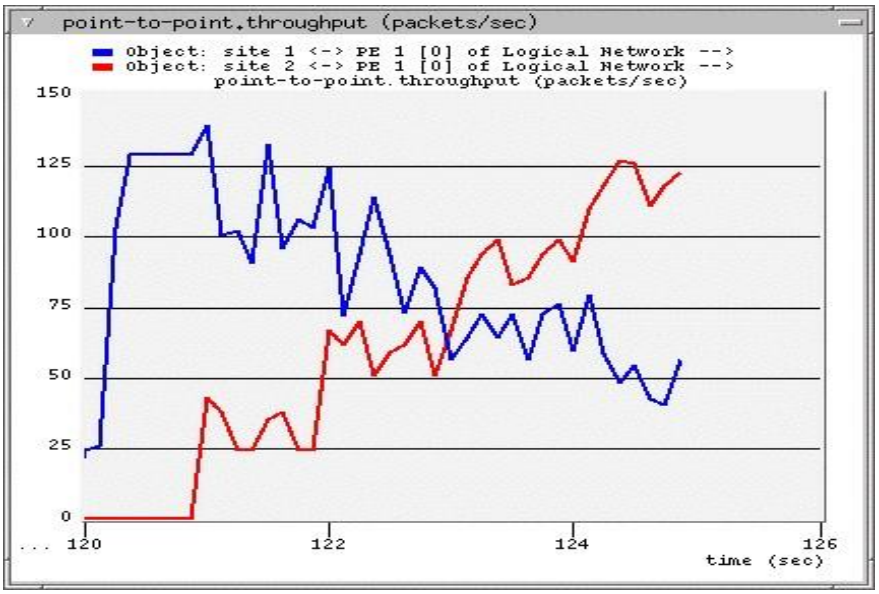

Рисунок 3.3 – Пропускна здатність TCP і UDP в пакетах на секунду

Ще одним отриманим у результаті моделювання виміром який відноситься до QoS, була пропускна здатність, шляхів між маршрутизаторами що обробляли потоки трафіку. Результати моделювання зображені на рисунках 3.4 і 3.5. З них можна бачити, що пропускна здатність шляху PE1-P1-P3-PE2 між маршрутизаторами не використовується взагалі на томість шлях PE1-P2-PE2 повністю завантажений. Це

вказує на недосконаліть протоколу у балансуванні трафіку. Можна бачити, що пропускна здатність одного шляху є нічим порівняно з іншим, якому необхідно значно більше пропускної здатності. З рисунків 3.4 та 3.5 можно побачити найкоротший шлях мав максимальну пропускну здатність 1,544,000 біт/с, в той час як що ненайкоротший шлях стабільно мав нульову пропускну здатність. З рисунку 3.5 можно спостерігати невелике падіння значеннь між 121 та 122 секундами. Невідомо чи було це пов’язано з програмним забезпеченням моделювання або з чимось іншим. Якби це відбулося точно на 121 секунді то можно було вказати, що це пов'язано з початком генерації UDP трафіку, проте це все ще може бути пов’язане із зареєстрованим результатом із запізненням лише на частку міллісекунди. Скоріше за все це пов'язано з помилкою програмного забезпечення і подальший розбір цього результату є недоцільним.

Метою цього моделювання було показати, що протокол маршрутизації не ефективно використовує мережеві ресурси в тоді коли на мережу припадає велике навантаження, та використовує лише найкоротший шлях між будь-якою парою вхідних і вихідних маршрутизаторів. Завдяки чому виникають вузькі місця та перевантаження в мережі. Якщо б топологія мережі при моделюванні була більш складною та інший трафік пересилався з інших маршрутизаторів використовуючи цей шлях до певного пункту призначення, результати були б значно гіршими від тих за отримані. У реальних мережах Інтернет-провайдерів різні типи трафіку можуть використовувати той самий найкоротший шлях, через що можна отримати такіж негативні результати у будь-якій точці між будь-якими маршрутизаторами, які стають частиною найкоротшого шляху. Це призводить до появи точок в мережі налаштованій згідно протоколу маршрутизації за найкоротшим шляхом.

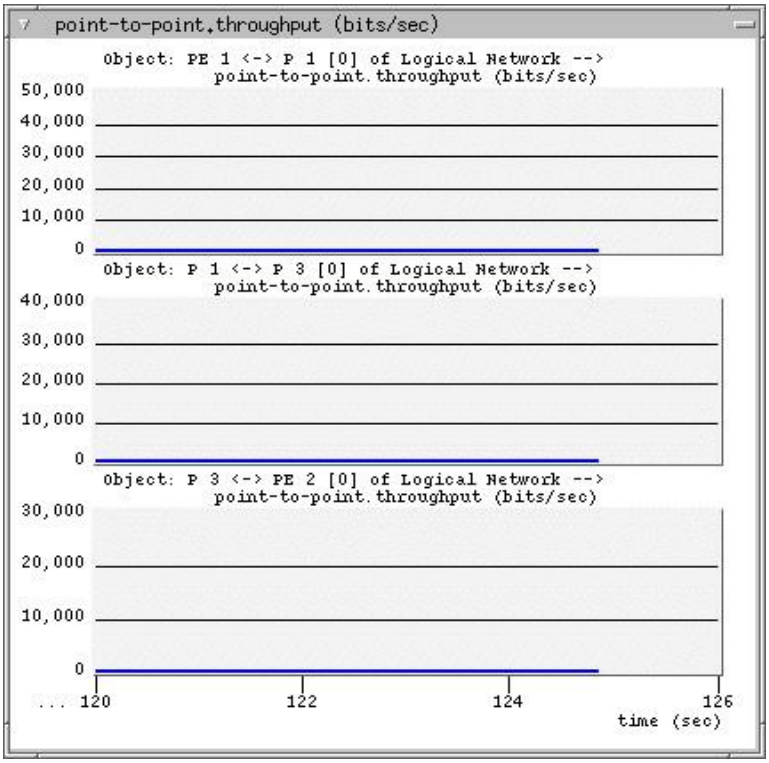

Рисунок 3.4 – Пропускна здатність PE1-P1-P3-PE2 в біт/с

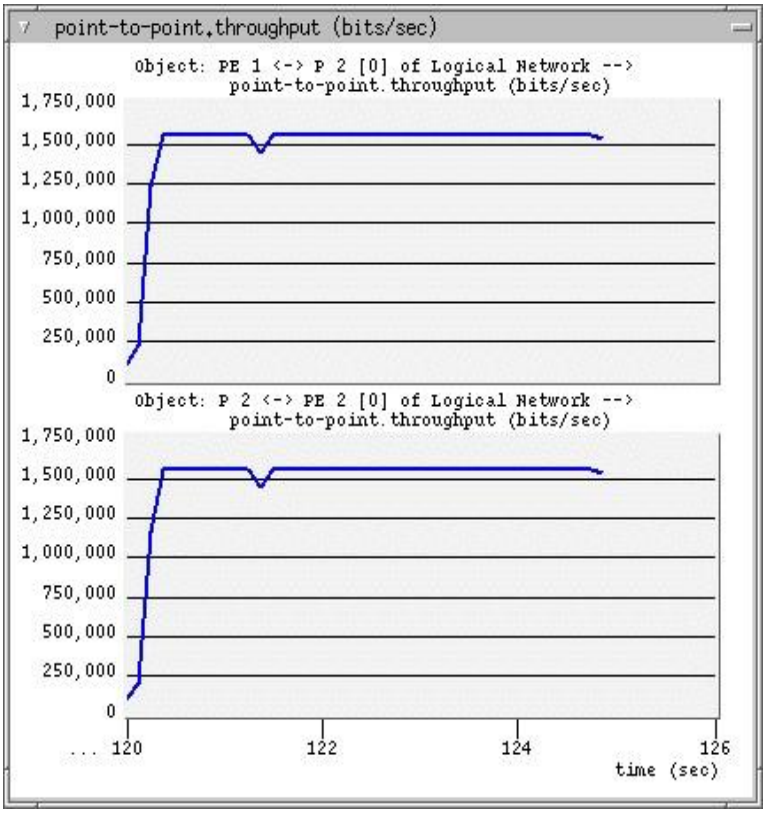

Рисунок 3.5 – Пропускна здатність PE1-P2-PE2 в біт/с

3.2.2 Затримки в черзі

Також були отримані результати затримки в черзі та пропускної здатності периферійних та основних маршрутизаторів. На рисунку 3.6 можно побачити що між маршрутизаторами, які поєднують ненайкоротший шлях не було зареєстрували жодних дій. Це закономірний результат, оскільки цей шлях не був використаний протягом часу моделювання. Проте, затримка в черзі від PE1-P2 зростає кожен раз, коли UDP трафік коли збільшує свою інтенсивність. Перше збільшення відбулося на 121 секунді, коли трафік UDP починає генерувати 300,000 біт/с. Відразу спостерігається невелике збільшення значення затримки в черзі. Кожного разу коли збільшується інтенсивніть трафіку UDP, можно бачити підвищення значення затримки в черзі. Це також закономірний результат через те що обсяг трафіку, який перевищує обмеження пропускної здатності, накладене посиланнями, збільшується щосекунди з моменту генерації трафіку UDP.

Іншим поясненням такого значення черги може бути у тому що не було застосовано раннє відкидання пакетів. Проте реалізація цього дала б вже інші результати. Через те ці трафіки пов’язані з класом найкращого обслуговування, їх можна було б викинути. З рисунка 3.7 видно, що черга набагато більша між вхідним маршрутизатором і першим маршрутизатором на шляху. Від другого маршрутизатора та після нього затримка в черзі має стабільне значення 0,008 секунди, що є нижчим порівняно з попередньою чергою на шляху. Це означає, що велика черга виникає лише між першими маршрутизаторами. Це обумовлено тим що вхідний маршрутизатор пересилає достатню кількість пакетів, що може перенести канал, підключений до першого маршрутизатора. Оскільки всі інші посилання на шляху мають однакову пропускну здатність, велика черга більше не важлива. Можна зробити висновок, що значення черги, між маршрутизатором P2 і вихідним маршрутизатором, зберігає нормальне значення, коли пересилається достатньо трафіку, який здатні перенести канали, безпосередньо підключені до нього.

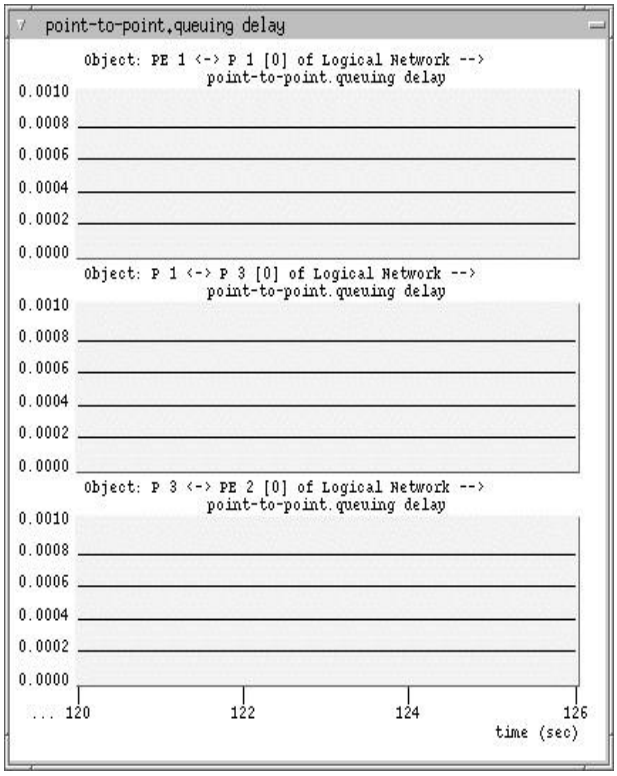

Рисунок 3.6 – Затримки в черзі шляху PE1-P1-P3-PE2

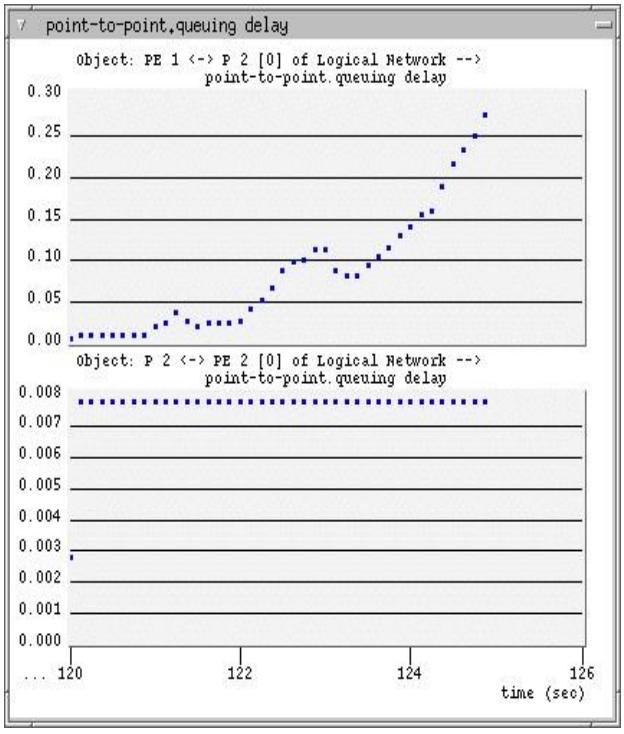

Рисунок 3.7 – Затримки в черзі шляху PE1-P2-PE2

3.2.3 Висновки по експерименту

Після отримання та аналізу результатів моделювання, вдалося змоделювати деякі проблеми які пов’язані з принципом маршрутизації найкоротшого шляху. З результатів симуляції можно зробити висновок, що в ситуаціях коли мережа з налаштованим найкоротшим шляхом є сильно завантаженою UDP-трафік починає заглушати TCP-трафік. Відповіддю на таку поведінку є те, що протокол TCP відчуває перевантаження та використовує свій механізму керування потоками через що сповільнюється передача трафіку в мережу. Він робить це, навіть якщо UDP-трафік не має вищої підтримки QoS, наданої постачальником мережевих послуг. У нашому моделюванні обидва потоки трафіку були налаштовані на використання BE класу обслуговування, але це не завадило UDP просто перевантажити мережу та заглушити потік трафіку TCP.

Негативний вплив на затримку в черзі між PE1 та P2 відбувається через трафік, що намагається використовувати лише найкоротший шлях до місця призначення. За умови сильного навантаження на мережу це невдалий вибір. Затримка в черзі зростає для одного шляху, в той час як інший шлях має достатньо можливостей для роботи з трафіком і не використовується. Затримка в черзі викликає стрімке зростання затримки як для TCP, так і для UDP трафіку. Незважаючи на те, що UDP-трафік не розуміє та не реєструє, чи досягають його пакети місця призначення чи ні, він продовжує підтримувати високу інтенсивність трафіку. Інтенсивність трафіку TCP діє навпаки, страждаючи від свого механізму керування потоками, через що заглушується трафіком UDP.

Маршрутизація найкоротшого шляху розчаровує коли йдеться про ефективне балансування трафіку. Звичайно є можливість балансування навантаження OSPF, проте це потребує значного адміністрування та може стати надзвичайно складним у більш складному мережевому середовищі. Маршрутизація за найкоротшим шляхом не передбачає ефективного балансування навантаження трафіку, тому можуть мати місце механізми більш ефективного використання мережевого середовища.

3.3 Імітаційний експеримент з використанням MPLS –TE

Рисунок 3.8 ілюструє сценарій управління трафіку з використання MPLS. Попередню мережеву модель було скопійовано, з єдиною відмінність, у вигляді червоної та синьої стрілки якими позначені два шляхи коммутації по мітках через експериментальну мережу.

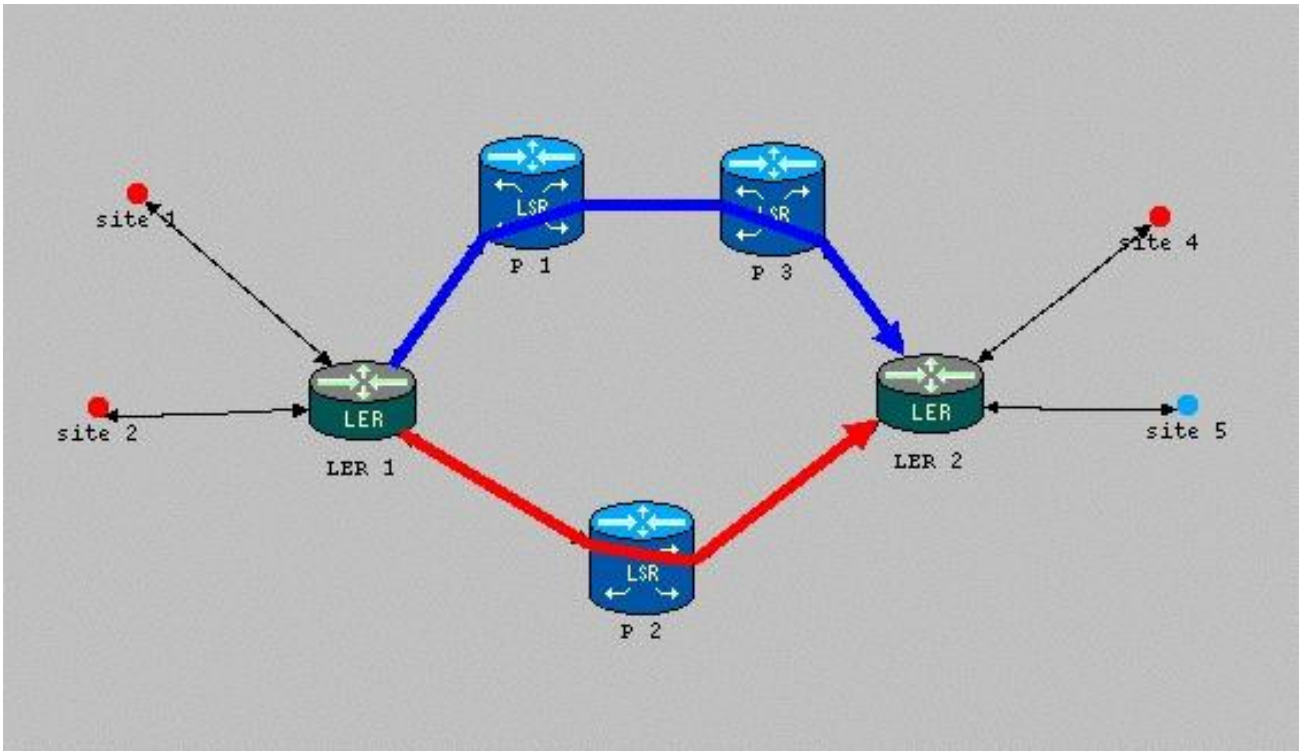

Рисунок 3.8 – Модель мережі MPLS

Щоб мати можливість керувати потоками трафіку, потрібно було встановити шляхи коммутації по мітках (LSP). Статичні LSP були створені, щоб мати більш точний контроль над шляхом, який має використовувати потік даних. Також були визначені специфікації потоку (Flowspec), які регулюються вхідним маршрутизатором для трафіку, що надходить в мережу. У таблиці 3.2 нижче описано дві частини потокової специфікації, TSpec і RSpec. Flowspec1 для трафіку, що надходить до червоного LSP, і його характеристики трафіку. TSpec було налаштовано на максимальну швидкість

передачі даних 1,544,000 біт/с, середню швидкість передачі даних 1,500,000 біт/с, максимальний розмір пакету 64,000 біт/с, а його RSpec (service request specification) був класом обслуговування найкращих зусиль. Копію цієї специфікації потоку було зроблено та налаштовано для синього LSP. Таблиця 3.2 підсумовує таблицю конфігурації специфікації потоку flowspec. Оскільки керванння трафіком відбувається за типом транспортного протоколу, трафік, що надходить у LSP без необхідного типу протоколу, відхиляється.

Таблиця 3.2 – Конфігурація специфікації потоку

Потоки	Максимальна швидкість передачі даних (біт/с)	Середня швидкість передачі даних (біт/с)	Макс. Розмір пакету (біт)	Дії поза профілем
Flowspec1	1,544,000	1,500,000	64,000	Відкинути
Flowspec2	1,544,000	1,500,000	64,000	Відкинути

LSP були встановлені між парою вхідних і вихідних маршрутизаторів LER1 та LER2. Ці маршрутизатори відіграють дуже важливу роль, оскільки вони керують та контролюють відображенням трьох важливих елементів конфігурації MPLS а саме класом еквівалентності пересилання (FEC), специфікацією потоку та використанням LSP. Один клас FEC було надано одному типу потоку, у нашому випадку трафіку TCP, а інший клас FEC було надано трафіку UDP. Потоки трафіку були налаштовані так, що вони надходять у мережу зліва направо, тобто site1 і site2 генерують трафік до site4 і site5, інтерфейси вхідного маршрутизатора (LER1) необхідно було налаштувати корректно. Під цим мається на увазі, що LER1 потрібно було налаштувати для призначення FEC на основі того, які інтерфейси та тип трафіку йому передавався. Крім того, щоб призначити FEC, інша інформація, зібрана з вхідних пакетів, також перевірялася на вхідному маршрутизаторі LER1. FEC було призначено на основі регулюючих правил, наведених у таблиці 3.3.

Таблиця 3.3 – специфікація FEC

Назва FEC	Використаний протокол	Адреса призначення	Використаний LSP
TCP Traffic	TCP	192.0.13.2 (Site5)	Синій LSP
UDP Traffic	UDP	192.0.11.2 (Site4)	Червоний

На вхідному маршрутизаторі LER1 пакетам призначаються відповідні FEC. Після чого FEC призначаються до відповідної специфікації поток, яка використовує певний LSP. Таким чином, вхідний трафік керується на основі певних адміністративних правил. Оскільки ціллю було усунути недоліки експериментальної мережі з найкоротшим шляхом, конфігурація MPLS-TE мала на меті виміряти продуктивність, передачі TCP та UDP трафіку розділеними шляхами у мережі. UDP-трафік був налаштований на використання червоного LSP, в той час TCP-трафік мав використовувати синій LSP.

3.3.1 Пропускна здатність

Згадаємо,що site1 налаштовано на генерацію TCP-трафіку з другої хвилини. Обсяг цього трафіку становив 1,500,000 біт/с. І як можна побачити по результатах рисунку 3.9 це значення було досягнуто і було стабільним, доки не почав генеруватися трафік UDP. Пам’ятаючи, що обидва трафіки використовували свої власні з’єднання до вхідного маршрутизатора, було зафіксовано, що інтенсивність трафіку UDP впливає на інтенсивність трафіку TCP. Помітний ефекти впливу виникав кожного разу, коли інтенсивність трафіку UDP змінювалася. Перехідні значення коливалися в діапазоні від значення максимальної пропускної здатності 1,544,000 біт/с аж до 1,250,000 біт/с. На отримані перехідні значення могли впливати декілька факторів.

По-перше, підтвердження TCP дійсно передавалися від сервера назад до клієнта найкоротшим шляхом. Через те що цей найкоротший шлях буде сильно зайнятий

обробкою трафіку UDP, що ускладнує передачу пакетів підтвердження коли інтенсивний трафік UDP конкурує з ним за ті самі ресурси найкоротшого шляху. Трафік UDP гарантував пропускну здатність для його використання односпрямованим LSP, який сервер використовував би для передачі пакетів підтвердження клієнту FTP. В випадку TCP-трафіку однією з причин є відсутність підтвердження, яке очікується від відправника. Під час налаштування експериментальної мережі не бралася до уваги ця проблема, але її бажано розглянути, щоб виміряти її вплив на трафік TCP. Під час управління трафіком TCP, можна взяти до уваги шлях, який може пройти пакет підтвердження до сторони передавача. Звичайно, це не актуально, коли доступна достатня пропускна здатність. При тому пакети підтвердження відносно невеликі за розміром, а з'єднання, що використовувалися, були дуплексними. Тому не можно бути впевненим, чи впливає ця проблема на зареєстровані значення падіння інтенсивності трафіку TCP. У нашому випадку пропускної здатності було достатньо, щоб впоратися як з трафіком UDP, так і з пакетами підтвердження TCP, доки трафік UDP, який використовує найкоротший шлях, не досяг максимальної інтенсивності трафіку під час останнього збільшення інтенсивності трафіку. Саме тоді була зареєстрована найнижча пропускну здатність TCP. Проте менше чим через секунду пропускна здатність повертається до максимальної інтенсивності трафіку. Припущення, що така швидка повторної передача трафіку здійснюється за допомогою деталей реалізації TCP RENO.

По-друге, звернемо увагу ще до одного фактора пов'язаного з вхідним маршрутизатором, який відповідає за перенаправлення переданого йому трафіку. Пакети, призначені для обробки трафіку, повинні відповідати політиці та резервувати шляху комутації по мітках, який вони використовуватимуть. Використовуючи LSP, маршрутизатор повинен відстежувати, яку специфікацію потоку встановлену для LSP, пакети можуть використовувати. LER1, який є вхідним маршрутизатором, повинен керувати величиною середньої швидкості передачі даних, дозволеною специфікацією потоку, визначеною для кожного LSP.

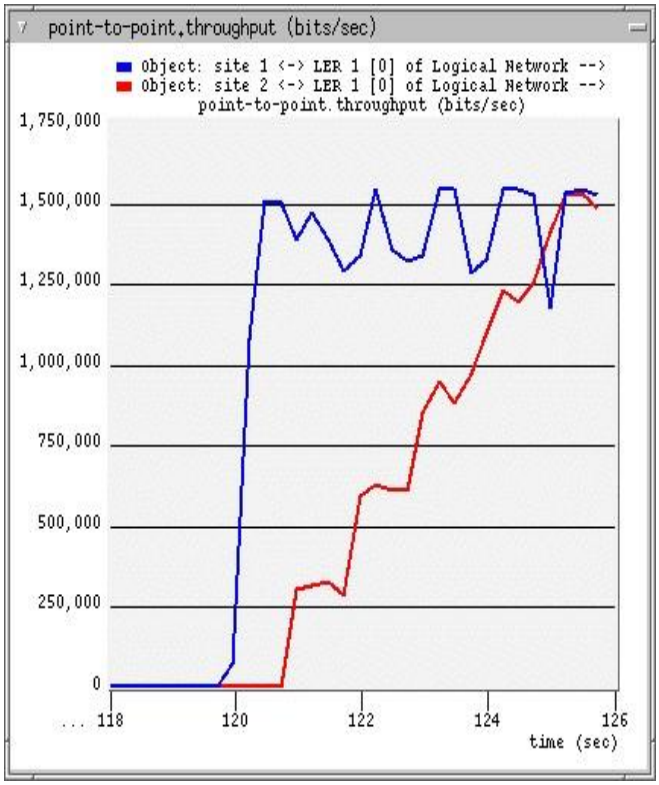

Рисунок 3.9 – Пропускна здатність TCP і UDP до LER1

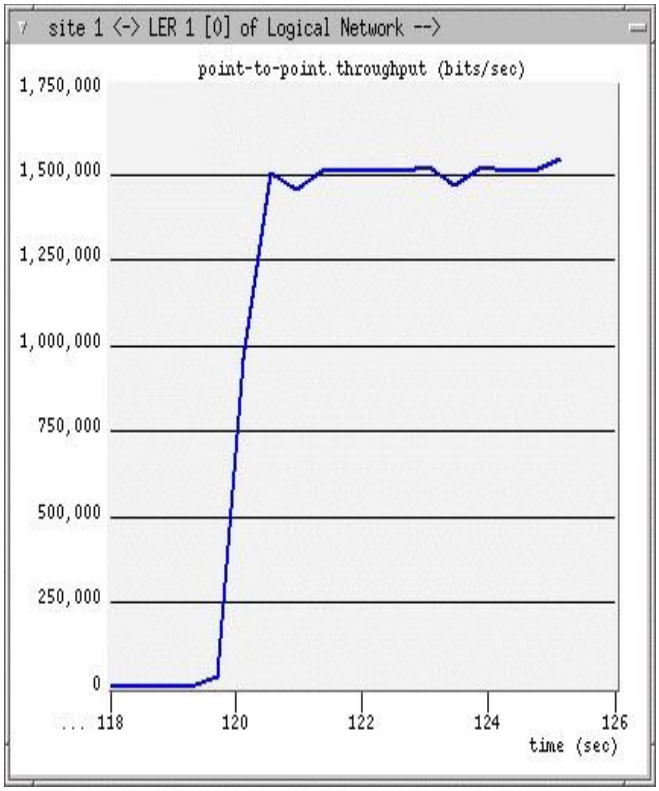

Рисунок 3.10 – Пропускна здатність TCP до LER1

Специфікація потоку яка визначена та використовується трафіком TCP, дозволяє середню швидкість передачі даних лише у розмірі 1,500,000 біт/с. Через те що TCP-трафік інколи перевищував дозволену середню інтенсивність трафіку, необхідно було створити певну чергу на вхідному маршрутизаторі, щоб регулювати розмір налаштованого обмеження середньої швидкості.

На рисунку 3.14 показано величину затримки в черзі між вхідним маршрутизатором LER1 і першим маршрутизатором на шляху. Затримка в черзі має певний прямий вплив на протокол TCP. Протокол TCP реєстрував би затримку та знижував би свою інтенсивність, таким чином викликаючи зареєстровані значення зниження інтенсивності трафіку. Через те що протокол TCP відчуває деяку затримку для підтвердження, він страждає від свого ж механізму керування потоками, таким чином знижуючи інтенсивність передачі. Це ймовірно є головним фактором цього інциденту. Зважаючи на отримані значення можно бачити що кожного разу, коли UDP-трафік збільшує свою активність, на його активність впливає затримка в черзі між входом і першим основним маршрутизатором на шляху. Отже, це знову відображається на пропускній здатності TCP між джерелом і вхідним маршрутизатором. Кожне збільшення інтенсивності трафіку UDP означає падіння інтенсивності трафіку TCP.

Проте метею було отримати результат при якому, трафік TCP не страждав від трафіку UDP, що генерується в мережу, шляхом його проектування в окремий шляху. У попередньому досліді було змодульовано пригнічення трафіку TCP, при конкуренції з трафіком UDP за ті самі ресурси найкоротшого шляху. Оскільки TCP має механізм керування потоком, він знижує інтенсивність трафіку, коли в мережі з’являться ознаки перевантаження. Трафік UDP, з іншого боку, не страждає від цього механізму керування потоком, завдяки чому він стає переможцем двох протоколів за умови високого навантаження. Оскільки ці потоки були спроектовані з розділенням шляхів за допомогою MPLS-TE, обидва типи трафіку постійно зростали майже до максимальної доступної смуги пропускання. Це показує, що навіть із деяким зниженням інтенсивності трафіку TCP, зареєстрованого від джерел до вхідного маршрутизатора, трафік TCP та

UDP має прийнятну продуктивність. Досягнення практично повного використання доступних ресурсів мережі.

Іншими результатами, отриманими в результаті експеременту MPLS-TE, були вимірювання пропускної здатності шляхів між маршрутизаторами, що обробляють потоки трафіку. На рисунках 3.11, 3.12 показано результати моделювання. Було зареєстровано, що пропускна здатність між маршрутизаторами, що поєднують найкоротший шлях і ненайкоротший шлях, була більш збалансованою порівняно з мережею з найкоротшим шляхом, що була змодельованою раніше. Проте на рисунку 3.11 можно спостерігали пропускну здатність трафіку TCP, що проходить через синій LSP. Тут пропускна здатність починає зростати до запланованих 1,500,000 біт/с. Після чого реєструються нестабільні значення пропускної здатності, які відбуваються приблизно кожну секунду. Кожну секунду пропускна здатність зменшується, а потім повертається до максимальної пропускної здатності. Причиною такої поведінки може бути поєднанням проблем, розглянутих нижче. Тут відчутен більш сильний зв'язок між інтенсивністю трафіку TCP та UDP. Щоразу, зі збільшенням інтенсивність трафіку UDP можно спостерігати його вплив на інтенсивність трафіку TCP. Підводячи підсумок, що секунди під час експеременту інтенсивність трафіку UDP збільшувалась. Зниження пропускної здатності TCP відбувається приблизно в той самий час, коли збільшується інтенсивність трафіку UDP. Це не великою проблемою, оскільки пропускна здатність зберігає початкову високу пропускну здатність одразу після реєстрації збільшення інтенсивності трафіку UDP.

З зареєстрованих результатів можно підтвердити, що ненайкоротший шлях був більш ефективно використаний за допомогою можливостей MPLS-TE. Без інжирингу трафіку, ймовірно, не спостерігалася б жодна активність пропускної здатності вздовж ненайкоротшого шляху, як було змодельовано в попередньому розділі. Тоді TCP-трафік постраждав би набагато більше, конкуруючи трафіком UDP за найкоротшим шляхом.

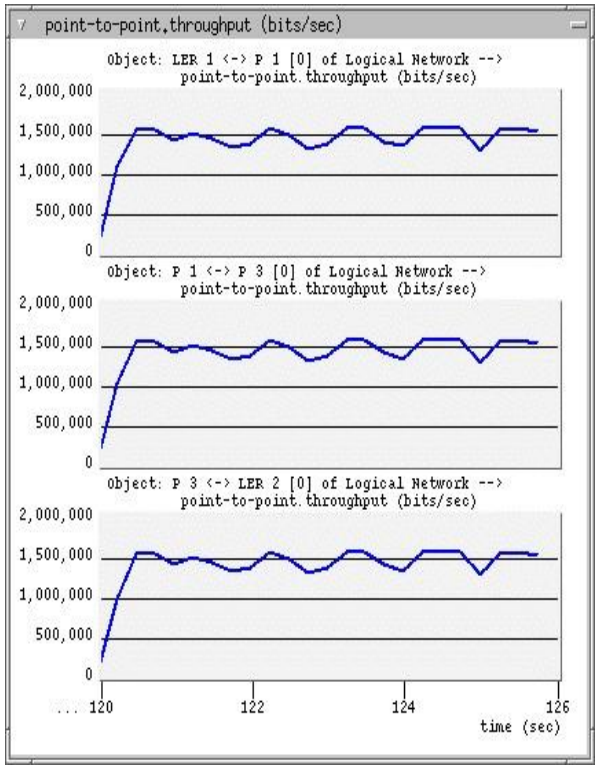

Рисунок 3.11 - Пропускна здатність LER1-P1-P3-LER2

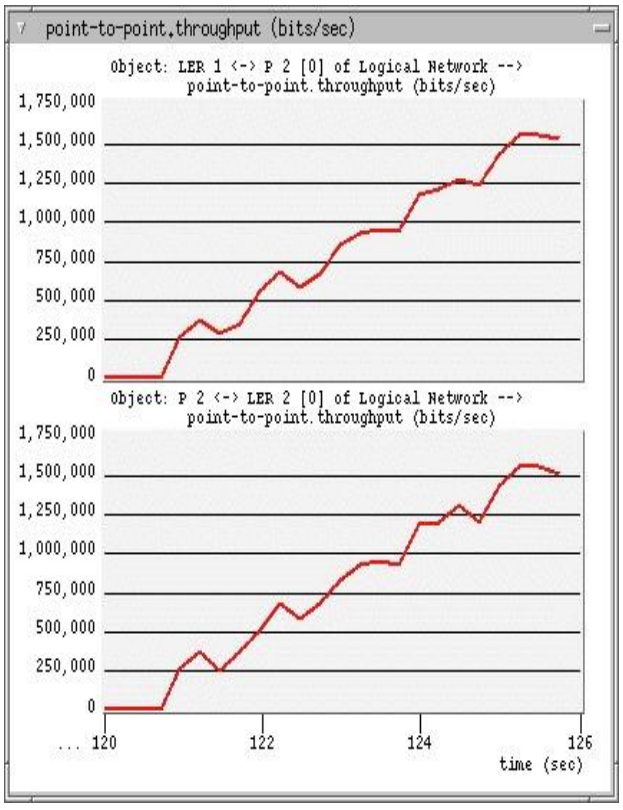

Рисунок 3.12 - Пропускна здатність LER1-P2-LER2

На рисунку 3.12 можно спостерігати інтенсивність пропускної здатності маршрутизаторів, що об’єднують шляхи LER1-P2-LER2 через червоний LSP. Отримані значення пропускної здатності трафіку UDP були менш цікавими. Однак і тут були зафіксовані дещо нестабільні значення пропускної здатності. Проте вони настільки малі, що їх дослідження є малоактуальними. Оскільки UDP-трафік використовує лише цей шлях, нам вдається уникнути перевантажень у мережі. Якби було налаштовано маршрутизацію за найкоротшим шляхом, ми б використали цей шлях надмірно, через що обидва потоки трафіку страждали б від заторів у мережі.

Також були зібрані статистичні результати щодо обсягу трафіку, який намагався увійти, та фактичного обсягу трафіку, якому вдалося вийти з LSP. На рисунках 3.13 та 3.14 показано нанесені на графік результати. На рисунку 3.13, що показує кількість трафіку, яка входить і виходить із синього LSP, було зареєстровано трафік обробки TCP, досягнутий у цьому LSP. Лінія чорного кольору на графіку показує кількість трафіку, що входить до LSP, тоді як лінія зеленого кольору вказує на кількість трафіку, що виходить з LSP. На рисунку 3.14 нижче можно бачити, що трафік, накладений на LSP, добре обробляється, і показує, що той самий обсяг трафіку пересилається за допомогою LSP. Звичайно, були зареєстровані деякі відмінності між двома побудованими графіками. Однак кількість трафіку, що виходить з LSP, не була зареєстрована нижчою, ніж кількість трафіку, що входить до LSP, до двох останніх зареєстрованих скачків. Проте ці відхилення є незначними і не є ані важливими, ані настільки відносними, щоб про них розповідати далі. Те саме стосується трафіку UDP і використання LSP червоного кольору. Тут також кількість трафіку, що входить і виходить з LSP, була рівною.

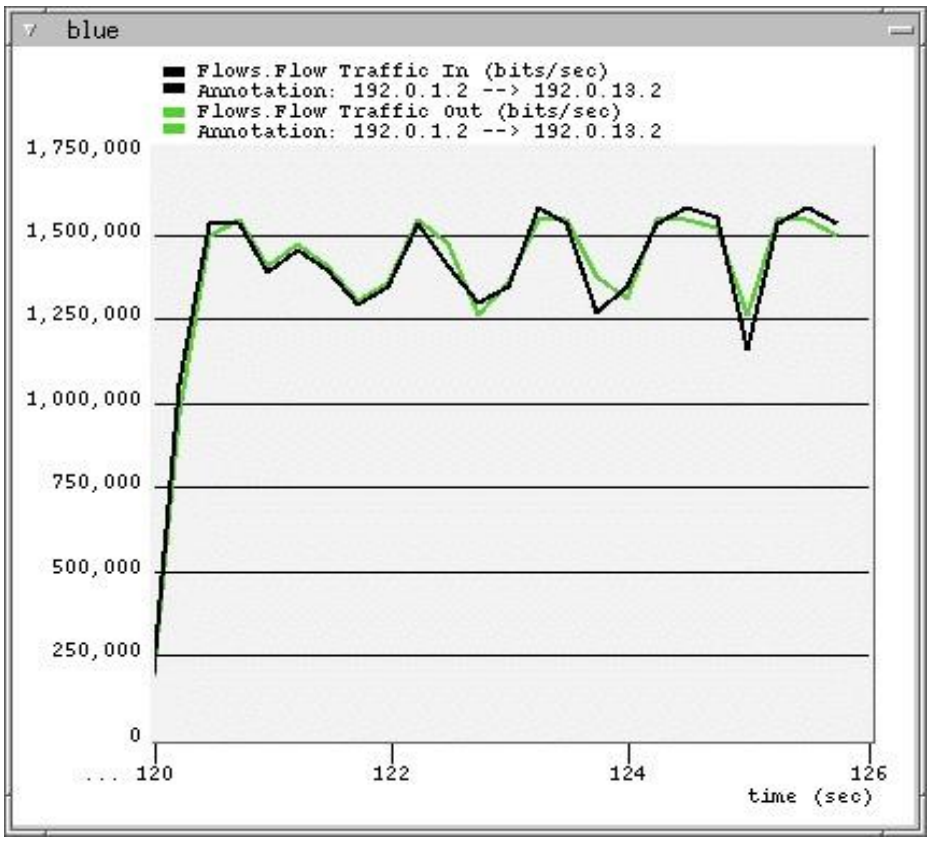

Рисунок 3.13 – Вхідна, вихідна пропускна здатність синього LSP

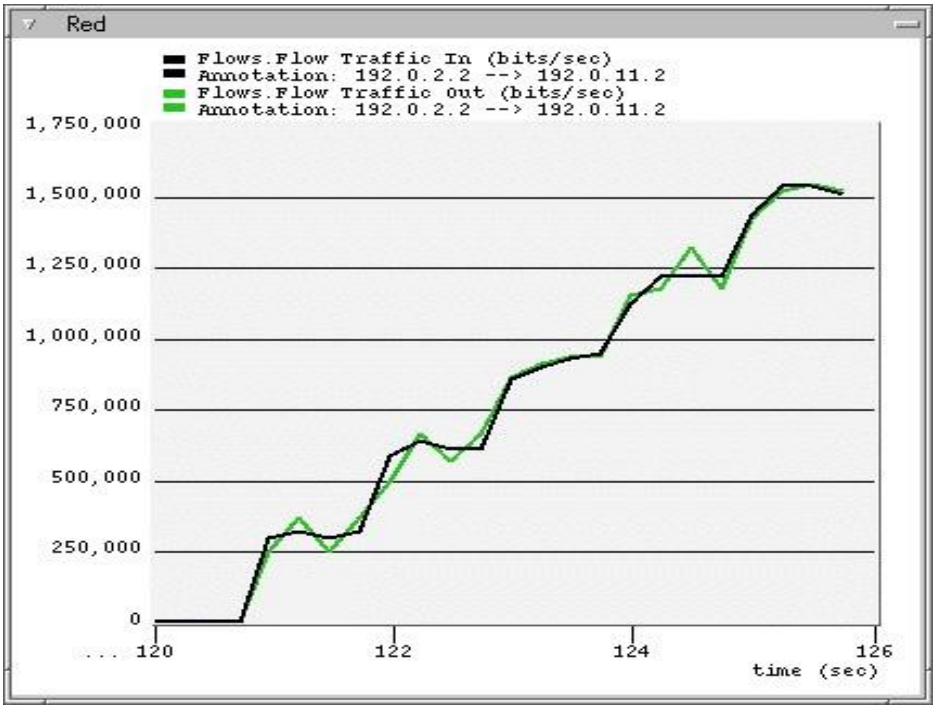

Рисунок 3.14 – Вхідна, вихідна пропускна здатність червоного LSP

3.3.2 Затримки в черзі

Зібрано результати щодо затримки в черзі від периферійних та основних маршрутизаторів, що пов’язана з QoS. З рисунків 3.15 та 3.16 можно бачити, що затримка в черзі більш збалансована між обома шляхами, у порівнянні з випадком маршрутизації найкоротшого шляху. На вхідному маршрутизаторі LER1 значення затримки в черзі деяким чином підвищувалося кожного разу коли збільшувалася кількість трафіку UDP, що проходить через нього. Значення затримки в черзі щоразу збільшувалося, а потім поверталося до свого нормального значення. Крім того, кількість цього раптового збільшення пов’язана з збільшенням обсягу трафіку UDP. Кожного разу, коли трафік UDP збільшував свою інтенсивність трафіку на 300,000 біт/с, затримка в черзі впливала з більш вищим значенням на час затримки в черзі трафіку TCP. Причиною цього ефекту може бути той факт, що вхідний маршрутизатор, який обробляє обидва типи трафіку, стає більш зайнятим, пересилаючи трафік. Цей небажаний ефект виникає навіть тоді, коли обидва типи трафіку використовують окремі шляхи до вихідного маршрутизатора в межах домену MPLS.

Трафік UDP, який використовує шлях LER1-P2-LER2, здається, має нижчі значення затримки в черзі, ніж трафік TCP. Це так, доки інтенсивність трафіку UDP не почне наближатися до максимальної доступної пропускної здатності каналу. Він зберігає стабільне значення приблизно на 0,0075 секунди до останнього додаткового збільшення на 300,000 біт/с, досягаючи 1,200,000 + 300,000 = 1,500,000 біт/с. Потім він починає вимірювати максимальну та середню швидкість передачі даних, дозволену специфікацією потоку, визначеною для трафіку, призначеного для використання червоного кольору LSP. Саме тоді значення починає зростати до 0,0125 секунди в кінці часу моделювання. Іншою цікавою деталлю є невелике зменшення затримки в черзі кожну секунду протягом часу моделювання. Це падіння пов’язане з часом, коли інтенсивність трафіку збільшується на 300,000 біт/с. Це може бути проблемою реалізації інструменту моделювання програмного забезпечення.

Ще одним отриманим результатом був той факт, що майже всі значні черги з’явилися між першими двома маршрутизаторами на обох шляхах. Після цього значення підтримували стабільні значення затримки в черзі між іншими маршрутизаторами шляху пересилання. Цьому явищу є просте пояснення. Через те що всі основні черги відбуваються між вхідним і першим маршрутизаторами шляху, а значення черги не дуже високі, отримуємо дуже стабільне значення черги між іншими маршрутизаторами шляху. Обсяг трафіку між цими маршрутизаторами більш передбачуваний, оскільки другий маршрутизатор уздовж шляху отримує ту кількість трафіку, яку він може перенаправляти ближче до певного пункту призначення. Це перший маршрутизатор, що ставить у чергу великий обсяг трафіку, який канали не можуть передати негайно.

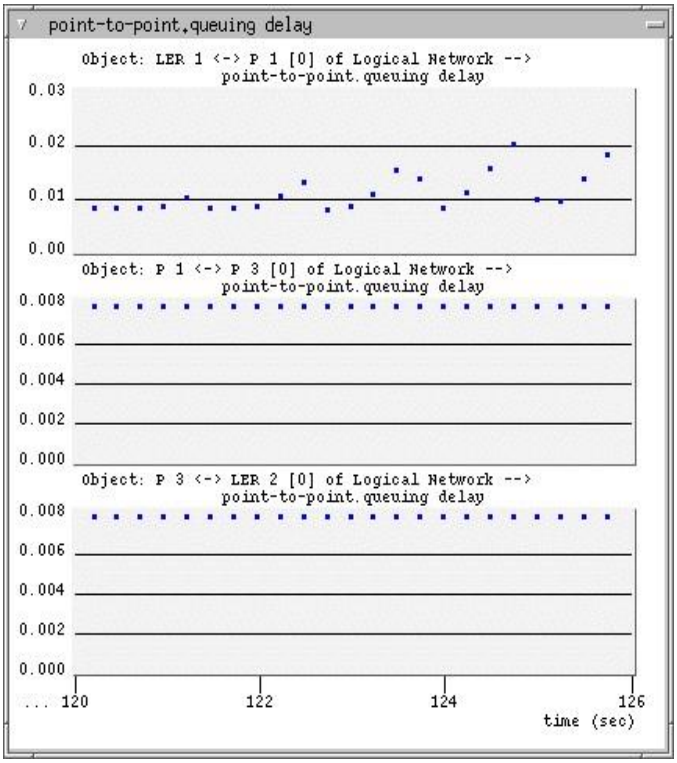

Рисунок 3.15 – Затримки в черзі шляху LER1-P1-P3-LER2

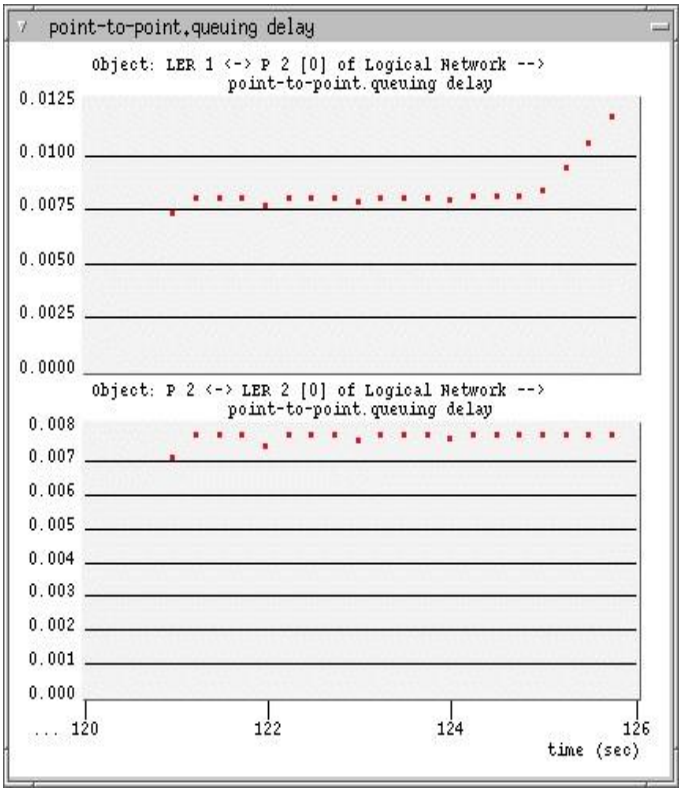

Рисунок 3.16 - Затримки в черзі шляху LER1-P2-LER2

Мета експеременту полягала не в глибокому дослідженні характеристик TCP і UDP, а в дослідженні величини збільшення продуктивності в мережі з TE у порівнянні з простою мережею з найкоротшим шляхом. Порівнюючи ці результати з попередніми результатами з налаштованої мережі маршрутизації за найкоротшим шляхом, затримка в черзі отримує набагато менше значення затримки в черзі між вхідним маршрутизатором і першим маршрутизатором уздовж найкоротшого шляху, ніж сценарій маршрутизації за найкоротшим шляхом.

3.3.3 Висновок по експерименту

Експеримент та його аналіз розкриває характеристики продуктивності MPLS-трафіку. Використовуючи технологію MPLS-TE можно досягти підвищення продуктивності з точки зору затримки в черзі, пропускної здатності та використання

шляху. Завдяки цьому можно підтвердити можливість використовування технології для подолання недоліків протоколів маршрутизації за найкоротшим шляхом та використанням його в мережах наступного покоління.

Значення пропускної здатністі були зареєстровані як прийнятні для трафіку TCP у сценарії MPLS-TE. Трафіку TCP не потрібно було знижувати інтенсивність трафіку, оскільки він не конкурував з трафіком UDP за мережеві ресурси. Виміряно пропускну здатність TCP-трафіку між вихідним і вхідним маршрутизаторами та маршрутизаторами між ними. Можно було спостерігали деяке падіння пропускної здатності TCP між відправником і вхідним маршрутизатором. Дано тлумачення цих падінь. Було вирішено, що причиною зареєстрованого результату пропускної спроможності може бути два фактори разом. Тим не менш, зареєстровану пропускну здатність можно оцінювати позитивно для трафіку TCP, знаючи, що якби інжиніринг трафіку не було реалізовано, трафік TCP постраждав би від конкуренції з трафіком UDP за ті самі ресурси найкоротшого шляху. Поліпшення також було показано у випадку використання шляху. Висновки показують, що за допомогою проектування трафіку можна досягти більш ефективного використання мережевих ресурсів. Змодельована топологія мережі не представляє мережу постачальника послуг, але вона чітко показує, які можливості може надати MLPS-TE, коли справа доходить до більш ефективного використання мережевих ресурсів. Постачальники послуг можуть організовувати певні потоки трафіку за допомогою місцевої адміністративної політики, щоб ефективніше використовувати свої ресурси.

Що стосується затримки в черзі, зареєстровано менший час затримки, оскільки потоки використовували обидва шляхи, доступні між вхідним і вихідним маршрутизаторами. Таким чином, досягається більш збалансована інтенсивність трафіку між шляхами, доступними до вихідного маршрутизатора. Проте було виявлено, що навіть якщо для трафіку UDP і TCP використовуються два різні шляхи, збільшення інтенсивності трафіку UDP мало деякий вплив на затримку черги та пропускну здатність трафіку TCP. Вимірювання показали, що навіть з механізмом TE, деяке погіршення

продуктивності TCP-трафіку мало місце щоразу, коли UDP-трафік виконує певні дії. Проте виявленно, що значення черги, зареєстровані для обох типів трафіку, продемонстрували приріст продуктивності порівняно зі сценарієм найкоротшого шляху.

3.4 Імітаційний експеримент використанням MPLS-TE і Diffserv

Після експерименту із симуляцією з використанням лиже управління трафіком перейдемо до моделювання мережі з управлінням трафіком та підтримкою якості обслуговування. Метою цього моделювання було керуванням потоками трафіку та підтримувати QoS за допомогою диференційованих служб. Тут передача трафіку, описаного раніше, організована через один LSP. Призначивши згенерований трафік різним CoS, буде можливість виміряти проблеми з продуктивністю, спричинені MPLS-TE та diffserv.

3.4.1 Конфінурація MPLS-TE та підтримка QoS

На Рисунку 3.17 зображено модель мережі MPLS-TE із підтримкою QoS. Тут використовується попередня топологія мережі, з єдиною відмінністю, що був використаний лише один з налаштованих раніше LSP. Синьою стрілкою позначено LSP, налаштований на використання обома згенерованими трафіками з різними CoS.

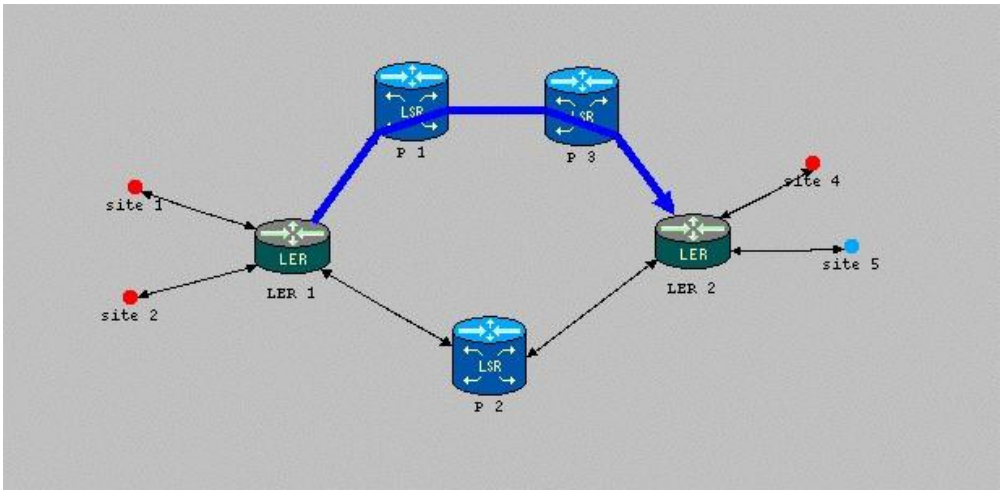

Рисунок 3.17 – Модель мережі MPLS QoS

У цій експериментальній мережі були внесені деякі зміни, щоб забезпечити мережеве середовище інжирингу трафіку з підтримкою QoS. LSP повинен обробляти дві специфікації потоку, керовані вхідним маршрутизатором. Таблиця 3.4 нижче описує ці дві окремі частини специфікації потоку; TSpec і RSpec. EF_flowspec для трафіку, що входить до синього LSP, і його характеристик трафіку (Tspec) було налаштовано з максимальною швидкістю передачі даних 1,544,000 біт/с, середньою швидкістю передачі даних 1,000,000 біт/с та максимальним розміром пакету 64,000 біт/с, а його RSpec був службою EF класу. Інша специфікація потоку, якою керував вхідний маршрутизатор, була AF11_flowspec. Характеристика трафіку цієї специфікації потоку (TSpec) була налаштована з максимальною швидкістю передачі даних 1,544,000 біт/с, середньою швидкістю передачі даних 500,000 біт/с та максимальним розміром пакету 64,000 біт/с, а її RSpec був класом обслуговування AF11. EF_flowspec було налаштовано, щоб піклуватися про трафік EF CoS і відхиляти трафік будь який інший трафік окрім трафіку цього конкретного типу, який надходить у LSP. Іншу специфікацію потоку, AF11_flowspec, було налаштовано для піклування за трафіком AF11 CoS і відхиленням будь-якого іншого трафіку, крім трафіку цього конкретного типу, який надходить у LSP. Таблиця 3.4 підсумовує таблицю конфігурації специфікації трафіку.

Таблиця 3.4 – Конфігурація спеціалізації потоку

Потоки	Максимальна швидкість передачі даних (біт/с)	Середня швидкість передачі даних (біт/с)	Макс. Розмір пакету (біт)	Дії поза профілем	Клас трафіку
EF_flowspec	1,544,000	1,000,000	64,000	Відкинути	EF
AF11_flowspec	1,544,000	500,000	64,000	Відкинути	AF11

Один клас FEC було надано одному типу потоку, у нашому випадку TCP-трафіку з EF CoS, а інший клас FEC було надано другому типу трафіку UDP-трафіку з AF11 CoS. Оскільки налаштовані потоки трафіку, надходять до мережі зліва направо, тобто site1 і site2 генерують трафік до site4 і site5 то інтерфейси LER1 потрібно було налаштувати правильно. LER1 потрібно було налаштувати для призначення FEC на основі інтерфейсу, який обробляв вхідний трафік, а також іншої інформації, з заголовку вхідного пакету. У нашому випадку FEC було призначено на основі керуючих правил, наведених у таблиці 3.5.

Таблиця 3.5 – Специфікація FEC

Назва FEC	DSCP	Використаний протокол	Адреса призначення
Site1	EF	TCP	192.0.13.2 (Site5)
Site2	AF11	UDP	192.0.11.2 (Site4)

На вхідному маршрутизаторі LER1 пакети класифікуються та призначаються до відповідного класу FEC. Потім FEC було зіставлено на правий трак трафіку, що використовує певний LSP. Таким чином, вхідний трафік був скерований на основі адміністративного правила. Оскільки метою було виміряти обробку цих двох потоків трафіку з різними вимогами QoS, MPLS-TE тепер було налаштовано для використання

архітектури QoS диференційованих послуг. Було використано Weighted Fair Queuing (WFQ) diffserv у поєднанні з відображенням коду DSCP, щоб керувати вимогами QoS для потоків. Більше значення WFQ було надано трафіку EF CoS порівняно з трафіком AF11 CoS. Трафік EF CoS отримав значення ваги 55 і можливість використовувати чергу з низькою затримкою, тоді як трафік CoS AF11 мав значення ваги 5, налаштоване для використання черги за замовчуванням. Щоб виміряти продуктивність цієї конфігурації, були зібрані дані про затримку WFQ, використання буфера WFQ, пропускну здатність потоку та затримку потоку, виміряні для обох потоків трафіку.

3.4.2 Затримка WFQ і використання буфера

Було зібрано статистичні дані щодо затримки Weighted Fair Queuing з виходу інтерфейсу вхідного маршрутизатора. Завдання полягало в дослідженні, скільки часу трафік знаходиться у черзі AF11 CoS з трафіком EF CoS. Результати показані на малюнку 7.1, де трафік EF CoS досяг затримки WFQ нижче 0,025 секунди. Реєструючи його нестабільні значення, він все ще зберігав набагато нижчі значення, навіть з його тимчасовими значеннями. З іншого боку, трафік AF11 CoS мав загальне нерегулярне, але вище значення. Він досягає дуже розріджених значень затримки WFQ протягом часу моделювання. З найвищим одноразово зареєстрованим значенням, що становить приблизно 0,125 секунди, він має загальні вищі розріджені значення, ніж трафік EF CoS. Це очікуваний результат, оскільки точка коду диференційованих послуг AF11 була налаштована з нижчим значенням пріоритету, ніж її конкурент.

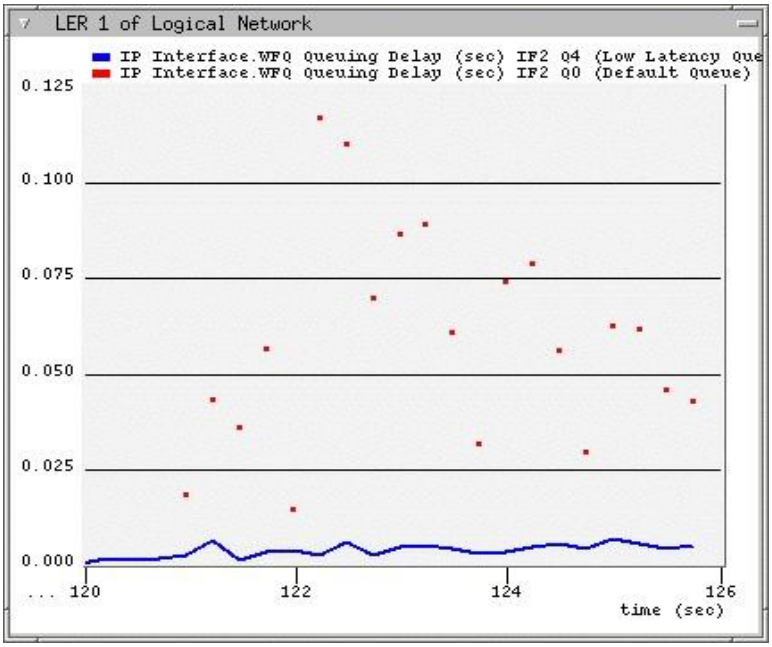

Рисунок 3.18 – WQF затримка на вихідному інтерфейсі LER1

На рисунку 3.19 показано використання буфера WFQ двома описаними типами потоків. Графік синього кольору відображає трафік EF CoS, а червоний – трафік AF11 CoS. Синій графік показує, що пакети EF CoS досягають бажаного часу затримки в черзі. Тут пакети EF CoS мають використовувати чергу з низькою затримкою на маршрутизаторі, тоді як пакети AF11 CoS мають використовувати чергу за замовчуванням. Черга з низькою затримкою налаштована на обробку перед будь-якою іншою чергою. Це означає, що будь-які пакети, які знаходяться в цій черзі з низькою затримкою, повинні бути оброблені першими та переслані перед пакетами, які знаходяться в черзі за замовчуванням. Таким чином, з наведеного вище рисунка можна бачити, що не більше одного пакета EF CoS знаходилося в черзі до обробки. Зворотня сторона цього ефекту впливає на пакети AF11 CoS, які досягають значення від одного до шести пакетів у черзі на вхідному маршрутизаторі.

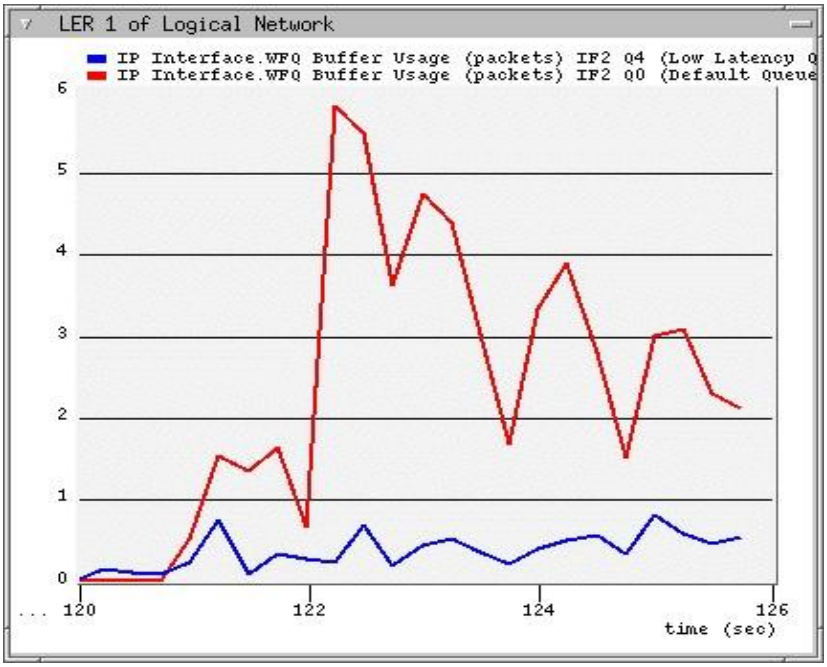

Рисунок 3.19 – WQF використання буфера на вихідному інтерфейсі LER1

3.4.3 Затримка потоку

Значення затримки потоку описують величину затримки, накладеної на потоки, які передаються через налаштований LSP. На рисунку 3.20 показані результати вимірювань затримки потоку, отримані в результаті моделювання. Кожен потік, що проходить через LSP, отримав певну затримку. Ця затримка сталася через підтримку QoS, яка надавалася кожному потоку, який проектується. Оскільки для трафіку AF11 CoS було надано нижчу підтримку QoS, йому було накладено більше значення затримки потоку, ніж для трафіку EF CoS. EF CoS мав майже стабільне значення затримки 0,025 секунди. Трафік AF11 CoS зберіг загальне вище значення затримки потоку. Графік показує, що важче досягти стабільного значення затримки потоку з AF11 CoS, оскільки цей тип трафіку використовує чергу за замовчуванням на маршрутизаторах. Однак для інших типів черг можна налаштувати більш точну та розраховану політику черг.

Ці значення були певним чином очікувані з результатів, інтерпретованих раніше. Вплив опції WFQ диференційованих послуг накладає кращу підтримку QoS для трафіку

EF CoS, таким чином досягаючи кращої затримки потоку для цього класу трафіку послуг. AF11 CoS не чутливий до затримки, як трафік EF CoS, тому залишається та витрачає більше часу в черзі. Таким чином, ці результати відповідали очікуваним результатам за допомогою WFQ, реалізованого в цій змодельованій мережі.

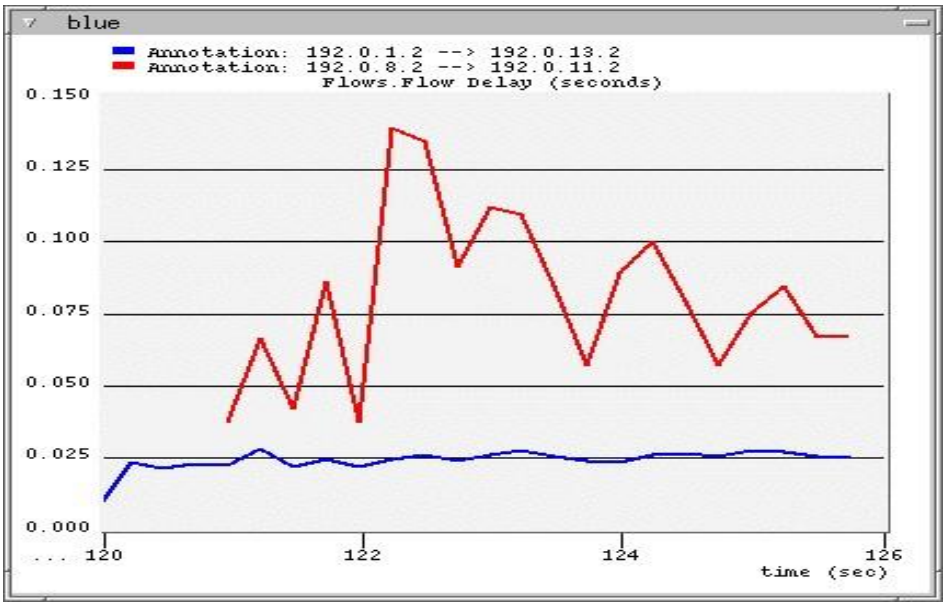

Рисунок 3.20 – затримки черги на синьому LSP

3.4.4 Пропускна здатність

Ще одним результатом, пов’язаним з QoS, отриманим у ході експерименту MPLS-TE, були пропускна здатність, виміряна від обсягу вхідного трафіку і вихідного трафіку LSP. EF_flowspec було дозволено справлятися із середньою швидкістю передачі даних 1,000,000 біт/с. AF11_flowspec мала справлятися із середньою швидкістю передачі даних 500,000 біт/с. Ці суми дорівнювали значенню 1,500,000 біт/с, що є майже максимальною пропускною здатністю кожного з'єднаня на шляху. Обидві характеристики потоку було налаштовано з максимальною швидкістю передачі даних 1,544,000 біт/с і значенням максимального розміру пакету 64,000 біт/с.

На рисунках 3.21 та 3.22 нижче показані результати, отримані в результаті моделювання. Було зафіксовано, що пропускна здатність вхідного трафіку була майже точно такою ж як і пропускна рздатність на виході з LSP. Налаштування дозволяють проходити через LSP лише фіксованому обсягу трафіку. Попередні вимірювання черги, описані раніше, показали, що не весь трафік, надісланий на вхідний маршрутизатор, міг негайно потрапити в LSP. Вхідному маршрутизатору вдається поставити в чергу великий обсяг переданого йому трафіку завдяки пропускній здатності каналу та LSP із відповідним обмеженням пропускної здатності. Вхідний маршрутизатор передає лише ту кількість трафіку, на обробку якої налаштовано LSP. На рисунку 3.21 показано, що трафік EF CoS, який представлений синім кольором, має приблизну середню швидкість передачі даних 1,000,000 біт/с. У той час як трафік AF11 CoS, який представлений червоним кольором, має приблизну середню швидкість передачі даних 500,000 біт/с. Ці значення швидкості потоку мають місце через обмеження середньої швидкості передачі, налаштоване специфікаціями потоку. Однак було зареєстровано кілька перехідних значень, які вказували на те, що маршрутизатор не міг точно обчислити обмеження середньої швидкості передачі, встановлених специфікаціями потоку. Перше зниження інтенсивності трафіку через трафік TCP EF CoS відбувається в той самий час, коли трафік UDP перевищує межу середньої швидкості передачі даних, яка регулюється AF_flowspec. Це вказує на те, що UDP трохи впливає на трафік TCP, коли обидва потоки починають передаватися через один і той же LSP з різними CoS. Здається, що для вхідного маршрутизатора легше підтримувати середнє значення швидкості потоку, що регулюється специфікаціями потоку, коли мова йде про трафік UDP, ніж трафік TCP. Трафік UDP зберігає більш стабільне значення навколо середньої швидкості потоку в 500,000 біт/с.

На рисунку 3.22 показано кількість трафіку, який виходить із магістралі. Порівнюючи обидві цифри можно бачити, що вони майже однакові. Це вказує, що обсяг трафіку, що прямує до та з LSP, був приблизно рівним. На рисунку також показано, що пропускна здатність EF CoS зберігає вищу середню швидкість передачі даних порівняно

з трафіком AF11 CoS. Це відбувається через те, що специфікація потоку трафіку EF CoS повинна була використовувати вищий ліміт пропускної спроможності. Загальна картина вказує на те, що за допомогою специфікацій потоку можна керувати потоками з різною CoS, щоб не використовувати надмірно мережеві ресурси, і в той же час отримати різну якість обслуговування.

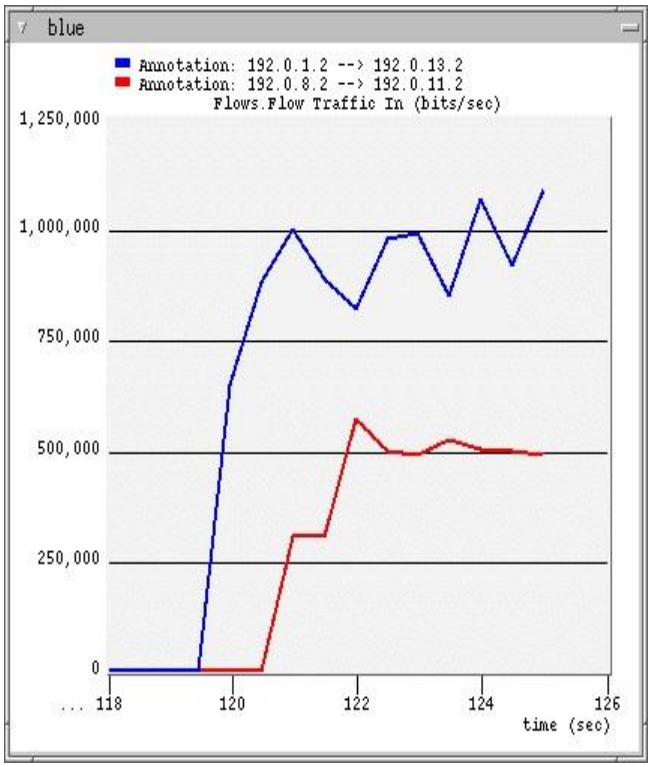

Рисунок 3.21 – Вхідний трафік LSP

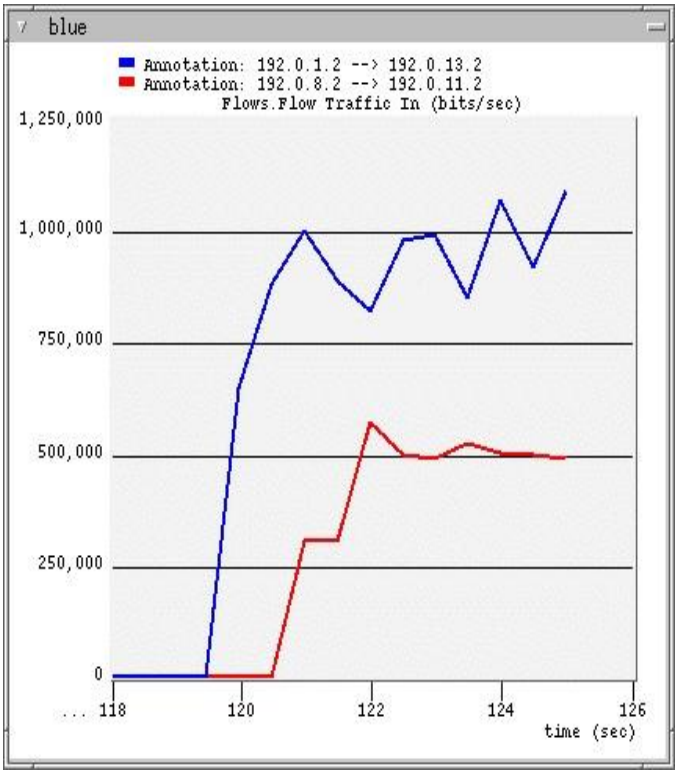

Рисунок 3.22 – Вихідний трафік LSP

3.5 Висновки до розділу 3

Експеримент та аналіз MPLS-TE у поєднанні з диференційованими службами WFQ розкривають можливості підвищення продуктивності, досягнуті, використанням інжирінгу трафіку з різними вимогами QoS. У поєднанні ці дві архітектури пропонують повний контроль трафіку та підтримку QoS. MPLS-TE керує обсягом трафіку, накладеного на ресурси мережі, і контролює шлях, яким інший тип трафіку має йти до місця призначення. У той час як зважена справедлива черга за допомогою диференційованих послуг DSCP регулює вимоги QoS до потоків.

Результати, отримані під час моделювання, показують, що трафіку CoS з вищим пріоритетом вдалося отримати кращу якість обслуговування від ресурсів на своєму шляху. Трафік EF CoS досяг меншого часу затримки потоку, ніж трафік AF11 CoS. Це пов’язано з тим, що трафік AF11 CoS не був чутливим до затримки, як трафік його конкурента EF CoS. Він також використовував чергу з низькою затримкою, а не чергу за

замовчуванням, у яку примусово потрапляли пакети AF11 CoS. Цю чергу з низькою затримкою було налаштовано на обробку перед будь-якою іншлю чергою. Таким чином, було зареєстровано не більше одного пакета EF CoS, який знаходиться в цій черзі в будь-який час під час моделювання. Оскільки було використано Weighted Fair Queuing для керування якістю обслуговування пакетів, вищий пріоритет, вага надавалася трафіку EF CoS на маршрутизаторах. Пакетам із диференційованими кодовими точками служби EF надано вищу вагу, що призводить до меншого часу затримки у чергах. Значення затримки WFQ і використання буфера WFQ були нижчими для трафіку EF CoS, що вказує на те, що час, проведений пакетами EF CoS у чергах на маршрутизаторах, був меншим, ніж пакетах AF11. Менше часу в чергах допомагає швидше дістатися до кінцевого пункту призначення. Це дає змогу швидше розпізнавати пакети підтвердження, щоб відправник підтримував високу інтенсивність трафіку. Таким чином, передавач EF CoS забезпечує високу пропускну здатність. Проте було зафіксовано певний прямий вплив трафіку AF11 CoS UDP на трафік TCP EF CoS. Вплив був не таким сильним, як якщо б вони збиралися конкурувати один з одним за ті самі мережеві ресурси, як було змодельовано раніше.

Обсяг трафіку, переданого мережею, регулювався специфікаціями flowspec для потоків, створених через LSP. Таким чином, трафік не міг потрапити в основну мережу більше, ніж дозволено. Завдяки керуванню трафіком трафіку через LSP вдалося контролювати пропускну здатність інтенсивності трафіку в межах домену MPLS, водночас підтримуючи якість обслуговування трафіку, що пересилається за допомогою диференційованих служб.

ВИСНОВКИ

Серед багатьох проблем, з якими стикається NGN, є питання якості обслуговування (QoS), як і в будь-якій мережі на основі IP; яка вимірюється з точки зору затримки мережі, пропускної здатності, зміни затримки пакетів, втрати пакетів тощо.У диссертації було змодельвано три експериментальні мережі. Проводилися експеременти з маршрутизацією за найкоротшим шляхом, інженерією трафіку MPLS та інженерією трафіку MPLS у поєднанні з диференційованими послугами для підтримки QoS. Метою ставилося аналіз механізмів управління трафіком технології багатопротокольної комутації по мітках задля їх використання у використання при впроваджені мереж наступного покоління

Принцип маршрутизації найкоротшого шляху базується на маршрутизації трафіку найкоротшим відомим шляхом до будь-якого пункту призначення. Під час пересилання трафіку протокол маршрутизації не повинен враховувати інші ненайкоротші шляхи, які не використовуються. Коли декілька джерел використовують один і той самий найкоротший шлях, цей шлях може стати перевантаженим. Перевантаження може виникнути на якомусь вхідному маршрутизаторі, який обробляє весь трафік, спрямований до певного пункту призначення за межами одного вихідного маршрутизатора. Завдяки такому підходу, запровадженому протоколом маршрутизації, важко уникнути неефективного використання мережевих ресурсів. Ненайкоротші шляхи часом будуть використовуватися недостатньо, тоді як найкоротший шлях використовуватиметься надмірно.

Для висвітлення згаданих недоліків, було змоделювано мережу з налаштованим протоколом маршрутизації за найкоротшим шляхом OSPF. Цей протокол в основному призначений для маршрутизації трафіку, використовуючи лише найкоротший шлях для пересилання трафіку через мережу. Він розраховує маршрути на основі стану з’єднання на маршрутизаторах і розраховує мінімальну вартість або показник до будь-якого відомого пункту призначення. За допомогою моделювання було виміряно проблеми з

продуктивністю, пов’язані із затримкою в черзі, пропускною спроможністю та використанням зв’язку. Результати були досить поганими, через що трафік страждав від недоліків протоколу маршрутизації. Було зафіксовано, що протокол маршрутизації без мети обробляв трафік UDP краще, ніж трафік TCP в умовах високого навантаження. Це сталося тому, що TCP має механізм керування потоком і відчуває появу перевантаження, змушуючи його зменшувати інтенсивність трафіку. Незважаючи на те, що обидва типи трафіку були налаштовані з рівним найкращим класом обслуговування, UDP-трафік отримав кращу обробку продуктивності в мережі, налаштованій за найкоротшим шляхом. Було виміряно їхню затримку в черзі, пропускну здатність і використання каналу. Завдяки цим результатам можно бачити, що найкоротший шлях за умови великого навантаження використовувався надмірно, і продуктивність, зареєстрована для обох типів трафіку показує, що протокол маршрутизації найкоротшого шляху не забезпечив їм хорошої продуктивності. Варто зазначити, що TCP-трафік найбільше постраждав порівняно з UDP-трафіком у всіх виміряних проблемах продуктивності. Ці негативні зареєстровані результати були пов’язані з тим, що весь трафік направлявся найкоротшим шляхом між вхідним і вихідним маршрутизаторами. Ненайкоротший шлях залишився невикористаним. На жаль, навіть якщо вдалося досягти кращої продуктивності за допомогою ненайкоротшого шляху, коли найкоротший шлях перебуває під великим навантаженням, протокол маршрутизації продовжував пересилати трафік найкоротшим шляхом.

Існують способи керування трафіком в мережах IP, щоб впоратися з проблемою балансування навантаження протоколів маршрутизації за найкоротшим шляхом. Спосіб керування трафіком полягає в маніпулюванні показниками каналу, наприклад OSPF. Але цей механізм потенційно призводить до кількох проблем. По-перше, зміна метрики каналу може призвести до зміни шляху всіх пакетів, що проходять через канал. По-друге, це не створює місця для динамічного резервування та не враховує характеристики пропонованого трафіку та обмеження пропускної здатності мережі під час прийняття рішень щодо маршрутизації.

Керування трафіком з використанням IGP в великих мережах є досить складним з наступних причин:

1. Між Equal-Cost Multi-Path (ECMP) від джерела кожен шлях матиме рівну частку навантаження. Це рівне співвідношення не можна змінити. Таким чином, один із шляхів може передавати значно більше трафіку, ніж інші шляхи, оскільки він також переносить трафік з інших джерел.

2. Розподіл навантаження між декількома шляхами з різною вартістю неможливий без значного адміністрування та ручного керування метриками каналів.

Для подолання недоліків управління трафіком протоколу маршрутизації найкоротшого шляху було використано багатопротокольну комутацію по мітках.

MPLS — це вдосконалена схема переадресації. Вона розширює маршрутизацію щодо пересилання пакетів і контролю шляху. Управління трафіком MPLS дозволяючи будь-якому шляху з комутацією міток (LSP) динамічно переключатися з перевантаженого шляху на альтернативний шлях. Це дозволяє постачальникам Інтернет-послуг працювати зі своєю мережею з набагато більшою пропускною здатністю за звичайних обставин, знаючи, що коли ось-ось відбудеться перевантаження, мережа шукатиме альтернативи, щоб уникнути перевантаження. Це також замінює необхідність ручного налаштування мережевих пристроїв для встановлення явних маршрутів.

Для експеременту було вирішино використовувати статичний варіант встановлення MPLS LSP. Це означає, що два різні типи трафіку, з якими експериментували в попередньому експерименті з маршрутизації найкоротшого шляху, були розподілені на їхні окремі шляхи. Було зроблено так, щоб потік TCP використовував не найкоротший шлях, дозволивши трафіку UDP використовувати ресурси найкоротшого шляху. Після чого порівняли отримані результати з експериментом з маршрутизації найкоротшого шляху, порівнюючи затримку в черзі, пропускну здатність і використання каналу. Зафіксовано, що обидва типи трафіку підвищили ефективність, коли трафік був скероаний різними шляхами до місця

призначення. Це змусило потік TCP підтримувати інтенсивність трафіку без пригнічення з боку трафіку UDP. Проте було зареєстровано деяке зниження інтенсивності трафіку з пропускною здатністю TCP від передавача до вхідного маршрутизатора. В цьому винен не протокол MPLS-TE та його поведінка, а вхідний маршрутизатор що став більш зайнятим, пересилаючи більше пакетів. Крім того, у випадку ефективного використання ресурсів результати були набагато більш задовільними. Тепер використовуються обидва шляхи між вхідним і вихідним маршрутизаторами порівняно зі сценарієм маршрутизації найкоротшого шляху. Це підтверджує, що з кількома шляхами, доступними між будь-якою парою вхідних і вихідних маршрутизаторів, управління трафіку може здійснюватися за допомогою MPLS, щоб уникнути перевантаження в мережі. Це також допомагає ефективніше використовувати мережеві ресурси, використовуючи шляхи, відмінні від найкоротшого. Мережа, використана під час експерименту, була невеликою та простою мережею, але вона могла представляти будь-яку частину будь-якої автономної системи.

З проведених експериментів можно бачити до MPLS-TE може використовуватися, задля контролювалю над трафіком для використання бажаних шляхів через мережу. Завдяки цьому контролю він може розраховувати на надання клієнту більш точної угоди про рівень обслуговування та мінімізацію вартості надання послуг, особливо витрат на використання дорогих мережевих ресурсів.

Метою різноманітних зусиль якості обслуговування Інтернету (QoS) є розширення цієї базової служби за допомогою ряду вибраних відповідей служби. Ці відповіді служби можна відрізнити від сервісу найкращих зусиль певною формою вищого рівня сервісу або вони можуть відрізнятися наданням передбачуваного відгуку сервісу, на який не впливають зовнішні умови, такі як кількість одночасних потоків трафіку.

Будь-яка відповідь мережевої служби є результатом ресурсів, доступних для обслуговування навантаження, і рівня самого навантаження. Щоб запропонувати такі відмінні послуги, існує не тільки вимога щодо надання диференційованої відповіді на послугу в межах мережі, але також є вимога контролювати кваліфіковане навантаження

в мережі, щоб ресурси, виділені мережею для підтримки відповіді конкретної служби здатні були забезпечити таку реакцію на отримане навантаження. Як загальне спостереження за архітектурами QoS, аспект керування навантаженням служби QoS є, мабуть, найбільш тривожним компонентом архітектури. Хоча існує широкий спектр добре зрозумілих механізмів реагування на обслуговування, які доступні для IP-мереж, зіставлення набору таких механізмів у контрольованому середовищі для відповіді на набір навантажень сервісу для досягнення повністю узгодженої відповіді на обслуговування залишається слабкою стороною всередині існуючі архітектури IP QoS.

Саме тут технологія MPLS поєднується з диференційованими послугами, щоб запропонувати такий контроль. MPLS вказує маршрут для потока та вказує на наступний стрибок, тоді як диференційовані служби визначають обробку пакета, який очікує на наступний стрибок. Таким чином, MPLS може контролювати обсяг трафіку, накладеного на маршрутизатор завдяки його можливостям резервування транків трафіку і, не пропускаючи більше трафіку в межах кожного транку, оскільки передбачається, що в мережі є ресурси для обробки навантаження трафіку.

У останній експериментальній мережі були використані позитивні результатам проектування трафіку MPLS, щоб поєднати його з архітектурними можливостями QoS диференційованого обслуговування. Цього разу метою було забезпечити QoS для потоків трафіку, які вимагали певного рівня QoS одночасно, оскільки трафік організовувався через LSP. Дві специфікації потоку мали піклуватися про трафік EF CoS і трафік AF11 CoS. Вдалося налаштувати мережу MPLS-TE на співпрацю з чергою за вагою diffserv для адміністрування аспекту QoS мережі. Призначивши більшу вагу трафіку EF CoS, з’ясовано, як оброблялися різні потоки CoS під час їх проектування. Зареєстровані вимірювання показали, що величина затримки в черзі, використання буфера в черзі, затримка потоку та пропускна здатність цих різних потоків трафіку CoS відрізнялися на користь вищого трафіку CoS. Потік з вищим пріоритетом отримав у всіх вимірюваннях кращу підтримку QoS порівняно з потоком CoS з нижчим значенням. Крім того, якщо подальші потоки трафіку з тією самою CoS будуть накладені на вхідний

маршрутизатор, додаткові транки не будуть потрібні. Трафік з однаковою CoS буде агрегований, щоб використовувати ту саму магістраль трафіку CoS.

Можно зробити висновок, що MPLS-TE та архітектура диференційованих послуг у поєднанні є корисним інструментом для виконання проектування трафіку з підтримкою якості обслуговування. Що дозволяє постачальнику послуг контролювати шлях, який буде використовувати потік, плюс обсяг трафіку, передаваємого в мережу, і в той же час забезпечити йому необхідний рівень якості.

Як вже згадувалося для реалізації мереж наступного покоління необхідна транспортна технологія здатна керувати трафіком різнотипних мереж та забезпечувати якість обслуговування послуг, що надаються цими мережами. З отриманих екперементальних результатів можно зробити висновок о перевагах використання комбінації механізму керування трафіком технології багатопротокольної комутації по мітках та диференційованих послуг, що дозволяє отримати більше контролю над трафіком програм у мережі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Телекомунікаційні системи та мережі наступного покоління: конспект лекцій. Модуль 5.2 / Педяш В.В. – Одеса: ОНАЗ ім. О.С. Попова, 2017. – 76 с.
2. Голиков А.М. Транспортные и мультисервисные системы и сети связи: Учебное пособие. Часть1. – Томск: Томск. гос. ун-т систем управления и радиоэлектроники, 2015. – 83 с.
3. Лекции Сетевые технологии: Сети связи следующего поколения - НОУ ИНТУИТ
4. Гольдштейн, А. Б. Г63 Транспортные сети IP/MPLS. Технология и протоколы: у чебное пособие / А. Б. Гольдштейн, А. В. Никитин, А. А. Шкрыль ; СПбГУТ. – СПб., 2016. – 80 с.
5. Гольдштейн А.Б. Механизм эффективного туннелирования в сети MPLS, Журнал «Вестник связи» №2, 2004
6. Гольдштейн А.Б., Протоколы ускоренной маршрутизации. Технология маршрутизации по меткам MPLS – Санкт - Петербург, 2006.
7. Б.С Гольштейн, Н.А. Соколов, Г.Г. Яновский, “Сети Связи”, БВХ-Петербург, 2007.
8. Simha A., Osborne E. Traffic Engineering with MPLS. Cisco Press, 2002. – 675c.
9. MPLS AND NEXT-GENERATION NETWORKS FOUNDATIONS FOR NGN AND ENTERPRISE VIRTUALIZATION Monique Morrow and Azhar Sayeed Cisco Press 2007 – 421 c.
10. Imran Ikram “Traffic Engineering with MPLS and QOS” School of Engineering Blekinge Institute of Technology 2009 - 96c.
11. Multimedia Traffic Analysis of MPLS and Non MPLS Network Mahesh Kr. Porwal,Anjulata Yadav, S. V. Charhate International Journal Of Computer Science And Applications Vol. 1, No. 2, August 2008

12. ADVANCED FEATURES OF MPLS TECHNOLOGY BC. AUTHOR MARTIN VLÈEK BRNO 2009 – 90 c.
13. D. Awduche, A. Hannan, X. Xiao, “Applicability Statement for Extensions to RSVP for LSP-Tunnels”, RFC 3210, December 2001.
14. F. Le Faucheur “Protocol extensios for support of Diffserv-aware MPLS Traffic engineering”, RFC 4124, June 2005.
15. L.Wu, B. Davie, S. Davari, P. Vaananen “Multiprotocol Label Switching (MPLS) Support of Differentiated Servises” May 2002.
16. D.Awduche, J. Malcolm, J. Agogbua, M. O`Dell “Requirements for Traffic Enginering Over MPLS”, RFC 2702, September 1999.
17. “MPLS DiffServ-aware Traffic Engineering” Ina Minei, Juniper Networks, Inc.
18. E. Rosen, A. Viswanathan, R. Callon. “Multiprotocol Label Switching Architecture”, RFC 3031, January 2001.
19. Навчальний посібник для самостійної роботи з дисципліни “ТЕЛЕКОМУНІКАЦІЙНІ СИСТЕМИ ТА МЕРЕЖІ НАСТУПНОГО ПОКОЛІННЯ”, Заїка В.Ф., Варфоломеєва О.Г., Домрачева К.О., Гринкевич Г.О.,Київ – 2019.
20. L. Anderson, I. Minei, B. Thomas, “LDP Specification”, RFC 5036, October 2007.
21. Osagie Ighodalo Solomon, Ighagbon Oziegbe, “IP Routing for Next Generation Network Services” , Blekinge Institute of Technology June 2007.
22. Макаренко С. И., Чаленко Н. Н., Крылов А. Г.Сети следующего поколения NGN Systems of Control, Communication and Security 2016 – 22с.