Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Навчально-науковий центр заочної форми навчання
(повна назва)

Кафедра *Інформаційно-мережної інженерії*
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти другий (магістерський)

Аналіз механізмів забезпечення постійної працездатності мереж GMPLS
(тема)

Виконав:

студент *2* курсу, групи *ІМІзм-21-2*

Курятніков П.І.
(прізвище, ініціали)

Спеціальність *172 «Телекомунікації та радіотехніка»*
(код і повна назва спеціальності)

Тип програми *освітньо-наукова*
(освітньо-професійна або освітньо-наукова)

Освітня програма

«Інформаційно-мережна інженерія»
(повна назва освітньої програми)

Керівник *доц. Колтун Ю.М.*
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ *Безрук В.М.*
(підпис) (прізвище, ініціали)

2023 р.

Не містить відомостей заборонених до відкритого публікування.

Студент / *Курятніков П.І.* /

Керівник / *Колтун Ю.М.* /

Харківський національний університет радіоелектроніки

Навчально-науковий центр заочної форми навчання

Кафедра *Інформаційно-мережної інженерії*
(повна назва)

Рівень вищої освіти другий (магістерський)

Спеціальність *172 «Телекомунікації та радіотехніка»*
(код і повна назва)

Тип програми *освітньо-наукова*
(освітньо-професійна або освітньо-наукова)

Освітня програма *«Інформаційно-мережна інженерія»*
(повна назва)

ЗАТВЕРДЖУЮ:

Зав. кафедри _____
(підпис)

«*24*» *березня* 2023 р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

студентові *Курятнікову Павлу Ігоровичу*
(прізвище, ім'я, по батькові)

1. Тема роботи *Аналіз механізмів забезпечення постійної працездатності мереж GMPLS*

затверджена наказом університету від «*24*» *березня* 2023 р. № 59 *Стз*

2. Термін подання студентом роботи до екзаменаційної комісії *19 травня 2023 р.*

3. Вихідні дані до роботи *Базова фізична мережа переносу даних - ASON. Технологія мережної платформи ASON для передачі IP-трафіку – GMPLS. Мережна технологія ASON для імітаційного моделювання – Gigabit Ethernet.*

Проаналізувати особливості організації і принципи функціонування технології GMPLS з урахуванням архітектурної моделі і мережної структури ASON. Запропонувати і обґрунтувати механізми захисту та відновлення каналів і вузлів у мережах GMPLS в процесі розподілу трафіку. Дослідити взаємозв'язок захисних механізмів GMPLS з маршрутизацією із забезпеченням QoS у реальному масштабі часу. Зробити імітаційне моделювання маршрутизації трафіка в мережі GMPLS та запропоновати типовий розрахунок параметрів трафіку

4. Перелік питань, що потрібно опрацювати в роботі

Вступ

1. Загальний аналіз особливостей організації і принципів функціонування технологій MPLS і GMPLS.

2. Аналіз основних механізмів захисту та відновлення в мережах GMPLS.

3. Аналіз механізмів багаторівневого захисту GMPLS.

4. Імітаційне моделювання мережі GMPLS та типовий розрахунок параметрів трафіку.

Висновки

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (слайдів) *Слайди у форматі Power Point (назва, мета і етапи виконання кваліфікаційної роботи, спрощена структура домена мережі MPLS, принцип передачі пакета по мережі MPLS, таблиці LIB, що створюються маршрутизаторами MPLS у процесі передачі пакета, загальна структурна модель ASON, мережна архітектура транспортної ASON з використанням GMPLS, ієрархічна система міток і структура вкладених трактів в GMPLS, механізм захисту типу «місцеве відновлення», схема створення резервного LSP-з'єднання відповідно до механізму захисної комутації, механізм захисту за типом «швидкої перемаршрутизації», сценарії реалізації багаторівневого захисту у мережі GMPLS, організація багаторівневого захисту GMPLS, імітаційне моделювання мережі GMPLS, висновки)*

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Терміни виконання етапів роботи	Примітка
1	*Ознайомлення із завданням. Уточнення ТЗ.*	24.03 – 26.03.23	*виконано*
2	*Підбір літератури за темою роботи.*	27.03 – 03.04.23	*виконано*
3	*Виконання розділу 1*	04.04 – 14.04.23	*виконано*
4	*Виконання розділу 2*	15.04 – 22.04.23	*виконано*
5	*Виконання розділу 3*	23.04 – 01.04.23	*виконано*
6	*Виконання розділу 4*	02.05 – 13.05.23	*виконано*
7	*Оформлення пояснювальної записки*	14.05 – 18.05.23	*виконано*
8	*Оформлення презентаційного матеріалу,*		
	підготовка до захисту у ЕК	19.05 – 25.05.23	*виконано*

Дата видачі завдання *24 березня 2023 р.*

Студент _____
(підпис)

Керівник роботи _____ *доц. Колтун Ю.М.)*
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 78 с., 23 рис., 5 табл., 21 джерело, 3 додатки.

MPLS, GMPLS, MPλS, ASON, MPLS-TE, МІТКА, LSR, E-LSR, РОЗПОДІЛ ТРАФІКУ, ЗАХИСТ ТА ВІДНОВЛЕННЯ, МІСЦЕВЕ ВІДНОВЛЕННЯ, ЗАХИСНА КОМУТАЦІЯ; ШВИДКА ПЕРЕМАРШРУТИЗАЦІЯ, ШЛЯХ LSP, ТРАКТ LSP, БАГАТОРІВНЕВИЙ ЗАХИСТ, LSP-З'ЄДНАННЯ, МАРШРУТИЗАЦІЯ, QoS

Об'єкти дослідження – технологія GMPLS, архітектура ASON, механізми захисту та відновлення.

Мета роботи – аналіз основних механізмів захисту та відновлення, що надаються технологією GMPLS з метою забезпечення постійної працездатності та необхідної якості обслуговування в оптичних транспортних мережах типу ASON, які, у свою чергу, є базовою платформою для розгортання GMPLS.

Проведений аналіз широкого спектру механізмів, що застосовуються для захисту та відновлення комутованих LSP, таких як: місцеве відновлення, захисна комутація, швидка перемаршрутизація, багаторівневий захист. Для цих механізмів розглянуті різні практичні способи їх застосування на мережі із технологією GMPLS. Досліджений взаємозв'язок захисних механізмів GMPLS з маршрутизацією із забезпеченням QoS у реальному масштабі часу. Проведене імітаційне моделювання маршрутизації трафіка в мережі GMPLS та запропонований типовий розрахунок параметрів трафіку.

THE ABSTRACT

Explanatory note 78 pages, 23 fig., 5 tab., 21 sources, 3 app.

MPLS, GMPLS, MPλS, ASON, MPLS-TE, MITKA, LSR, E-LSR, TRAFFIC DISTRIBUTION, PROTECTION AND RECOVERY, LOCAL REPAIR, PROTECTION SWITCHING, FAST REROUTE, LSP PATH, LSP TRACK, MULTI-LEVEL PROTECTION, LSP CONNECTION, ROUTING, QoS

Objects of research – GMPLS technology, ASON architecture, protection and recovery mechanisms.

The purpose of work – analysis of the main protection and recovery mechanisms provided by GMPLS technology in order to ensure continuous operation and the required quality of service in optical transport networks of the ASON type, which, in turn, are the basic platform for the deployment of GMPLS.

The analysis the wide range of mechanisms used for protection and recovery of switched LSPs, such as: local repair, protective switching, fast rerouting, multi-level protection, is carried out. For these mechanisms, various practical methods of their application on networks with GMPLS technology are considered. The relationship of GMPLS security mechanisms with real-time QoS routing is explored. Simulation modeling the GMPLS network was carried out and a typical calculation of traffic parameters was proposed.

ЗМІСТ

С.
ПЕРЕЛІК СКОРОЧЕНЬ 8
ВСТУП 10
1 ЗАГАЛЬНИЙ АНАЛІЗ ОСОБЛИВОСТЕЙ ОРГАНІЗАЦІЇ І ПРИНЦИПІВ ФУНКЦІОНУВАННЯ ТЕХНОЛОГІЙ MPLS І GMPLS 13
1.1 Технологія MPLS 13
1.1.1 Базові особливості та елементи технології MPLS 13
1.1.2 Принципи функціонування мережі MPLS 17
1.2 Технологія GMPLS 22
1.2.1 Загальна структурна модель ASON 23
1.2.2 Технологія GMPLS як складова мережної архітектури ASON 26
1.2.3 Технологія GMPLS з підтримкою багатопротокольної λ-комутації 28
2 АНАЛІЗ ОСНОВНИХ МЕХАНІЗМІВ ЗАХИСТУ ТА ВІДНОВЛЕННЯ В МЕРЕЖАХ GMPLS 35
2.1 Механізм захисту типу «місцеве відновлення» 35
2.2 Механізм захисту типу «захисна комутація» 38
2.3 Механізм захисту за типом «швидкої перемаршрутизації» 40
2.3.1 Захист каналу 41
2.3.2 Захист вузлів 42
3 АНАЛІЗ МЕХАНІЗМІВ БАГАТОРІВНЕВОГО ЗАХИСТУ GMPLS 46
3.1 Особливості та принципи організації динамічного багаторівневого захисту 46
3.2 Маршрутизація із забезпеченням якості обслуговування в реальному масштабі часу та підтримкою багаторівневого захисту 48
4 ІМІТАЦІЙНЕ МОДЕЛЮВАННЯ МЕРЕЖІ GMPLS ТА ТИПОВИЙ РОЗРАХУНОК ПАРАМЕТРІВ ТРАФІКУ 53
4.1 Імітаційна модель маршрутизації трафіка в мережі GMPLS 53
4.2 Типовий розрахунок параметрів трафіка в мережі GMPLS 56
ВИСНОВКИ 59
ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ 62
ДОДАТОК А ЗНАЧЕННЯ ПАРАМЕТРІВ, ЩО НЕОБХІДНІ ДЛЯ СТВОРЕННЯ LSP, У РАЗІ ЗАПИТУ ЗАГАЛЬНОЇ МІТКИ 64
ДОДАТОК Б ПУБЛІКАЦІЇ 66
ДОДАТОК В СЛАЙДИ ПРЕЗЕНТАЦІЇ 70

ПЕРЕЛІК СКОРОЧЕНЬ

ASON (Automatic Switched Optical Network) – оптична мережа, що автоматично комутується;

BGP (Border Gateway Protocol) – протокол маршрутизації зовнішнього шлюзу;

DiffServ (Differentiated Service) – диференційоване обслуговування;

DLCI (Data Link Connection Identifier) – ідентифікатор з'єднання канального рівня;

E-LSR (LER, EDGE-LSR,) (Label Edge Routers) – прикордонні маршрутизатори MPLS;

EN (Edge Nodes) – прикордонні вузли;

FEC (Forwarding Equivalence Class) – клас еквівалентної пересилки;

FSC (Fiber-Switch Capable) – волоконно-оптичні інтерфейси;

GMPLS (Generalized MPLS) – технологія узагальненої (універсальної) багатопротокольної комутації за мітками;

GRP (Global Recovery Path) – глобальний шлях захисту;

IETF (Internet Engineering Task Force) – група інженерних проблем Internet;

IGP (Interior Gateway Protocol) – протокол маршрутизації внутрішнього шлюзу;

IPG (Inter Packet Gap) – міжкадровий інтервал;

IS-IS (Intermediate System-to-Intermediate System) – протокол маршрутизації проміжних систем;

λSC чи LSC (λ чи Lambda Switch Capable) – хвильові або оптичні канальні інтерфейси;

LDP (Label Distribution Protocol) – протокол розподілу міток;

LIB (Label Information Base) – таблиця інформаційної бази міток;

LRP (Local Recovery Path) – локальний шлях захисту;

LSP (Label Switched Path) – комутований за мітками шлях (тракт);

LSR (Label Switching Routers) – маршрутизатори, що комутують за мітками (транзитні маршрутизатори MPLS);

MPλS (Multi-Protocol Lambda Switching) – багатопротокольнаї λ-комутація або багатопротокольна комутація хвиль за мітками;

MPLS (Multi-Protocol Label Switching) – багатопротокольна комутація пакетів за мітками;

MSS (Maximum Segment Size) – кількість корисних даних;

MTU (Maximum Transmission Unit) – максимальний розмір кадру;

NGI (Next Generation Internet) – Інтернет наступного покоління;

NGN (Next Generation Network) – мережа наступного покоління;

NMI (Network Management Interface) – інтерфейс мережного управління;

NNI (Network-Network Interface) – інтерфейс «мережа-мережа»;

OOC (Optical Connection Controller) – контроллер оптичних з'єднань;

OSPF (Open Shortest Path First) – протокол пошуку найкоротшого шляху;

OTN (Optical Transport Network) – оптична транспортна мережа;

OXC (Optical Cross-Connect) – оптична кросова комутації;

PDU (Protocol Data Unit) – блок протокольних даних;

PLR (Point of Local Repair) – точка відновлення;

RRO (Route Record Object) – об'єкт запису маршруту

PSC (Packet-Switch Capable) – інтерфейс із можливістю пакетної комутації;

PSL (Path Switch LSR) – комутатор шляху;

QoS (Quality of Service) – якість обслуговування;

RIP (Routing Information Protocol) – протокол маршрутної інформації;

RSVP (Resource Reservation Protocol) – протокол резервування ресурсів;

TDM (Time-Division Multiplex Capable) – інтерфейс з можливістю часового розділення;

TE (Traffic Engineering) – інжиніринг трафіку;

TTL (Time To Live) – час життя;

UNI (User Network Interface) – інтерфейс «користувач-мережа»;

VCI (Virtual Circuit Identifiers) – ідентифікатори віртуального каналу;

VPI (Virtual Path Identifiers) – ідентифікатори віртуального шляху;

VPN (Virtual Private Networks) – віртуальна приватна мережа;

WP (Working Path) – основний (робочий) шлях.

ЕМВОС – еталонна модель взаємодії відкритих систем;

ОВ – оптичне волокно.

ВСТУП

В сучасних телекомунікаціях, в основі організації яких лежать передові високошвидкісні технологічні рішення, особлива увага приділяється надійності та стабільності роботи мереж, а також якості послуг, що надаються на їх платформах. Від того наскільки стійка мережева інфраструктура до аварій і збоїв апаратного та програмного забезпечення, як швидко відбувається відновлення після них, залежить рівень надійності мережі та якість послуг, що надаються.

Слід зазначити, що на сьогоднішній день у рамках надання сучасних та традиційних послуг різних типів, найбільшого поширення набули платформи, які базуються на концепції побудови мереж наступного покоління (Next Generation Network, NGN), особливістю яких є наявність універсальної транспортної платформи з розподіленою комутацією пакетів, яка відіграє функції ядра мережі. Практичною реалізацією транспортної платформи NGN фактично є мережа Інтернет, у якій основним протоколом здійснення мережного обміну є IP-протокол. Крім того, більшість інфокомунікаційних послуг типу Triple-Play Services також орієнтовані при створенні та наданні кінцевому користувачеві на IP транспорт [1].

Однак, незважаючи на широку поширеність IP-технологій та величезну кількість різноманітних послуг та додатків, що розроблені на цей час під них, існуючі архітектурні рішення організації транспортних IP-мереж часто неефективно використовують пропускну здатність у процесі передачі трафіку, а також вносять значні часові затримки при обробці даних внаслідок здійснення численних протокольних інкапсуляцій даних. Крім того, для таких мереж внаслідок безлічі технологій, що використовуються, залишаються високими поточні експлуатаційні витрати [2].

Ці фактори та вимоги, що швидко і постійно зростають, до пропускної здатності, вимагають впровадження нових архітектурних рішень організації транспортних IP-мереж, які мають враховувати більш ефективне використання мережних ресурсів, водночас дозволяючи розгорнути гнучкі механізми захисту та відновлення і зменшити експлуатаційні витрати. Одним із таких рішень є технологія багатопротокольної комутації на основі міток (Multi-Protocol Label Switching, MPLS). Вона розглядається як базова технологічна основа для побудови мереж NGN в якості мережної інфраструктури для надання нових

послуг та запровадження протоколу IP, як універсального транспорту для всіх видів додатків. Реалізація структури мережі на базі технології IP/MPLS дозволяє забезпечити ефективне управління транспортною мережею, забезпечити передачу трафіку реального часу з необхідною якістю обслуговування (Quality of Service, QoS), а також підвищити гнучкість та масштабованість маршрутизації IP мереж з дотриманням необхідних вимог для побудови NGN . Одночасне застосування технології MPLS в якості транспортного механізму протоколу IP дозволяє зменшити собівартість і покращити якість послуг [3 - 5].

Слід зазначити, що для сучасних транспортних платформ, зокрема і на базі технологій передачі даних IP/MPLS, фізичною основою забезпечення високошвидкісної передачі трафіку реального часу з необхідним QoS є оптичні лінії зв'язку [6, 7].

Такий симбіоз високошвидкісних оптичних технологій (наприклад, таких як Gigabit Ethernet, SDH, DWDM) та технологій IP/MPLS дозволить у подальшому сформувати єдині технологічні основи переходу до Інтернету наступного покоління (Next Generation Internet, NGI). В основі створення платформи NGI лежить організація транспортної інфраструктури, в якій враховується поточний та перспективний трафік послуг, де основою його передачі стає технологія IP/MPLS, яка гарантує надання послуг у реальному та відносному масштабі часу. До таких послуг відносять і традиційні голосові послуги, і широкосмугові, і досить великий спектр нових інфокомунікаційних послуг, що входять до концептуального набору Triple-Play Services (цифрове телебачення та радіомовлення, відео за запитом тощо). При цьому транспортні мережі мають дуже швидко реагувати на запити щодо обслуговування [6, 8].

Ці можливості реалізуються за рахунок впровадження в транспортні мережі протоколів сигнального керування, функціонування яких здійснюється у відповідності із принципами, закладеними у моделі організації технології узагальненої (універсальної) багатопротокольної комутації за мітками (Generalized MPLS, GMPLS), яка є продовженням еволюції класичної технології MPLS, та моделі побудови оптичних мереж, що автоматично комутуються. (Automatic Switched Optical Network, ASON). Моделі GMPLS та ASON є складовою глобальної стратегії розвитку NGN. Реалізована на їх основі оптична транспортна платформа, як частина загальної мультисервісної інфраструктури, забезпечить зниження витрат операторів на надання нових послуг при збереженні високої надійності, гнучкості та відкритості транспортної мережі [8, 9].

У цій магістерській кваліфікаційній роботі аналізується можливість забезпечення захисту та відновлення працездатності у мережах типу ASON на базі технології GMPLS. Метою проведення даного аналізу є висвітлення стратегій та підходів підвищення живучості оптичних мереж з використанням технології GMPLS із застосуванням механізмів захисту та відновлення. Транспортні мережі такого типу мають високу продуктивність каналів, але при цьому слабко пов'язані. В результаті вони є вразливими для відмов і, як наслідок, можуть призвести до втрати величезної кількості трафіку. Тому механізми захисту/відновлення у транспортних мережах GMPLS мають критичне значення, що говорить про актуальність роботи.

1 ЗАГАЛЬНИЙ АНАЛІЗ ОСОБЛИВОСТЕЙ ОРГАНІЗАЦІЇ І ПРИНЦИПІВ ФУНКЦІОНУВАННЯ ТЕХНОЛОГІЙ MPLS І GMPLS

1.1 Технологія MPLS

1.1.1 Базові особливості та елементи технології MPLS

Як було зазначено, найбільш перспективним напрямом побудови сучасної мережної інфраструктури є використання оптичних технологій для організації високошвидкісних магістралей транспортної мережі, а також реалізація єдиної системи сигналізації та управління, що дозволяє об'єднувати різні типи середовищ і систем передачі інформації. Провідні провайдери прагнуть організувати свій сервіс так, щоб на базі однієї опорної мережі можна було б надавати комплекс різних традиційних та сучасних інфокомунікаційних послуг, таких, як IP-телефонія, інтерактивні ігри, потокове відео (IPTV), електронна торгівля, вебінари, відеоконференції, електронна медицина та багато інших. В якості такої об'єднуючої технології на цей час пропонується технологія MPLS, яка значно розширює наявні перспективи мережного масштабування, підвищує швидкість обробки трафіку і надає величезні можливості для організації додаткових послуг [5, 10].

Ця технологія первісно була розроблена компанією Cisco для передачі даних від одного вузла мережі до іншого за допомогою міток без використання традиційних методів адресації. Вона поєднує у собі можливості управління трафіком, що властиві технологіям канального рівня, та масштабованість і гнучкість протоколів, що є характерним для мережного рівня. Будучи результатом злиття механізмів різних компаній, вона увібрала найбільш ефективні рішення кожної. Тому сучасні мережі MPLS можуть працювати з IP-пакетами, комірками ATM, кадрами SDH, і навіть можуть бути використані для передачі стандартних кадрів Ethernet [10, 11].

Таким чином, багатопротокольність технології MPLS означає, що вона є інкапсулюючим протоколом і може транспортувати безліч інших протоколів нижчих рівнів еталонної моделі взаємодії відкритих систем (EMBBC), як показано на рис. 1.1. При цьому слід зазначити, що MPLS не замінює IP-маршрутизацію, а працює поверх неї [5, 11].

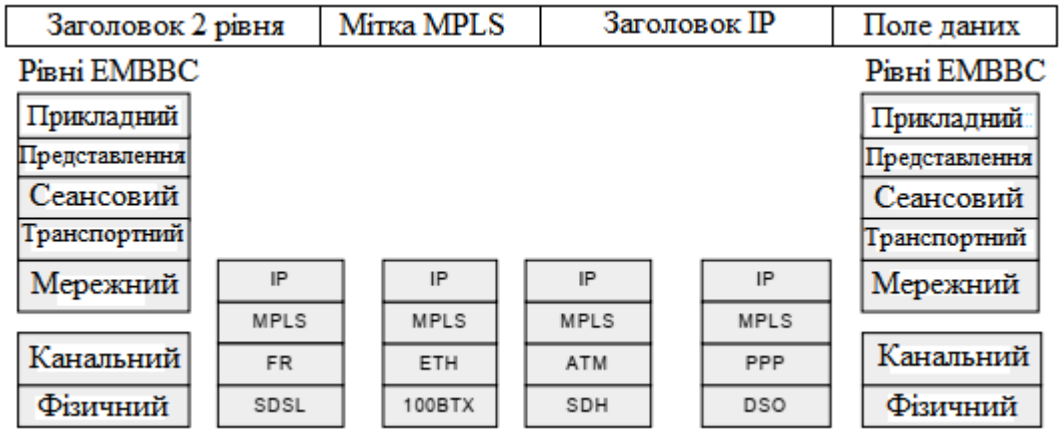

Рисунок 1.1 – Розташування MPLS у відповідності до рівнів EMBBC

Фізичний рівень містить функції, що забезпечують використання фізичного середовища для двосторонньої передачі бітів (з тією достовірністю, яку забезпечує це середовище) по прямому тракту, що зв'язує два вузли мережі. Другий рівень (Layer 2 (L2), канальний рівень) містить функції, що забезпечують формування у цьому тракті надійної логічної ланки зв'язку, по якій відбувається двосторонній обмін інформаційними блоками між вузлами. На цьому рівні виявляються і виправляються помилки, і гарантується достовірність передачі. Третій рівень (Layer 3 (L3), мережний рівень) містить функції, що забезпечують транспортування інформаційних блоків від відправника до одержувача через кілька вузлів мережі за придатним для цього маршрутом транспортування, що складається з ланок другого рівня [5].

З точки зору EMBBC (рис. 1.1), технологія MPLS включає в себе комбінацію методів передачі даних на рівнях L2 і L3. Контроль трафіку реалізується за допомогою передачі частини функцій від L2 до L3. Тому таке одночасне функціонування MPLS на рівнях L3 та L2 призводить до утворення комбінованого підрівня – L2.5, що поєднує їх переваги. На цьому рівні L2,5 і виконується комутація за мітками [5, 10].

У мережах MPLS пакетам даних присвоюються так звані «мітки» (Label), а саме функціонування MPLS побудовано навколо протоколу IP. Мітки використовуються як своєрідна адреса вузла, якому призначений конкретний пакет даних. При цьому вміст самого пакета не має значення, а дані передаються відповідно до мітки. Основна перевага міток полягає в тому, що вони комутуються швидше, ніж здійснюється маршрутизація пакетів в мережах IP.

Застосовуючи різні мітки, можна створювати кілька різних віртуальних мереж на базі одних і тих самих вузлів. Крім того, мережі MPLS можна масштабувати [10].

Технологія MPLS задіює протоколи маршрутизації для обміну інформацією з іншими маршрутизаторами. З використанням цієї інформації створюється і модифікується спочатку таблиця маршрутизації, а потім, з урахуванням інформації про суміжні системи на кожному інтерфейсі – таблиця комутації міток. Відповідний запис у таблиці комутації міток вказує, на який вихідний інтерфейс системи необхідно направити пакет, що надійшов [4].

Класичний формат мітки MPLS показаний на рис. 1.2. Він включає чотири поля, загальний обсяг яких становить 32 біти [10, 12].

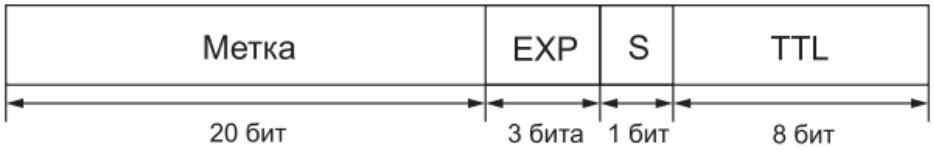

Рисунок 1.2 – Класичний формат мітки MPLS

Перше поле «Мітка» має розмір 20 біт і визначає шлях комутації за мітками. Друге поле «Резерв» (Experimental, Exp) займає 3 біти. Воно первісно було зарезервовано для розвитку технології, а також це поле можна використовувати для зазначення класу трафіку, що необхідний для забезпечення потрібного рівня QoS. Третє, однобітове поле – ознака «Дно стека міток» (Set field, S) – визначає ієрархію стека міток MPLS. У заголовку останньої мітки біт S = 1, а у всіх інших біт S = 0. Останнє поле: «Час життя» (Time to Live, TTL), – займає 8 біт і використовується для визначення кількості задіяних транзитних маршрутизаторів. Інформація цього поля дозволяє вибраковувати із пакета закільцьовані або пошкоджені посилки [10, 12].

Мітка передається у складі будь-якого пакета, причому спосіб її прив'язки до пакета залежить від технології канального рівня, що використовується. Так, наприклад, у мережах ATM роль міток виконують ідентифікатори віртуального шляху або віртуального каналу (Virtual Path Identifiers / Virtual Circuit Identifiers, VPI/VCI), а в мережах Frame Relay використовуються ідентифікатори з'єднання канального рівня (Data Link Connection Identifier, DLCI). Її значення унікальне лише для ділянки шляху між сусідніми вузлами мережі MPLS, які називаються

маршрутизаторами, що комутують за мітками (Label Switching Router, LSR). Мітка використовується для пересилання пакетів від верхнього маршрутизатора до нижнього, де, будучи вхідною, замінюється на вихідну мітку, що має локальне значення на наступній ділянці шляху. Таким чином, значення мітки змінюється по мірі просування пакета мережею [4].

За значенням мітки пакета у кожному вузлі маршруту, за яким цей пакет передається, визначається його належність певному класу еквівалентності пересилки (Forwarding Equivalence Class, FEC). Клас FEC є формою подання групи пакетів з однаковими вимогами до їх передачі, тобто. всі пакети в такій групі обробляються в маршрутизаторі однаково і однаково прямують до пункту призначення. Прикладом FEC можуть бути всі IP пакети з адресами пунктів призначення, що відповідають деякому префіксу, наприклад, «128.87». Можливі також FEC на основі префікса адреси та ще якогось поля IP-заголовка, наприклад, «тип обслуговування». Кожен маршрутизатор мережі MPLS створює таблицю інформаційної бази тегів (Label Information Base, LIB), за допомогою якої визначає, як має передаватися пакет. Ця таблиця містить всю множину міток, що використовується для передачі пакета, і для кожної з них відповідну прив'язку «FEC-мітка» [3, 4].

Метод передачі пакетів на основі прив'язки «FEC-мітка», що застосовується MPLS, має ряд переваг перед методами, що орієнтовані на аналіз заголовків IP-пакетів. Зокрема, передачу за технологією MPLS можуть виконувати маршрутизатори, які здатні читати і замінювати мітки, але при цьому або взагалі не здатні аналізувати заголовки IP пакетів, або не здатні робити це досить швидко [3].

Клас FEC являє собою набір FEC-елементів, кожен з яких ідентифікується певною міткою. На сьогоднішній день існує всього два FEC-елементи: «Address Prefix» і «Host Address» [3].

Таким чином, при здійсненні співвіднесення пакетів за різними класами еквівалентності пересилання велику роль відіграють IP-адреси, пріоритети обслуговування та інші параметри трафіку. Кожен FEC обробляється окремо, що дозволяє підтримувати потрібне QoS у мережі MPLS.

Розподіл міток між LSR призводить до встановлення всередині домену MPLS комутованих за мітками шляхів або трактів (Label Switching Path, LSP). Такий тракт являє собою послідовністю LSR, а за своєю суттю він є віртуальним каналом у загальнодоступній мережі передачі даних (наприклад, Інтернет). Всередині комутованого по мітках тракту створюється LSP-тунель, при цьому найчастіше початок і кінець тунелю не збігаються з початком і кінцем LSP-

тракту, оскільки тунель може бути коротшим. Набір пакетів, що передається LSP, відноситься до одного FEC, і кожен маршрутизатор LSR в LSP тунелі призначає для нього свою мітку. В одному LSP може бути створено кілька LSP тунелів з різними точками прийому та передачі, а в кожному тунелі можуть бути створені LSP тунелі іншого рівня, що говорить про ієрархічність структури MPLS [3, 13].

Таким чином, LSP можна розглядати як тракт, що створюється шляхом з'єднання однієї або більше ділянок маршруту, який дозволяє пересилати пакет, здійснюючи заміну на кожному вузлі мережі MPLS вхідну мітку вихідною міткою (так звана процедура перестановки міток). Іншими словами, LSP в мережі MPLS можна розглядати як тунель, у разі створення якого в IP-пакет вставляється заголовок - мітка, що було показано вище. Створення у віртуальному тракті тунелів, за якими проходять інші віртуальні тракти, ґрунтується на інкапсуляції пакетів, що передаються, в пакети, що слідують по цьому тракту до даної адреси призначення. Слід зазначити, що LSP встановлюються перед передачею даних (з управлінням від програми), або при виявленні певного потоку даних (що управляються безпосередньо даними LSP) [3].

1.1.2 Принципи функціонування мережі MPLS

Мережа MPLS ділиться на дві функціонально різні області – ядро та прикордонну область. Ядро утворюють пристрої, мінімальною вимогою до яких є підтримка MPLS та участь у процесі маршрутизації трафіку для того протоколу, який комутується за допомогою MPLS. Маршрутизатори ядра займаються лише комутацією на основі міток. Всі функції класифікації пакетів за різними FEC, а також реалізацію таких додаткових сервісів, як фільтрація, явна маршрутизація, вирівнювання навантаження та управління трафіком, беруть на себе прикордонні LSR (Label Edge Routers, LER (EDGE-LSR, E-LSR)). В результаті інтенсивні обчислення припадають на прикордонну область, а високопродуктивна комутація виконується в ядрі, що дозволяє оптимізувати конфігурацію пристроїв MPLS залежно від їх розташування в мережі [4].

Узагальнено функціонування мережі MPLS полягає у наступному. Кожен маршрутизатор LSR, як було зазначено вище, містить таблицю LIB, яка ставить у відповідність парі «вхідний інтерфейс, вхідна мітка» трійку – «FEC, вихідний інтерфейс, вихідна мітка». Отримавши пакет, маршрутизатор LSR за номером інтерфейсу, на який прийшов пакет, і за значенням прив'язаної до пакета мітки, а

також використовуючи таблицю LIB, визначає для нього вихідний інтерфейс. Значення FEC застосовується лише для побудови таблиці LIB і у самому процесі комутації не використовується. Старе значення мітки замінюється на нове, що міститься в полі «вихідна мітка» таблиці, і пакет відправляється до наступного пристрою на шляху LSP [4].

Вся операція вимагає лише одноразової ідентифікації значень полів в одному рядку таблиці. Це займає набагато менше часу, ніж порівняння IP-адреси відправника з найбільш довгим адресним префіксом у таблиці маршрутизації, яке використовується при традиційній маршрутизації [4].

Ключова особливість MPLS – відокремлення процесу комутації пакета від аналізу IP-адрес у його заголовку. Очевидним наслідком є той факт, що черговий сегмент LSP може не збігатися з черговим сегментом маршруту, який мав би бути обраним у разі здійснення традиційній маршрутизації від джерела [4].

В якості прикладу на рис.1.3 показаний домен мережі MPLS, що містить маршрутизатори двох типів: прикордонні (E-LSR), що формують прикордонні ділянки мережі, і транзитні (LSR), що становлять область ядра мережі. До домену підключені маршрутизатори R1 та R2, що використовують традиційну IP-маршрутизацію. Розглянемо шлях проходження IP-пакета від маршрутизатора R1 до маршрутизатора R2 через MPLS-домен. Адресою призначення IP-пакету є 128.87.21.4 [4].

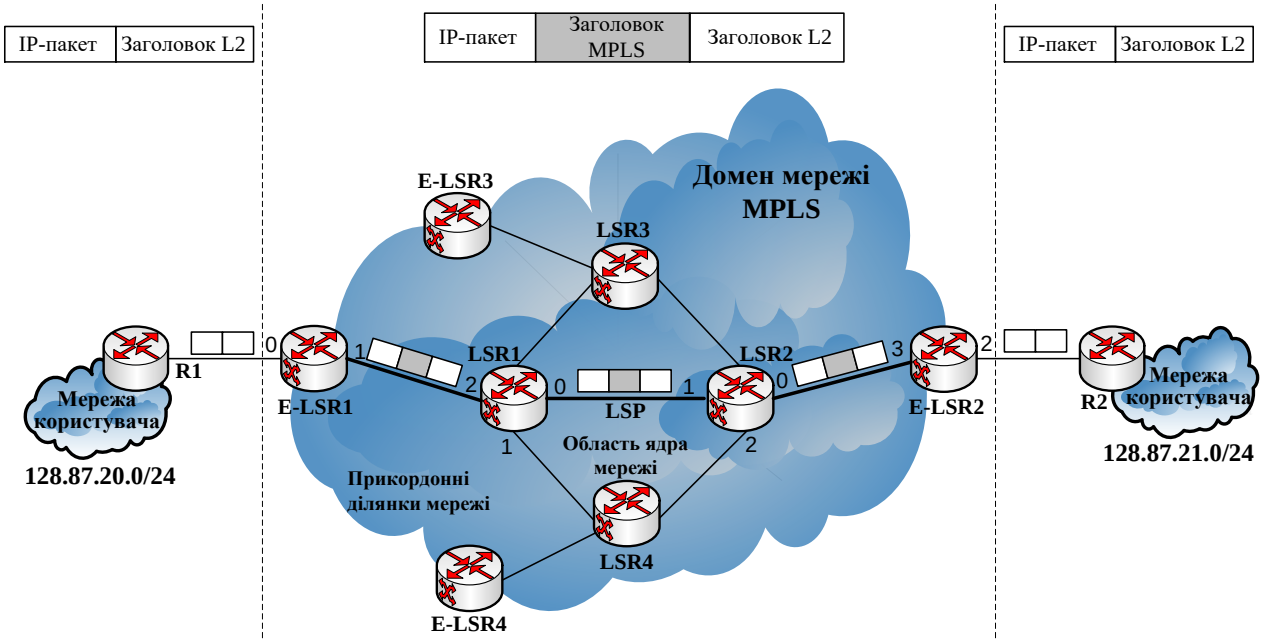

Рисунок 1.3 – Спрощена структура домена мережі MPLS

Маршрутизатор R1 пересилає звичайний IP-пакет у бік прикордонного маршрутизатора E-LSR1. Мережа автоматично формує таблиці маршрутизації за допомогою протоколів маршрутизації [4].

Такими протоколами може бути [4]:

- протокол маршрутизації внутрішнього шлюзу (Interior Gateway Protocol, IGP), що використовується для обміну інформацією про маршрутизацію між шлюзами (зазвичай маршрутизаторами) в автономній системі (Інтернет);

- протокол пошуку найкоротшого шляху (Open Shortest Path First, OSPF) – протокол динамічної маршрутизації, що ґрунтується на технології відстеження стану каналу та використовує для знаходження найкоротшого шляху алгоритм Дейкстри;

- протокол маршрутної інформації (Routing Information Protocol, RIP), що дозволяє маршрутизаторам динамічно оновлювати маршрутну інформацію, одержуючи її від сусідніх маршрутизаторів;

- протокол маршрутизації проміжних систем (Intermediate System-Intermediate System, IS-IS) - це різновид протоколу маршрутизації внутрішніх шлюзів. Він оперує інформацією про стан лінків інших маршрутизаторів. Кожен маршрутизатор IS-IS формує власну базу топології мережі, збираючи отриману інформацію. Як і OSPF, протокол IS-IS використовує алгоритм Дейкстри для прорахунку найкращих маршрутів та інші протоколи.

Таким чином, маршрутизатор E-LSR1 отримує топологічну інформацію про мережу, беручи участь у роботі алгоритмів маршрутизації протоколів OSPF, BGP, IS-IS. Потім він починає взаємодіяти із сусідніми маршрутизаторами, розподіляючи мітки за допомогою спеціального протоколу розподілу міток (Label Distribution Protocol, LDP). Цей протокол за допомогою таблиць маршрутизації визначає значення міток, що вказують на сусідні пристрої. Внаслідок цієї операції формуються LSP. Ознакою створення LSP-тракту є те, що у кожному маршрутизаторі LSR на вибраному маршруті сформовано таблиці LIB. Зазначимо, що LSP створюється до того, як з'являється трафік [4].

Як показано на рис. 1.3, маршрутизатор E-LSR1 класифікує пакет, що надійшов на його вхід (відносить його до класу FEC 128.87), далі на основі таблиці маршрутизації визначає мітку, яку необхідно призначити пакету, і пересилає пакет у напрямку вузла LSR1 по певному маршруту сформованого тракту LSP. У кожній точці просування пакета в області ядра мережі (маршрутизатори LSR1 і LSR2, що належать тракту LSP) здійснюється операція

зчитування мітки вхідного пакета, заміна старої мітки новою і просування пакета далі по ядру [4].

Прикордонний маршрутизатор E-LSR2 видаляє мітку, зчитує IP-заголовок пакета і передає маршрутизатору R2 [4].

Більше детально принцип передачі пакету по мережі MPLS розглядається на рис. 1.4, де наведений приклад формування таблиць LIB (див. рис. 1.5) [4].

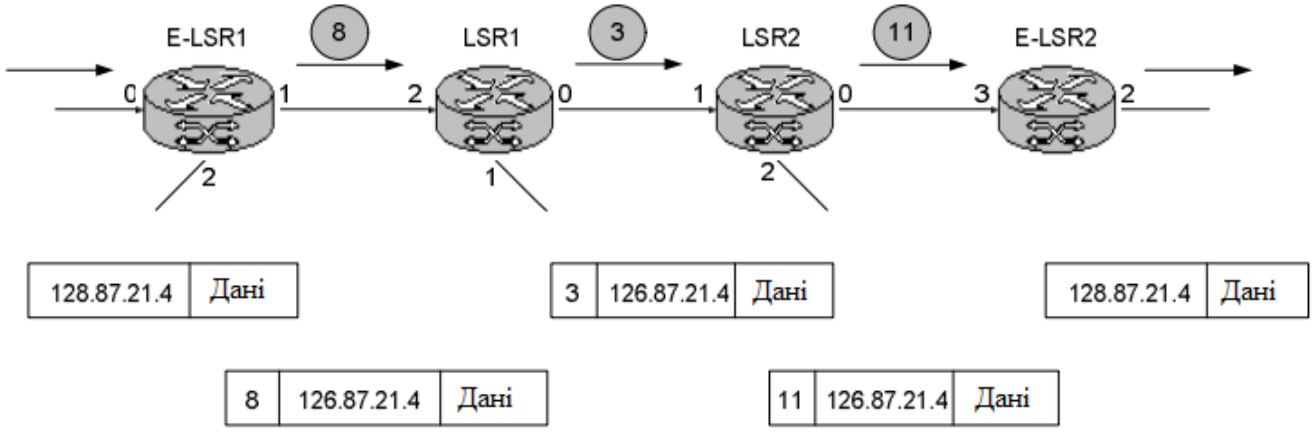

Рисунок 1.4 – Принцип передачі пакета по мережі MPLS

На першому кроці маршрутизатор E-LSR1, куди надходить пакет на вхідний порт «0», зчитує FEC (префікс призначення 128.87) і звертається до таблиці LIB (рис. 1.5а). Після цього E-LSR1 вставляє необхідну мітку 8 і передає пакет на вихідний порт 1 в напрямку до LSR1 [4].

На другому кроці маршрутизатор LSR1, який отримав пакет на вхідний порт «2», зчитує мітку, відповідно до таблиці LIB (рис. 1.5б), замінює мітку «8» на мітку «3» і передає пакет на вихідний порт «0» напрямку до LSR2 [4].

На третьому кроці маршрутизатор LSR2 отримує пакет на вхідний порт «1», зчитує мітку, відповідно до таблиці LIB (рис. 1.5в), здійснює заміну мітки «3» на мітку «11» і передає пакет на вихідний порт «0» напрямі до E-LSR2 [4].

Нарешті, прикордонний маршрутизатор E-LSR2 отримує пакет на вхідний порт «3», обробляє його і в точці виходу відповідно до таблиці LIB (рис. 1.5г), де зазначено, що цю мітку необхідно видалити, направляє пакет без мітки на вихідний порт 2 у напрямку звичайного IP-маршрутизатора R2 (див. рис. 1.3) [4].

У будь-якому сегменті LSR можна виділити «верхній» і «нижній» маршрутизатор LSR по відношенню до трафіку. Наприклад, для сегмента LSR1-

LSR2 перший маршрутизатор буде верхнім, а другий нижнім. Використання маршруту в мережі MPLS, що явно задається, вільне від недоліків стандартної маршрутизації від джерела, оскільки вся інформація про маршрут міститься в мітці, і пакеті не потрібно нести адреси проміжних вузлів, що покращує управління розподілом навантаження в мережі.

а)

Вх. мітка	Вх. порт	Префікс	Вих. мітка	Вих. порт
-	0	128.87	8	1
		…		
-	0	128.87	9	2
		…		
		. . .		

б)

Вх. мітка	Вх. порт	Префікс	Вих. мітка	Вих. порт
8	2	128.87	3	0
		…		
10	2	128.88	10	1
		…		
		. . .		

в)

Вх. мітка	Вх. порт	Префікс	Вих. мітка	Вих. порт
3	1	128.87	11	0
		…		
10	1	128.87	25	2
		…		
		. . .		

г)

Вх. мітка	Вх. порт	Префікс	Вих. мітка	Вих. порт
11	3	128.87	-	2
		…		
30	1	128.87	-	2
		…		
		. . .		

Рисунок 1.5 – Таблиці LIB, що створюються маршрутизаторами MPLS у процесі передачі пакета

Таким чином, MPLS – це один із кроків на шляху еволюційного розвитку мереж, що орієнтовані у цілому на підтримку протоколу IP та особливо мережі Інтернет, у бік спрощення мережної інфраструктури, шляхом інтеграції функцій другого (комутація) та третього (маршрутизація) рівнів [5].

Як видно із рис. 1.1, а також з вищевикладеного, MPLS є універсальною технологією. За її допомогою можна досить легко створювати віртуальні канали

між вузлами мережі та інкапсулювати різні протоколи передачі. Вона дає можливість створення наскрізного віртуального каналу з будь-яким протоколом передачі, незалежного від середовища передачі. В цілому ж можна вирішити безліч інших задач [5, 10]:

- інтеграція з протоколом IP інших пакетних технологій (ATM, Frame Relay);
- прискорене просування пакетів по мережі оператора вздовж традиційних найкоротших маршрутів;
- створення віртуальних приватних мереж (Virtual Private Network, VPN);
- вибір та встановлення шляхів з управлінням трафіку (Traffic Engineering, TE).

Узагальнюючи вищевикладене в попередньому підрозділі, можна бачити, що технологія MPLS забезпечує передачу трафіку найменш завантаженими маршрутами IP-мережі, при цьому підвищує його швидкість обробки та надає можливості для організації додаткових послуг. Успіх MPLS наштовхнув на ідею розробки певної узагальненої технології комутації, яка функціонувала б згідно з принципами, що були закладені в MPLS, і уніфікувала функції управління різних технологій передачі даних [14].

Такою технологією стала технологія GMPLS, у якій термін «узагальнена» підкреслює той факті, що GMPLS охоплює всі аспекти комутаційних можливостей: комутацію пакетів, комутацію з часовим розділенням, комутацію за довжинами хвиль і просторову комутацію. Технологія MPLS еволюціонує до GMPLS шляхом поширення поняття мітка на: довжину оптичної хвилі (так звана «багатопротокольна λ-комутація»), номер оптичного волокна в каналі, номер SDH-контейнера або канального інтервалу в WDM і т.ін. При цьому слід зазначити, що мітки не є виключно додатковими полями в заголовку пакета мережевого рівня [3, 15].

1.2 Технологія GMPLS

Модернізована, розширена версія MPLS, що отримала назву GMPLS, розроблена технічною комісією Інтернет (Internet Engineering Task Force, IETF) і описана в документі RFC 3495. Специфікація GMPLS підтримує роботу з оптичними мережами, що автоматично комутуються (ASON), які позиціонуються

як новий напрямок розвитку оптичних транспортних мереж (Optical Transport Network, OTN) на базі високошвидкісних технологій, таких як Gigabit Ethernet, SDH та DWDM. Цей напрямок є складовою розвитку сучасних телекомунікацій, зокрема, NGN [8, 10].

Інфраструктура транспортної мережі формується з урахуванням поточного та перспективного трафіку послуг. При цьому, як зазначалося, у такій мережі переважає трафік IP, що дозволяє реалізувати послуги у реальному та відносному масштабі часу. При цьому транспортні мережі зобов'язані реагувати на запити щодо обслуговування з мінімальними часовими затримками. Це можливо здійсните у разі впровадження протоколів сигнального управління у транспортні мережі, що організуються з використанням GMPLS. Такий підхід дозволяє помітно покращити їх якість експлуатації, адміністрування та обслуговування [8, 9].

Перед більш глибоким аналізом технології GMPLS необхідно розглянути фізичну мережну структуру, на якій вона застосовується.

1.2.1 Загальна структурна модель ASON

Структурна модель ASON визначена у рекомендаціях ITU-T G.807, G.808 та показана на рис. 1.6 [8].

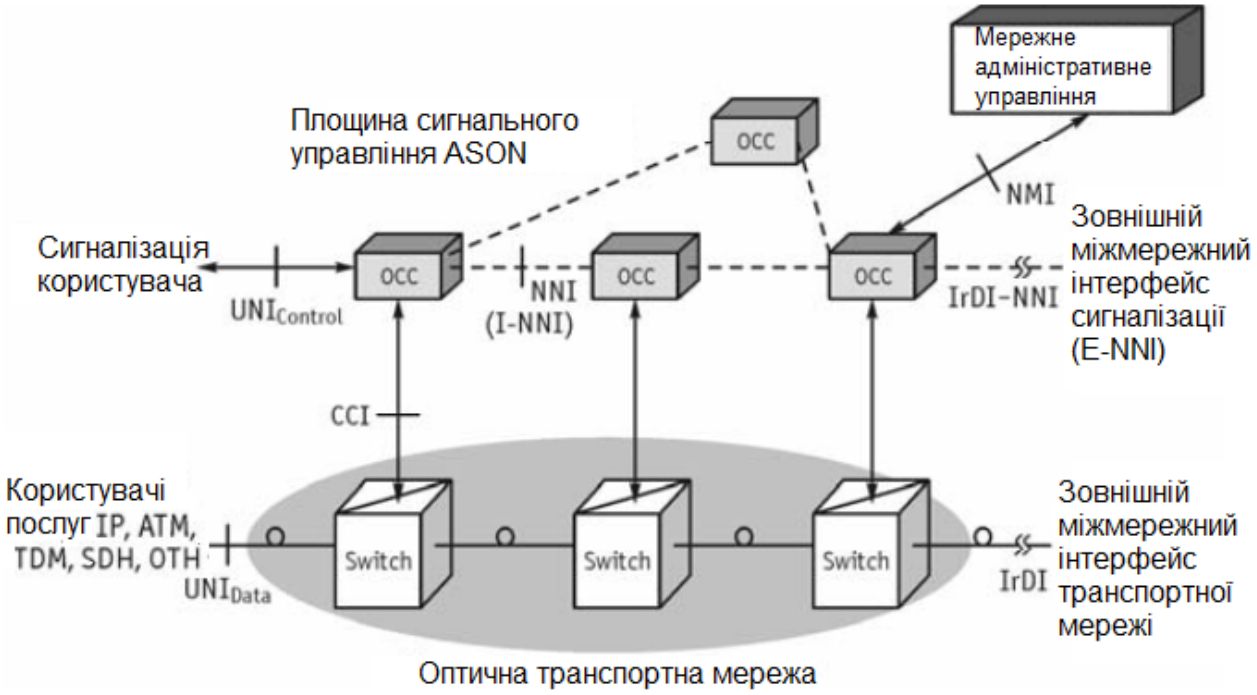

Рисунок 1.6 – Загальна структурна модель ASON

Структура моделі представлена трьома логічними площинами [8, 9]:

- Оптична транспортна площина відповідає за транспортування сигналів даних користувачів ASON. Вона представляється на рис. 1.6 відповідними комутаторами (Switch) та інтерфейсами «користувач-мережа» (User Network Interface Data, UNI_{Data});

- площина сигнального управління передбачає дії щодо встановлення безперервних зв'язків з такими властивостями, як час зв'язку, захист з'єднання, призначення довжини хвилі і т.ін. Ці властивості визначаються користувачем у процесі встановлення з'єднання, а прийнятним рішенням здійснення можливостей площини сигнального управління служить протокол GMPLS. Вона представляється на рис. 1.6 контроллерами оптичних з'єднань (Optical Connection Controller, OOC), між вузловими інтерфейсами «мережа-мережа» (Network-Network Interface, NNI), сигнальними інтерфейсами користувачів $UNI_{Control}$;

- площина адміністративного управління заснована на базових положеннях концепції управління телекомунікаціями, тому ASON включає систему мережного адміністрування з відповідним інтерфейсом мережного управління (Network Management Interface, NMI), яка відповідає за управління конфігурацією транспортної мережі, ліквідацію пошкоджень, безпеку, тощо.

Функціональні особливості моделі ASON визначаються двома різними структурами [9]:

- фізичним ядром та кордоном мережі;

- системою взаємодії клієнт-сервер.

Основні функції ASON, головним чином, пов'язані з комутацією оптичних каналів у межах мережі. Комутація може бути ініційована як площиною сигнального управління за запитом клієнта, так і площиною адміністративного управління [8].

Основними функціями ядра мережі є [8, 9]:

- підтримка відкритої топології мережі. Ця функція забезпечується протоколами маршрутизації у разі наявності достатньої інформації про топологію та ресурси мережі для визначення маршруту передачі трафіку користувача. Для реалізації цієї функції елементи мережі ув'язані у фізичну структуру. Кожен мережний елемент має базу даних, де фіксується інформація про фізичну та логічну структуру інших мережних елементів [8];

- підтримка оптичної маршрутизації. Ця функція визначає маршрут від вузла джерела до вузла призначення з певним набором обмежень (ретрансляції, діапазон довжин хвиль, тощо) [8];

- передача повідомлень сигналізації. Цей набір функцій пов'язаний із сигнальною мережею і дозволяє підтримувати обмін сигналами та повідомленнями управління через певні інтерфейси між мережними елементами, мережами адміністративного сигнального управління, між ASON та її клієнтами. Передача сигнальних повідомлень включає функції обробки з'єднань: встановлення, руйнування, модифікацію [8];

- безперервний захист/відновлення. Є набором функцій, що задіяні у відновленні безперервного оптичного зв'язку, на яку впливає відмова. Ці функції відповідають за виявлення відмови, оптичну маршрутизацію, встановлення тракту захисту, автоматичне безперервне відновлення. У разі відсутності резервного маршруту відбувається стандартна перемаршрутизація [9];

- підтримка автоматичного безперервного оптичного каналу OCh, що готується до роботи. Виконується на запит користувача мережею адміністративного управління або сигнальною мережею, при задіянні сигнального інтерфейсу користувача. Функція включає процедури: визначення маршруту для каналу, його встановлення із резервуванням ресурсу (наприклад, довжин хвиль) і комутації в мережних вузлах [8];

- управління вузлом та його зв'язками. Це набір функцій по управлінню станом мережного вузла, можливостями комутації (оптичною, електричною, пакетною, тощо.) [9];

- підтримка безпеки мережних вузлів. Це функції для забезпечення безпеки мережного вузла та в мережі послуг, а також заданої якості обслуговування. Ці функції мають бути в кожному мережному вузлі (як на кордоні, так і в ядрі мережі) [9].

Функціональні можливості на кордоні ASON полягають у тому, що прикордонні вузли (Edge Nodes, EN) фіксують вхідні та вихідні точки потоків трафіку клієнтів і кінцеві точки оптичних каналів. Потоки трафіку клієнтів, що надходять в оптичну мережу від маршрутизаторів IP, комутаторів ATM , комутаторів Gigabit Ethernet, кросових комутаторів і мультиплексорів SDH, направляються на входи EN. З іншого боку, між вузловий трафік підтримують оптичні канали OCh, які комутуються у вузлах оптичної кросової комутації

(Optical Cross-Connect, OXC) та закінчуються у прикордонних вузлах. При цьому система управління мережею дає інструкції про те, як потоки трафіку користувачів мають оброблятися EN, тобто, як узгоджуються можливі запити на послуги та можливості мережі ASON, що в результаті визначає функціональні можливості прикордонних вузлів [8].

Функції фізичних інтерфейсів повинні реалізовувати адаптацію циклів чи смуги пропускання між обладнанням клієнта та прикордонними вузлами, при цьому можлива здійснення контролю QoS, а також характеристик класів обслуговування [8].

Доступні функції користувача безпосередньо пов'язані з ресурсами OTN і можливостями сигналізації, яка підтримується інтерфейсом користувача. Через інтерфейс користувача здійснюються запит на встановлення з'єднання, ініціація послуги, визначення транспортних послуг, призначення адреси, визначення загрози безпеці, тощо [9].

По відношенню до користувача мережа OTN забезпечує кросову комутацію, виділення та введення оптичних каналів, групування трафіку користувачів у цифрові потоки, перетворення довжини хвилі, оптичне мультиплексування/демультиплексування, захист з'єднання у разі виникнення пошкоджень, тощо.

1.2.2 Технологія GMPLS як складова мережної архітектури ASON

Можливість розповсюдити парадигму заміни міток на нові оптичні технології була вперше представлена як специфікація управління світловими шляхами. Було вище показано, прийнятним рішенням для реалізації можливостей мережного управління ASON служить протокол GMPLS. Він уніфікує управління мережею, забезпечуючи наскрізну інтелектуальність, тобто, від одного кордону мережі оператора через її ядро до іншого кордону на основі уніфікованих засобів сигналізації. Тобто GMPLS є основою сигнальної системи таких мереж. При такому розкладі ті ж самі протоколи, що створюють шлях на канальному або мережному рівнях, будуть використані для створення шляху на фізичному рівні. Якщо класична технологія MPLS використовує мітки, що фізично додаються до пакетів, то в GMPLS ця концепція здійснюється шляхом впровадження нових типів міток, що відносяться до різних оптичних елементів, таких як віртуальні контейнери SDH, лямбди волокна, лямбди канальних інтервалів DWDM, кадри

Gigabit Ethernet, тощо. Дані елементи представлені у вигляді міток у керуючій площині протоколів мережі і використовуються оптичними комутаторами та маршрутизаторами для встановлення з'єднання GMPLS, що дозволяє змінювати процес комутації за мітками для урахування відмінностей у способах призначення міток, а також поширення повідомлень сигналізації та взаємодії з вхідними та вихідними пристроями [3, 5].

Результатом впровадження технології є простота управління, висока пропускна здатність, великий ступінь передбачуваності, підтримка QoS та угод про рівень сервісу (Service Level Agreement, SLA), що робить формування сервісу справою швидкою та оперативною. Збільшення чи зменшення необхідної пропускної здатності можна здійснювати залежно від вимог кінцевих користувачів [4].

Розглянемо типовий приклад мережевої архітектури транспортної ASON у якій для управління потоками трафіку використовується GMPLS (рис. 1.7) [5].

Ця мережна архітектура містить два рівні: рівень пакетів і рівень оптичного транспорту. Останній складається з ОХС, що з'єднані один з одним одним або декількома оптичними волокнами (ОВ), які є фізичними ланками [5].

У кожному ОВ організуються один хвильовий канал, що відповідає одній несучій, якщо використовуються технології Gigabit Ethernet або SDH для організації OTN, або здійснюється мультиплексування декількох хвильових каналів (що відповідають різним канальним несучим) в один груповий (на робочій довжині хвилі третього вікна прозорості), якщо Для організації OTN використовується технологія DWDM. Оптичні з'єднання встановлені через всю мережу між відправником і вузлом одержувача. Оптичні з'єднання та логічні ланки показані на рис. 1.7 пунктирними лініями на рівні пакетів та подвійними пунктирними лініями на оптичному транспортному рівні відповідно [5].

Зібрані разом, ці логічні ланки, що з'єднують між собою маршрутизатори LSR, становлять логічну топологію (еквівалент пакетного рівня для фізичної топології транспортного рівня). Пакетні LSP, що також називаються MPLS LSP, або простими LSP, можуть бути встановлені відповідно до цієї логічної топології (рис. 1.7 червоні лінії) [5].

Наприклад, на рис. 1.7, щоб з'єднати LSR B і LSR F, задіяні LSR B, що називається кінцевим вузлом входу, ОХС b - магістральний кінцевий вузол входу, ОХС f - магістральний кінцевий вузол виходу та LSR F - кінцевий вузол виходу.

Можуть існувати і інші ОХС між ОХС входу і ОХС виходу – вони називаються (проміжними) магістральними вузлами [5].

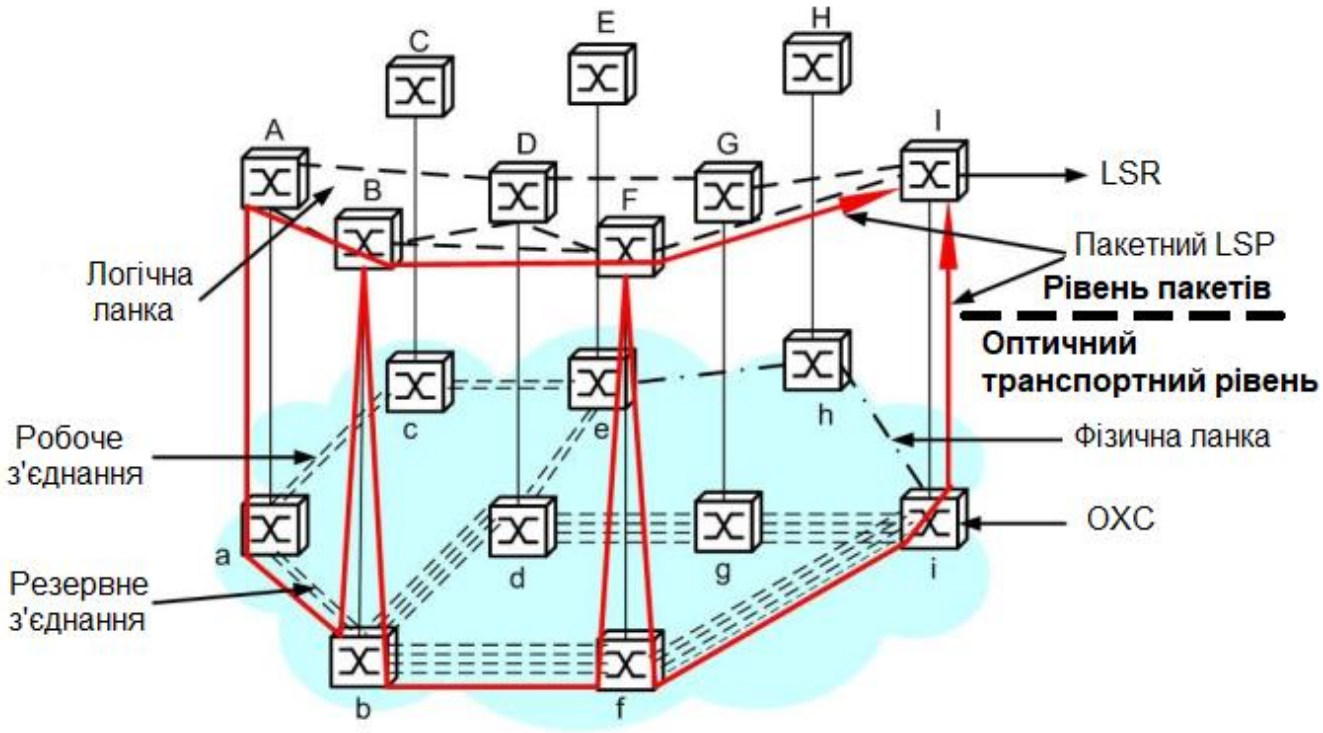

Рисунок 1.7 – Мережна архітектура транспортної ASON з використанням GMPLS

Зазначимо, що у існуючих мережах є безліч рівнів комутації. З економічних причин відбуватиметься їх скорочення так, що залишиться лише кілька. Очікується, що залишаться лише рівні MPLS та Ethernet як комутаційні технології для транспортування IP-трафіку [5].

1.2.3 Технологія GMPLS з підтримкою багатопротокольної λ-комутації

Як вже неодноразово зазначалося, та відповідно до рекомендацій ITU-T G.7713.2 та G.7713.3 технологія GMPLS є основою для реалізації системи сигналізації мережі ASON, а для підтримки оптичної комутації в таких мережах запропоновано рішення, що отримало назву багатопротокольної λ-комутації або багатопротокольної комутації хвиль за мітками (Multi-Protocol Lambda Switching, MPλS). У даному випадку передбачається використання концепції вкладених шляхів з комутацією за мітками. Тут лямбди є мітками, що є важливим як у разі

організації технології оптичного управління, так і при використанні в технології комутації пакетів фізичного шляху поверх оптичного. Це, перш за все, пов'язано із зменшенням кількості функціональних рівнів необхідних для виконання тих же самих завдань, оскільки завдяки використанню MPLS безпосередньо поверх рівня DWDM усувається необхідність у таких рівнях як ATM і SDH [3, 8, 9].

GMPLS можна розглядати як узагальнення MPλS і як більш універсальне розширення технологій ядра MPLS, які використовують парадигму заміни міток та протоколи площини управління для різних комутаційних технологій, насамперед оптичних. Так, якщо знову звернути увагу на рис. 1.7, можна наступним чином застосувати підхід MPλS. Кожен вузол OXC взаємодіє, подібно до MPLS LSR, з площиною управління. Між сусідніми OXC створюється окремий канал управління IP. Світлові шляхи стають трактами LSP, а вибір лямбд та портів крос-з'єднання виявляється процесом, який є аналогічним процесу призначення міток та прив'язки їх до FEC у класичній технології MPLS. Отже, у цьому випадку передбачається використання концепції вкладених комутованих за мітками шляхів (маршрутів, трактів) [3].

Це допускає ще одне трактування терміну «узагальнена» (Generalized) у назві технології GMPLS. Мова йде про те, що GMPLS розширює кількість типів обладнання, що входить в мережу MPLS, а її універсальність полягає в тому, що вона може включати в себе LSR, що не здатні аналізувати заголовки пакетів, але здійснюють маршрутизацію на основі часових інтервалів, довжин хвиль або фізичних портів. Таким чином, інтерфейси між усіма LSR можуть бути поділені на такі класи [3, 15]:

- інтерфейси із можливістю пакетної комутації (Packet-Switch Capable, PSC), тобто інтерфейси між тими LSR, які здатні розрізняти кордони пакетів і виконувати маршрутизацію, ґрунтуючись на змісті їх заголовків, наприклад, інтерфейси між звичайними MPLS LSR або ATM-комутаторами;

- інтерфейси з можливістю часового розділення (Time-Division Multiplex Capable, TDM), через які дані маршрутизуються з урахуванням часових інтервалів, наприклад, інтерфейси SDH чи інтерфейси між цифровими АТС;

- хвильові або оптичні канальні інтерфейси (λ чи Lambda Switch Capable, λSC чи LSC), маршрутизація через які ведеться з урахуванням довжини хвилі, тобто. інтерфейси між оптичними λ-комутаторами;

- волоконно-оптичні інтерфейси (Fiber-Switch Capable, FSC), через які дані маршрутизуються з урахуванням фізичного середовища їх передачі, наприклад, ланки між оптичними комутаторами, які працюють із кількома фізичними волокнами.

При цьому ієрархічна система міток трактів LSP (фактично ієрархія маршрутизації) буде виглядати наступним чином (рис.1.8). На верхній сходинці ієрархії знаходяться інтерфейси FSC, за ними йдуть інтерфейси λSC або LSC, потім TDM, і, нарешті, PSC [8, 9].

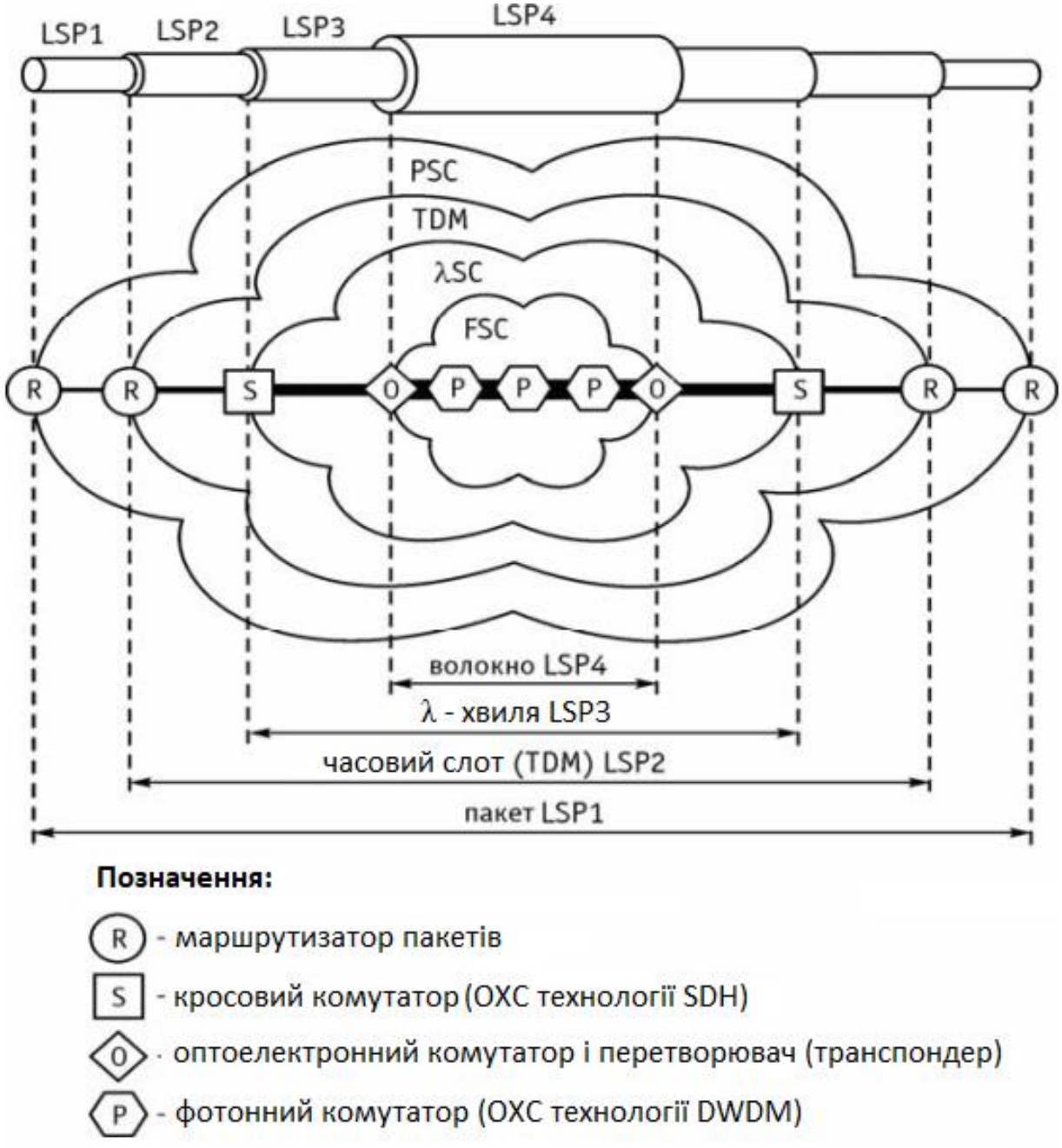

Рисунок 1.8 – Ієрархічна система міток GMPLS трактів LSP

Таким чином, можна бачити, що LSP, який починається і закінчується інтерфейсом PSC, може (разом з декількома іншими LSP) бути поміщений в LSP, що починається і закінчується інтерфейсом TDM. LSP рівня TDM, та інших рівнів, також можуть бути вкладені в тракти LSP, що ієрархічно розташовані вище. Це наочно показано на рис. 1.9 [3].

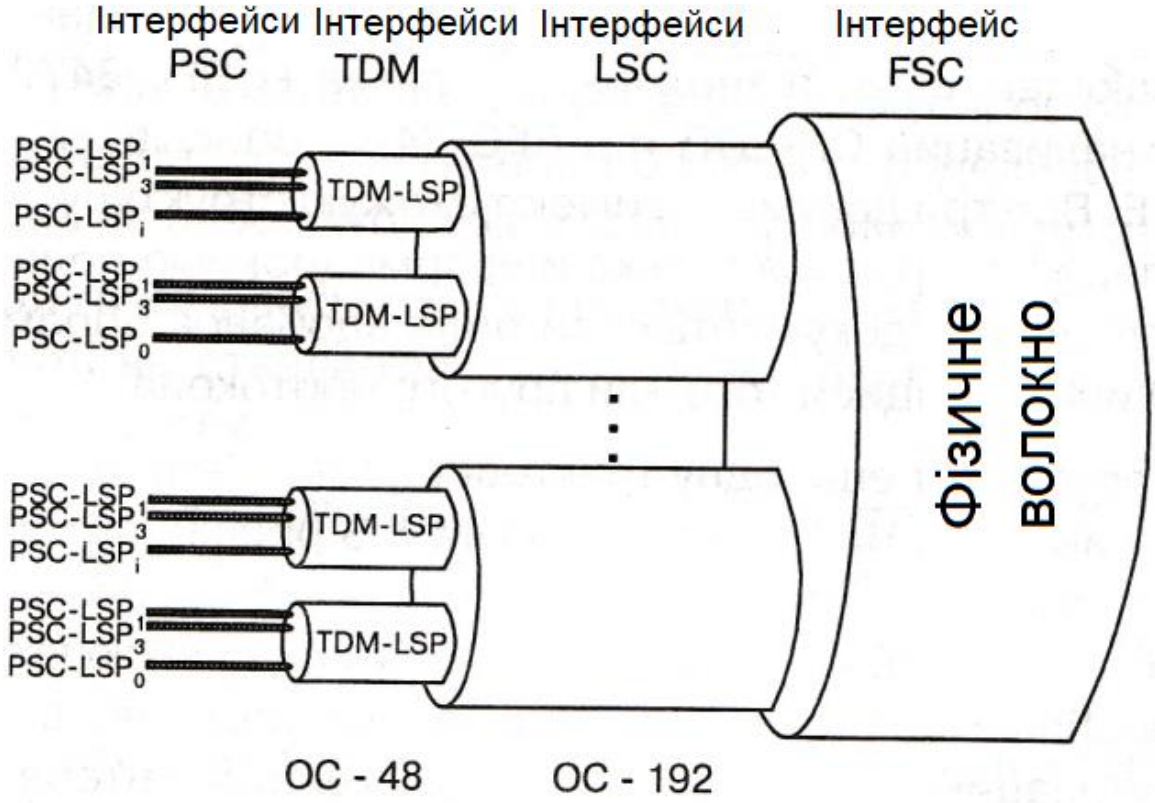

Рисунок 1.9 – Структура вкладених трактів LSP в GMPLS

Для передачі сигнальних повідомлень у мережі запропоновано використання загальних (універсальних) міток. Загальна мітка містить достатньо інформації, щоб дозволити вузлу, що приймає, програмувати комутацію незалежно від типу з'єднання. Структура формату запиту загальної мітки наведена на рис. 1.10 [8].

Повна ємність поля загальної мітки запиту становить 32 біти. Біти 0…7 визначають необхідний для LSP тип кодування (наприклад, мітці «2» відповідає кодування для Ethernet, мітці «5» відповідає кодування для SDH, мітці «8» відповідає λ-комутації, і т.д. (Додаток А, рис .А.1)) [3, 8].

У бітах 8…15 кодується тип комутації, яка має здійснюватися в заданому каналі (наприклад, мітці «150» відповідає λ-комутація LSC, а мітці «200» –

комутація оптичних портів FSC (Додаток А, рис. А.2)). Це поле необхідне для ланок, які допускають комутацію більш одного типу [3, 8].

У бітах 16...31 кодується тип корисного навантаження, що переноситься LSP (наприклад, встановлення з'єднання для мережі Ethernet кодується міткою «33», типи довжин хвиль (Lambda) канальних інтервалів DWDM кодуються міткою «37» (Додаток А, рис. А.3)). Це поле використовується кінцевими вузлами LSP або передостаннім вузлом LSP [3, 8].

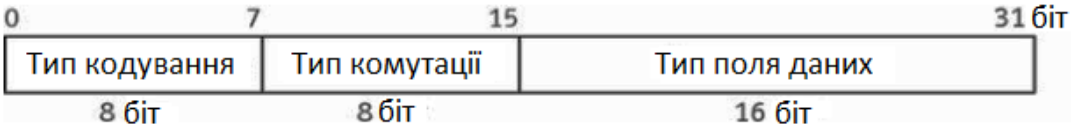

Рисунок 1.10 – Формат запиту загальної мітки

Узагальнена мітка містить у собі лише мітку одного рівня, тобто вона є ієрархічним об'єктом. Для мережі із кількох рівнів (див. рис. 1.8) потрібно кілька рівнів міток. При цьому кожен LSP повинен формуватися окремо, а мітка може мати змінну довжину. Так в залежності від ділянки оптичної мережі ідентифікуються дані про ОВ в пучку, хвильовий канал в діапазоні ОВ, хвильовий діапазон із набору діапазонів ОВ. Наприклад, мітка довжиною 32 біта вказує на ідентифікатор каналу найменшої довжини хвилі у визначеному діапазоні хвиль, а кінцева мітка довжиною теж 32 біта вказує на ідентифікатор каналу найбільшої довжини хвилі в цьому діапазоні. Таким чином, мітка містить три блоки по 32 біти (рис. 1.11) [8].

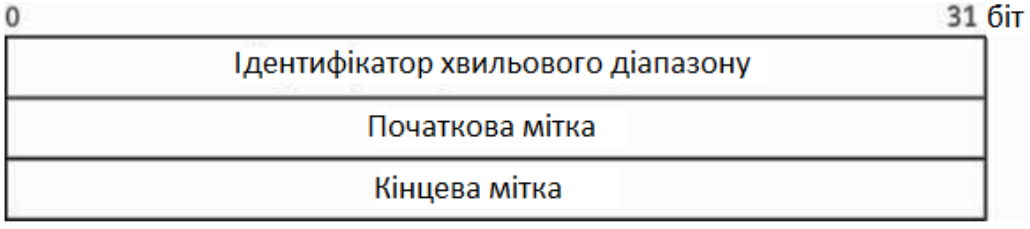

Рисунок 1.11 – Загальна мітка для λ-коммутации

Запропонована мітка використовується для повідомлень вузлам, що лежать нижче, переважних міток від вузлів , що лежать вище (див. рис. 1.8, де самий нижчий вузол R, над ним вузол S, далі за порядком проходження знаходяться

вузли O, P). Таким чином, вузол, що лежить вище, може почати конфігурування обладнання з використанням цієї мітки до того, як ця мітка буде передана вузлам, що лежать нижче. Це рішення може підвищити швидкість процедур встановлення з'єднання та відновлення з'єднання у разі збоїв або відмові [8].

З метою обмеження вибору міток для вузла «нижче за передачею» використовується набір міток для кожного кроку в з'єднанні. Для оптичної мережі можуть використовуватися чотири варіанти набору міток [8]:

- перший варіант реалізується, коли кінцеве обладнання здатне передавати обмежений набір довжин хвиль або діапазонів;

- другий варіант застосовується, коли послідовність інтерфейсів не підтримує перетворення довжин хвиль і необхідно використання лише однієї хвилі по всьому оптичному шляху;

- третій варіант застосовується, коли бажано обмеження числа перетворень довжин хвиль для зменшення оптичних спотворень;

- четвертий варіант передбачає підтримку каналу з різними хвилями по його кінцям.

Набори міток необхідні для обмеження діапазону міток на ділянці одного LSP між двома користувачами. Одержувач набору міток має обмежити свій вибір однією міткою субканалу із набору N (рис. 1.12) [8].

Набір міток складається з однієї або більше міток об'єктів. При цьому під об'єктом прийнято розуміти пакет сигнальної інформації. Кожен об'єкт містить один або більше елементів набору міток. Кожен елемент позначається як субканал і має такий же самий формат, як і загальна мітка. Поле «дія» вказує, що об'єкт містить один або більше субканальних елементів, які включені у набір міток. Поле «резерв» ігнорується під час обробки мітки. Поле типу мітки вказує на тип і формат міток, що містяться в об'єкті. Значення поля залежить від сигналу GMPLS. Поле субканалу представляє мітку довжини хвилі, ОВ, тощо [8].

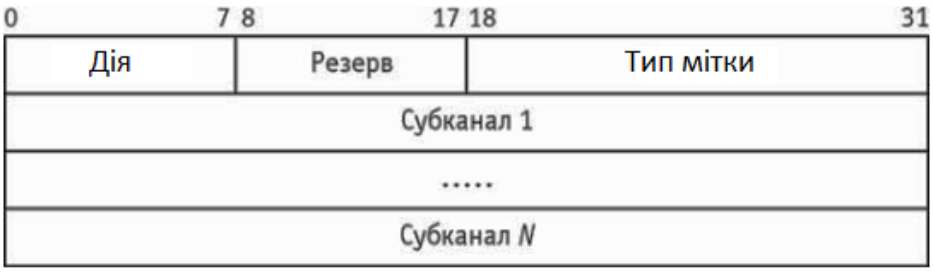

Рисунок 1.12 – Структура блоку даних набору міток

Таким чином, використання технології GMPLS забезпечує наступні переваги: високий рівень контролю за пропускною здатністю, гнучкість і високу швидкість формування транспортного сервісу, просте забезпечення QoS, гарантовану пропускну здатність, масштабованість. Це дозволить провайдерам управляти топологічною структурою мережі у відповідь на зміни картини трафіку, зменшувати кількість рівнів мережі, проводити оптичне відновлення трафіку у разі розриву шляху передачі.

2 АНАЛІЗ ОСНОВНИХ МЕХАНІЗМІВ ЗАХИСТУ ТА ВІДНОВЛЕННЯ В МЕРЕЖАХ GMPLS

У сучасних мережах ASON, які організуються з урахуванням сучасних високошвидкісних технологій, особлива увага приділяється надійності та стабільності роботи, тобто потрібна наявність універсальних механізмів захисту та відновлення мереж. Ці механізми не повинні залежати від типу транспортної мережі та мають дозволяти обслуговувати з'єднання, які можуть починатися на пакетних мережах Gigabit Ethernet та проходити через кільця SDH і оптичні комутатори DWDM. При цьому використання нових сучасних технологій вимагає наявності у них характеристик, принаймні, не гірших, ніж у існуючих оптичних мережах. У зв'язку з цим у технології GMPLS розроблено низку механізмів, що дозволяють ефективно виявляти несправності та здійснювати відновлення працездатності мережі [5].

Під захистом мережі розуміється організація резервних каналів, що активізуються у разі виявлення несправності. Під відновленням працездатності мережі розуміється набір механізмів, що дозволяють розраховувати і динамічно встановлювати заново з'єднання у разі виявлення аварії. В якості механізмів захисту та відновлення працездатності мереж, що можна використовувати у технології GMPLS, проаналізуємо наступні [5]:

- місцеве відновлення (Local Repair);
- захисна комутація (Protection switching);
- швидка перемаршрутизація (Fast reroute).

2.1 Механізм захисту типу «місцеве відновлення»

Захист типу «місцеве відновлення» використовується при втраті встановленого LSP-з'єднання. Відновлюється шлях за рахунок формування нового LSP з урахуванням ситуації на мережі, що змінилася. Для формування нового LSP використовуються сигнальні протоколи GMPLS. Визначені два способи захисту, що відносяться до механізму місцевого відновлення [5]:

- відновлення LSP-з'єднання від джерела;
- відновлення LSP-з'єднання від точки виявлення пошкодження.

Перший із названих способів реалізує порядок відновлення шляху наступним чином. Комутатор LSR B, який діагностував розрив LSP-з'єднання, що проходить через нього, направляє аварійне повідомлення комутатору LSR A, що сформував це з'єднання. Отримавши аварійне повідомлення, комутатор LSR A здійснює оновлення своїх маршрутних таблиць, знаходить, за наявності такої можливості, альтернативний маршрут через комутатор LSR D і перевстановлює з'єднання, як це наведено на рис. 2.1 [5].

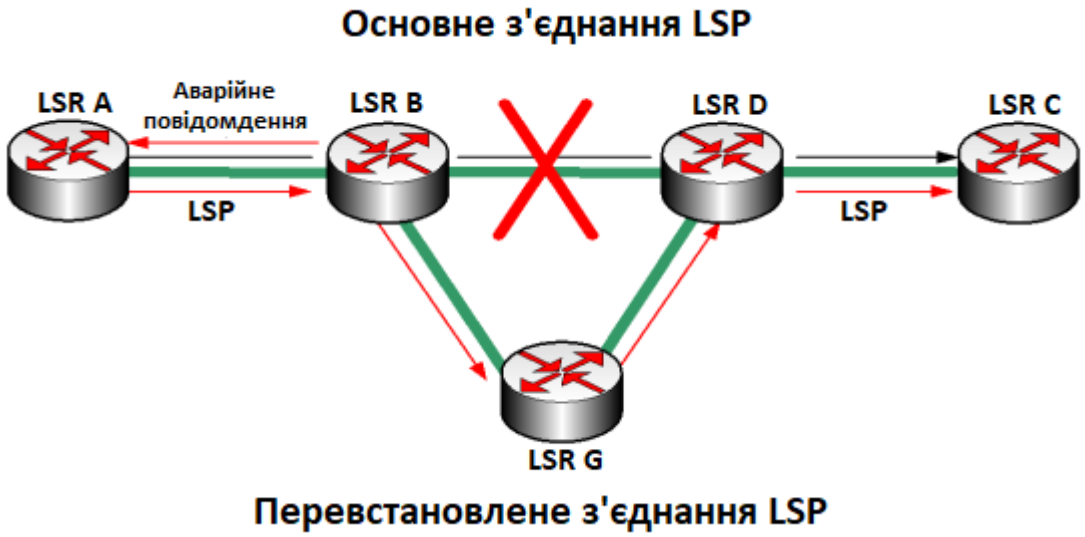

Рисунок 2.1 – Схема відновлення LSP-з'єднання від джерела

Такий спосіб місцевого відновлення є досить повільним. Зокрема, щоб сформувати нове LSP-з'єднання початковому комутатору LSR A спершу потрібно отримати аварійне повідомлення, зробити перерахунок таблиці маршрутизації (застосовуючи для цього свій протокол маршрутизації), проаналізувати нову топологію мережі і після цього вибрати оптимальний маршрут. Здійснивши всі ці кроки він може встановлювати нове з'єднання. Це все потребує багато часу, з урахування того, що кожен із перерахованих послідовних кроків може виконуватися різними протоколами [5].

Виконання механізму місцевого відновлення можна здійснювати швидше, якщо аварійне LSP-з'єднання буде відновлюватися не від джерела, як показано на рис. 2.1, а в місці виявлення пошкодження, тобто локально, як це показано на рис. 2.2. Зазначимо, що таке місце виявлення пошкодження називається точкою відновлення (Point of Local Repair, PLR) [5].

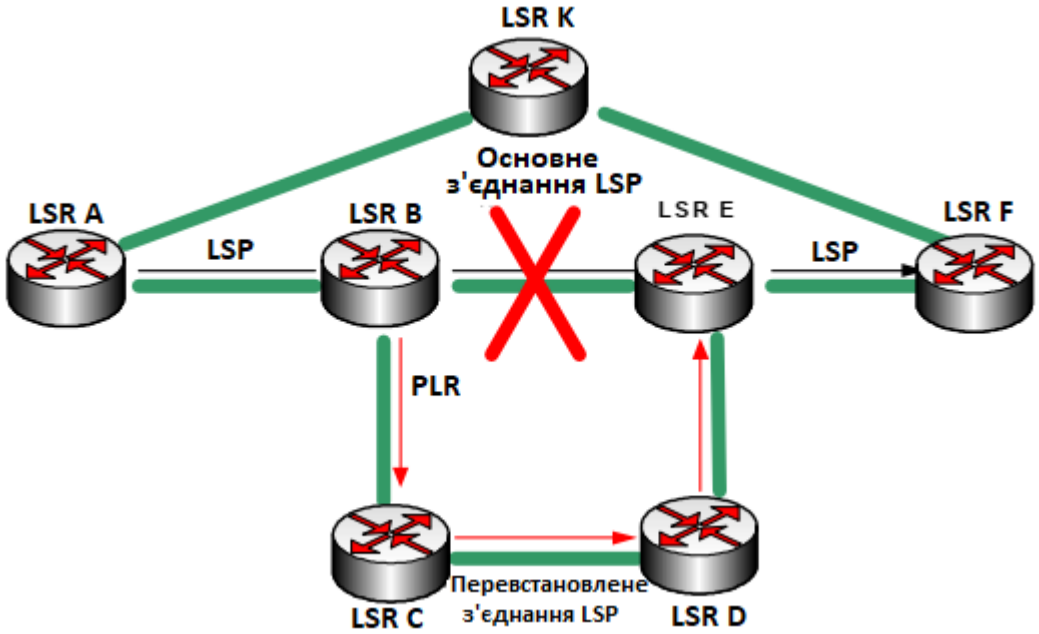

Рисунок 2.2 – Схема відновлення LSP-з'єднання в місці виявлення пошкодження

Спосіб відновлення в точці відновлення не потребує наявності додаткової сигналізації для передачі інформації про аварію до комутатора LSR A, що робить процес відновлення значно швидшим, але тут є низька недоліків [5]:

- маршрут, що обирається для перевстановлення частини LSP-з'єднання від точки PLR на комутаторі LSR B, може бути не зовсім оптимальним. Так, наприклад, оптимальним з точки зору мережі в цілому може бути маршрут від комутатора LSR A через LSR K;

- не всі сигнальні протоколи можуть функціонувати в такому режимі. Так, протокол LDP висуває вимоги щодо повернення до початкової точки, якщо буде виявлений розрив з'єднання LSP. Він не може робити відновлення аварійного LSP-з'єднання від середини. У цьому аспекті більш гнучким буде використання протоколу RSVP-TE, тому що він дозволяє адаптуватися до змін у мережній топології та перевстановлювати LSP-з'єднання, якщо відсутні необхідні ресурси або втрачений зв'язок;

- неможливість здійснення в загальній моделі управління трафіком контролю за ресурсами, що локально зайняті ділянками LSP-з'єднання, які були відновлені. Це досить серйозний недолік. Перш за все він пов'язаний з відсутністю повноцінної сигналізації з'єднання із «кінця в кінець».

Слід зазначити, що способи, які відносяться до місцевого відновлення, є досить простими в реалізації на будь-якій існуючій мережі, тому що не потребують

модифікації сигнальних протоколів і можуть використовувати наявну аварійну сигналізацію. Ці способи попередньо не резервують ресурси, що значно підвищує ефективність їх використання та мінімізує обмеження по їх застосуванню в мережах, де кількість ресурсів є обмеженою. Відмінність один від одного розглянутих способів полягає в тому – як розташуванні точки перемикання і прийняття рішення. Зокрема при використанні місцевого відновлення від точки виявлення пошкодження, трафік перемикається на LSR, який виявив аварію. Таким чином, відбувається зменшення часу реакції, тому що відсутня затримка на розповсюдження аварійної сигналізації [5].

2.2 Механізм захисту типу «захисна комутація»

В мережах GMPLS у разі використання механізму захисної комутації створюються альтернативні LSP-з'єднання для кожного напрямку, що є потенційно небезпечним. Таким чином, між кожними кінцевими LSR у разі створення LSP-з'єднання автоматично створюється резервне LSP-з'єднання, що сформоване за іншим маршрутом [5].

Застосування даного механізму дозволяє значно зменшити час відновлення мережі у разі виникнення пошкоджень, тому що для пере встановлення втраченого LSP-з'єднання треба тільки зробити перемикання основного LSP-з'єднання на резервне, що вже створено і знаходиться в гарячому резерві. Механізм типу «захисна комутація» широко використовуватися в оптичних мережах SDH, відповідно з чим стали можливими схеми, що реалізують резервування типу «1+1» або «1:1» [5].

При застосуванні резервування «1+1» формуються і є активними обидва LSP-з'єднання: основне і резервне. По ним одночасно передаються одні і ті ж дані і кінцевий комутатор GMPLS тільки приймає рішення стосовно того, дані якого LSP-з'єднання потрібно використовувати, як це наведено на рис. 2.3 [5].

Рішення, що приймається про перемикання з основного LSP-з'єднання на резервне, може ґрунтуватися на інформації про аварію і/або на цілісності даних, що надходять. Тип захисту із здійсненням резервуванням «1+1» має дуже хороші характеристики, але для нього потрібне істотне збільшення мережних ресурсів. Це робить використання цього типу захисту не досить практичним, хоча і в деяких випадках виправданим [5].

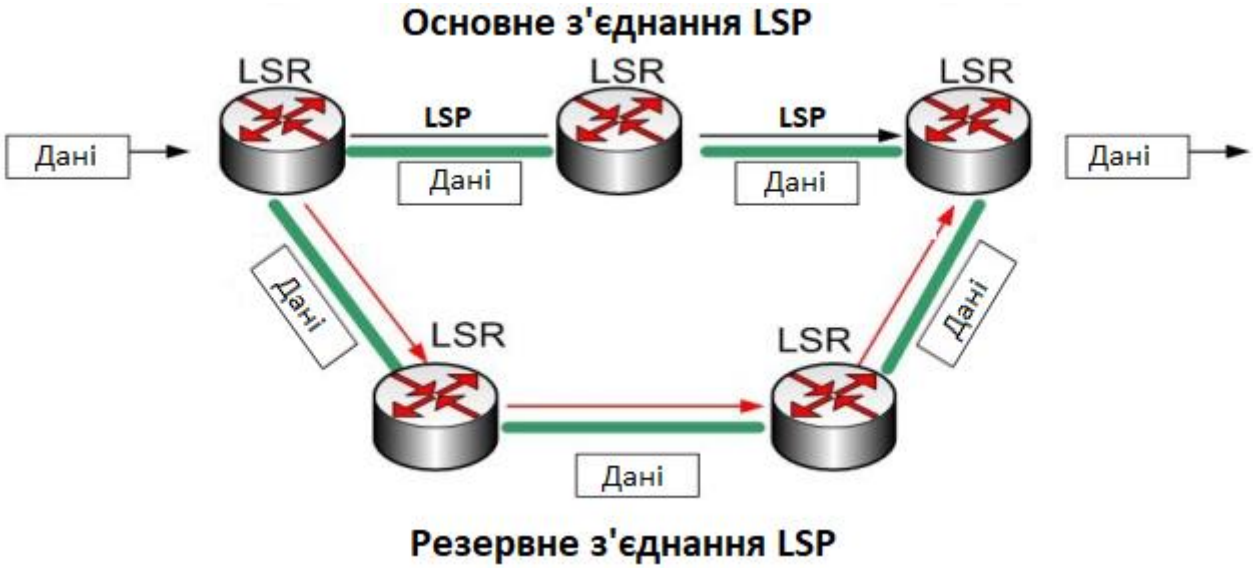

Рисунок 2.3 – Схема створення резервного LSP-з'єднання

При застосуванні резервування «1:1» також створюються два LSP-з'єднання у мережі, але резервне LSP-з'єднання тут перебуває в гарячому резерві і не використовується безпосередньо для передачі даних. Якщо буде втрачене основне LSP-з'єднання, про що мережа дізнається із аварійного повідомлення, первісний LSR зробить перемикання трафіку на зарезервоване з'єднання [5].

Можливі різні варіанти реалізації цих способів захисту, наприклад, резервне LSP-з'єднання створюється без здійснення резервування ресурсів, а у випадку перемикання на нього трафіку воно відбирає ресурси у з'єднань, що є менш пріоритетними. Також трафік LSP-з'єднання, що захищається, може перемикатися на інші LSP-з'єднання, що прямують в ту ж саму сторону, але здійснюють обслуговування менш пріоритетного трафіку. У цьому випадку трафік, що є менш пріоритетним, буде просто видалятися [5].

Перевага захисної комутації полягає в тому, що при виникненні аварійної ситуації, додаткового часу на розповсюдження сигнальних повідомлень для створення нового маршруту, не потрібно. Це робить значно швидшою роботу цього механізму захисту, але аварійні повідомлення все ж таки потрібно поширити від точки виявлення аварії до точки перемаршрутизації, яка у випадку із захисною комутацією знаходиться у початковому LSR, і на це потрібен деякий час [5].

Розглянуті вище способи захисної комутації не вимагають змін в існуючій сигналізаціїGMPLS, але потрібна стандартизація механізмів встановлення і

обслуговування резервних LSP-з'єднань. Також слід зазначити, що загалом можлива організації захисту за типом «M:N», тобто коли M LSP-з'єднань захищаються N резервними з'єднаннями. При цьому кількість N резервних з'єднань може бути більшою, дорівнювати або бути меншою за M. Захист «M:N» також не потребує модифікації існуючої сигналізації, що дещо спрощує процес його розгортання на існуючій мережі [5].

2.3 Механізм захисту за типом «швидкої перемаршрутизації»

У разі застосування даного механізму захисту та відновлення трафік GMPLS може бути перемаршрутизований без додаткової сигналізації у разі виявлення аварії. За своєю сутністю швидка перемаршрутизація є комбінуванням механізмів захисту, що були розглянуті вище, яка комбінує в собі як компоненти захисту, так і компоненти відновлення мереж після аварій [5].

В основі механізму швидкої перемаршрутизації лежать організовані попередньо альтернативні з'єднання. При цьому захист здійснюється, як правило, не все з'єднання LSP, а окремих найбільш небезпечні його трактів. При виявленні аварійної ситуації GMPLS-трафік просто робить заміну своєї мітки і продовжує просуватися за попередньо організованому резервному LSP-з'єднанню. Крім здійснення простої заміни міток також можливе застосування стека міток, що дозволяє захистити і зберегти оригінальну мітку LSP-з'єднання. Пропонується два основних способи реалізації механізму швидкої перемаршрутизації в GMPLS: захист каналу і захист вузлів [5].

Ці способи більш докладніше розглядаються нижче.

2.3.1 Захист каналу

Цей спосіб захисту є самим простим і полягає в захисті магістрального з'єднання між сусідніми LSR. Він застосовується у разі, якщо існує імовірність виникнення розриву фізичного з'єднання між двома магістральними комутаторами LSR. Попередньо для захисту каналу створюється резервне LSP-з'єднання між двома прикордонними LSR (E-LSR) через альтернативний канал. У разі виявлення розриву основного каналу, весь трафік, що передавався по ньому (у тому числі всі LSP-з'єднання), перемикається на резервне LSP-з'єднання.

Особливо треба звернути увагу на те, що пропускної здатності резервного LSP-з'єднання має бути достатньо для здійснення обслуговування всіх потоків трафіку, які перемкнули на нього. У іншому випадку, тобто коли немає у наявності необхідної кількості ресурсів, можливо здійснити перемаршрутизацію тільки для деяких потоків даних, наприклад тих, що мають найбільший пріоритет [5].

Резервне LSP-з'єднання, яке захищає канал між комутаторами LSR B і LSR C – це фактично тунель, у якому додається додаткова мітка до LSP-з'єднань, що перемикаються, тобто формується стек міток (рис. 2.4). Потрібно зазначити, що у цій схемі не потрібно створювати нові таблиці комутації міток. Тут мітка, яка згенерована комутатором LSR B на початку аварійного каналу, інкапсулюється в стек міток, а вже до неї додається додаткова мітка тунелю [5].

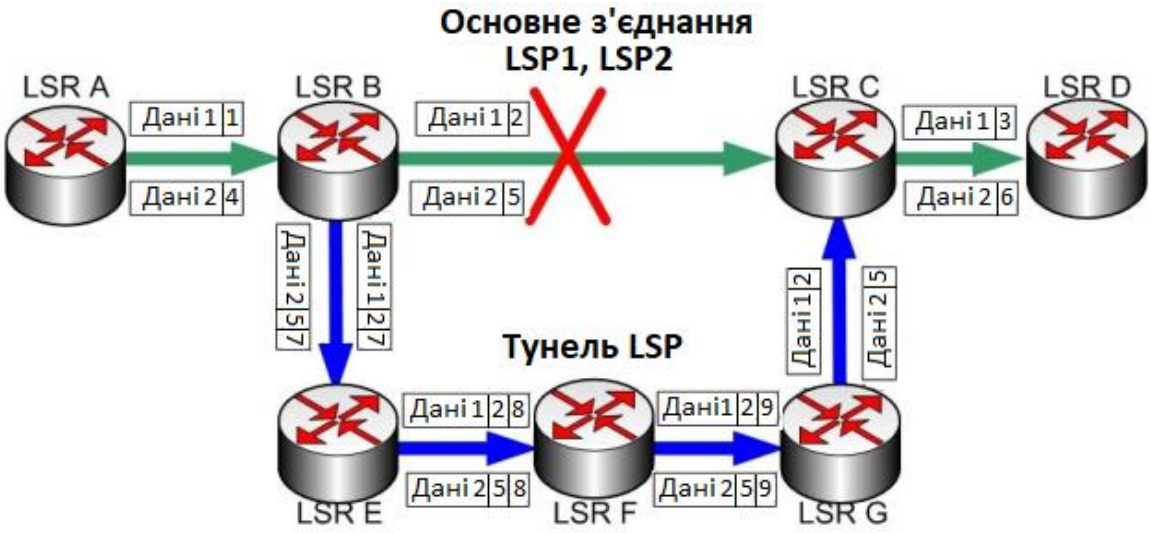

Рисунок 2.4 – Схема організації захисту каналу

У комутаторі LSR G, на якому закінчується тунель, зовнішня мітка відкидається, і на LSR C, що розташований на іншому кінці каналу, який потрібно захистити, надходить пакет з міткою, що була встановлена на вихідному кінці аварійного каналу. Комутатор LSR C не робить перерахунок таблиці комутації, а досить просто передає пакет далі у відповідності до наявних поточних таблиць [5].

Потрібно звернути увагу на те, що комутація трафіку в GMPLS здійснюється на основі пар компонентів: «вхідний інтерфейс-мітка» та «вихідний інтерфейс/мітка». Тут змінюється номер вхідного інтерфейсу, навіть не зважаючи на те, що мітка у разі застосування цього способу захисту залишається незмінною. Пропонується два можливі підходи для вирішення цієї проблеми. По-перше, можна

використовувати додаткові таблиці відповідностей між цими інтерфейсами, що досить складно і незручно. По-друге, можна використовувати так званий Глобальний Розподіл Міток, у разі застосування якого унікальні мітки встановлюються не на кожен інтерфейс комутатора LSR, а на весь комутатор. Тобто LSR буде неважливо, з якого інтерфейсу надходить пакет – він просто здійснює обробку пакету відповідно до мітки, що надійшла [5].

Простота способу захисту каналу полягає в тому, що він може захистити тільки з'єднання між двома сусідніми комутаторами GMPLS і не є працездатним у тих випадках, коли виходять з ладу кілька послідовно включених каналів або повністю комутатор LSR [5].

2.3.2 Захист вузлів

Цей спосіб використовується механізмом швидкої перемаршрутизації в GMPLS для захисту від втрати комутаторів. Він є аналогічним щодо способу захисту каналів і полягає у організації резервного LSP-з'єднання в обхід зарезервованого комутатора GMPLS. У разі виявлення аварії зарезервованого комутатора LSR, трафік перемикається на резервне LSP-з'єднання. Далі все функціонує так само, як і у разі використання способу захисту каналу, але за одним винятком. Мітка, яка встановлюється крайнім комутатором LSR B на вході у резервний тунель LSP, являє собою мітку для транзитного зарезервованого комутатора LSR C, але не для LSR D, що розташований в кінці тунелю. Тому, коли такий трафік вийде з резервного LSP-тунелю, то цей кінцевий комутатор LSR D не зможе сформувати для нього правильний маршрут [5].

Вирішення цієї проблеми ґрунтується на використанні певного сигнального протоколу, в обов’язки якого буде входити інформування комутатора в точці відновлення LSR B про значення мітки, яку очікує комутатор LSR D. Наприклад, можна в якості такого протоколу задіяти протокол резервування ресурсів (Resource Reservation Protocol, RSVP) для управління трафіком в процесі передачі (Traffic Engineering, TE), тобто протокол RSVP-TE. Цей протокол обробляє розподіл пропускної здатності та здійснює управління трафіком по всій GMPLS мережі. Протокол RSVP-TE дозволяє створювати основний і запасний LSP, резервувати ресурси на всіх вузлах, виявляти аварії на мережі, заздалегідь будувати обхідні шляхи, здійснювати швидке перенаправлення трафіку, уникати каналів, які фізично проходять по одному шляху. Об'єкт запису маршруту (Route

Record Object, RRO) протоколу RSVP-TE володіє інформацією про всі транзитні комутатори на шляху LSP-з'єднання, а також про мітки, що були використані, як це видно із рис. 2.5 [5, 16].

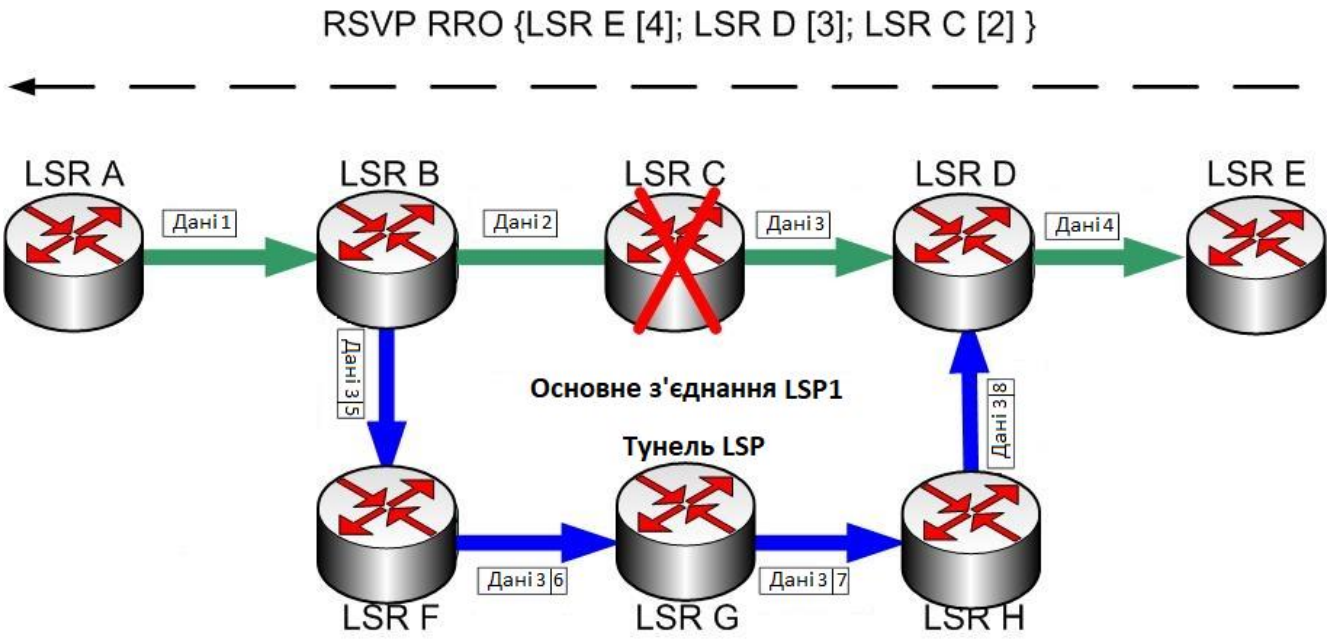

Рисунок 2.5 – Схема організації захисту вузла

Зокрема на рис. 2.5 можна бачити, що мітка 3, яка мала б бути використана аварійним комутатором LSR C для комутатора LSR D, встановлюється на комутаторі LSR B у пакет перед здійсненням його тунелювання по резервному LSP-з'єднанню. Тим самим забезпечується надходження трафіку з правильною міткою на LSR D, а застосування Глобального Розподілу Міток вирішує проблему появи трафіку на іншому інтерфейсі [5].

Способи швидкої перемаршрутізації повністю базуються на власній сигналізації, але фактично являють собою інтеграцією механізмів захисної комутації і місцевого відновлення. Сигналізація забезпечує можливості як аварійної сигналізації для розповсюдження аварійних повідомлень, так і сигналізації для організації резервних LSP-з'єднань. Крім того сигналізація забезпечує деяку модифікацію протоколів внутрішньої маршрутизації для забезпечення мінімального часу організації резервного LSP-з'єднання за альтернативним маршрутом, що у свою чергу дозволяє гарантувати потрібний рівень QoS [5].

При цьому перший спосіб (захист каналу), що полягає в організації захисту одного з'єднання LSP, в стандарті IETF носить назву «об'їзду». Він дозволяє не витрачати час на розповсюдження аварійної сигналізації, тому що канал, який захищається, напряму підключений до точки перемикання. Другий спосіб, що полягає в організації захисту вузла та всіх з'єднань, що проходять через цей вузол, у стандарті IETF носить назву «обходу». Він надає можливість відновлювати з'єднання при втраті одного чи декількох вузлів і відповідно кількох каналів, що потребує розповсюдження аварійної сигналізації починаючи від місця аварії і до точки перемикання PLR. На це може витрачатися деякий час [5].

Обидва способи швидкої перемаршрутізації можуть робити попереднє резервування ресурсів з використанням схеми «M:N», що робить застосування цих способів гнучким і задовольняє більшості вимог мереж на базі технології GMPLS.

Із вищевикладеного є очевидним, що найбільш швидкісними методами захисту є ті, в яких вдається мінімізувати час передачі і кількість сигнальних повідомлень. Основні затримки, які пов'язані з сигналізацією, складаються з [5]:

– часу, який потрібний для виявлення несправності в точці перемикання, тобто часу розповсюдження аварійного повідомлення від місця аварії до точки перемикання;

– часу, який потрібний на організацію нового LSP-з'єднання для відновлення функціоналу розірваних з'єднань.

У зв'язку з цим методи, що здійснюють перемикання від точки виявлення несправності PLR і застосовують заздалегідь встановлені резервні LSP-з'єднання, мають найбільшу перевагу [5].

До них відносяться способи, що реалізують механізм швидкої перемаршрутизації. Зокрема, спосіб організації «об'їзду» майже не потрібно ніякого часу на здійснення перемикання трафіку на резервне LSP-з'єднання. Виняток можуть бути ті випадки, коли треба зробити одночасне перемикання великої кількості LSP-з'єднань. Наприклад, у випадках застосування схем захисту «M:N», у яких кількість зарезервованих ресурсів заздалегідь є меншою за необхідну. В цьому випадку комутатору у точці PLR потрібен деякий час, щоб визначити, які LSP-з'єднання є найбільш пріоритетними і тому вимагають перемаршрутизації в першу чергу [5].

Таким чином, серед проаналізованих у даному розділі кваліфікаційної роботи механізмів захисту і відновлення мереж GMPLS від аварій найбільш ефективними є способи швидкої перемаршрутизації, які дозволяють забезпечити відновлення мережі за час, що не перевищує 50 мс [5].

Застосування цих способів захисту в GMPLS дозволить уніфікувати складову, що відповідає за здійснення управління OTN, а це у свою чергу сприятиме широкому впровадженню та розповсюдженню технології GMPLS, в якості єдиного стандарту організації системи сигналізації для сучасних високошвидкісних технологій мереж ASON.

3 АНАЛІЗ МЕХАНІЗМІВ БАГАТОРІВНЕВОГО ЗАХИСТУ GMPLS

3.1 Особливості та принципи організації динамічного багаторівневого захисту

Для розробки механізму управління відмовами в мережі GMPLS пропонується застосування методу багаторівневого захисту, в якому реалізується управління декількома захисними системами, кожна з яких організовує різні рівні захисту, залежно від типу класу трафіку. Отже сценарій багаторівневого захисту динамічно встановлюється із використанням основних особливостей підходів по забезпеченню маршрутизації в мережі з QoS в реальному масштабі часу [17].

У випадку мережі з високими вимогами щодо захисту, застосування багаторівневого управління відмовами може збільшити продуктивність у порівнянні з однорівневим управлінням. Тим не менш, її структурна організація та забезпечення управління буде значно складнішим і дорожчим (у термінах часу та ресурсів), таким чином, кращим виходом буде застосування компромісного сценарію. Так, наприклад, організація захисту шляхом організації резервного шляху у разі виходу з ладу робочого шляху – може забезпечуватися по глобальному шляху захисту (Global Recovery Path, GRP). У разі необхідності підвищення вимог захисту в мережі, наприклад, якийсь із трактів GRP також вийшов з ладу, може бути встановлений новий – локальний шлях захисту (Local Recovery Path, LRP), що, у свою чергу, забезпечить новий захисний рівень (рис. 3.1) [17].

Таким чином, переваги використання такого підходу багаторівневого захисту реалізується у сценаріях із множинними відмовами. На рис. 3.1(а) показаний приклад, у якому основний (робочий) шлях передачі трафіку (Working Path, WP) представляє послідовність маршрутизаторів: LSR1, LSR3, LSR5, LSR6. Якщо тракт (або вузол) LSR3-LSR5 основного шляху виходить з ладу, то трафік буде передаватися захисним шляхом GRP, який представлений маршрутизаторами: LSR1, LSR2, LSR4, LSR6. У випадку множинних відмов, тобто, якщо вийшли з ладу тракт (або вузол) LSR3-LSR5 шляху WP та тракт (або вузол) LSR1-LSR2 шляху GRP, то для доставки трафіку буде задіяний шлях LRP, що реалізується маршрутизаторами LSR1, LSR3, LSR4, LSR6 і, який дозволить обійти несправні сегменти.

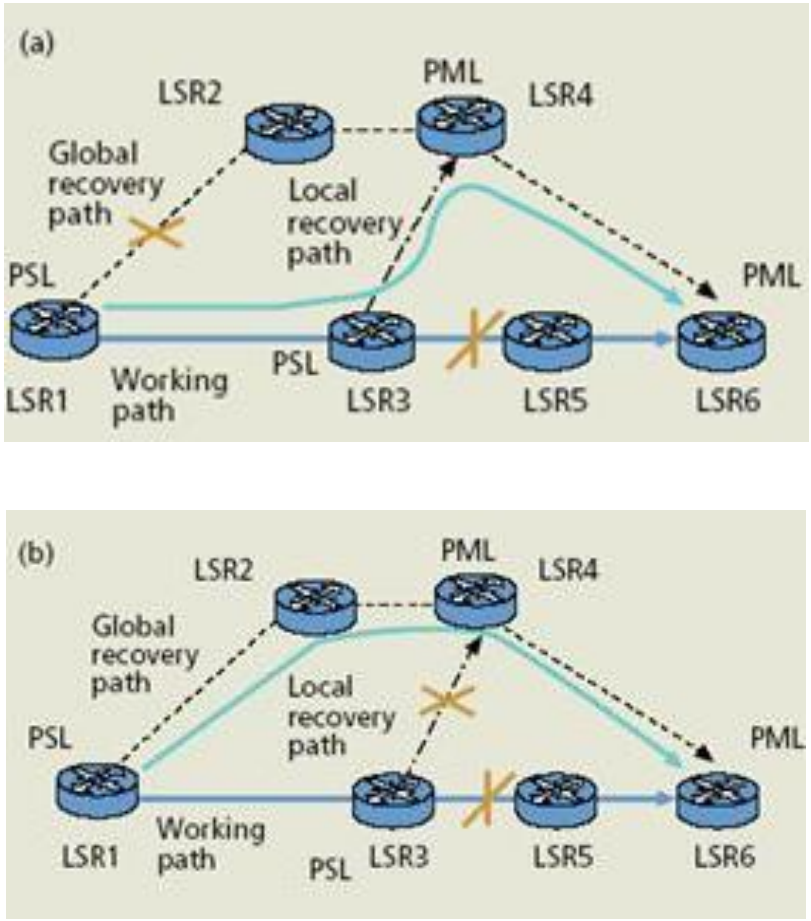

Рисунок 3.1 – Сценарії реалізації багаторівневого захисту у мережі GMPLS

Ще один можливий приклад застосування багаторівневого захисту наведений на рис. 3.1(б). Тут так само, як і в попередньому випадку, вважатимемо, що вийшов з ладу тракт (або вузол) LSR3-LSR5 основного шляху WP (LSR1, LSR3, LSR5, LSR6). В даному випадку спочатку використовується шлях LRP (LSR3, LSR4, LSR6). Однак надалі, якщо, наприклад, тракт (або вузол) LSR3-LSR4, що відносяться до захисного шляху LRP, виявляться несправними, то буде використаний глобальний захисний шлях резервування GRP для передачі трафіку і подолання відмов, що виникли.

Слід зазначити, тракти (шляхи) GRP, LRP, WP, що аналізуються, на рис. 3.1 і далі, фактично являють собою LSP, які умовно поділені за рівнем реалізації багаторівневого захисту у мережі GMPLS на: глобальний, локальний і основний (робочий) тракти [17].

3.2 Маршрутизація із забезпеченням якості обслуговування в реальному масштабі часу та підтримкою багаторівневого захисту

Основною задачею будь-якого алгоритму маршрутизації є пошук відповідного шляху (шляху з достатньою пропускною здатністю), який забезпечує ефективне використання ресурсів. Крім того, маршрути, які вибираються з використанням маршрутизації з QoS, повинні мати достатні ресурси для вимог якості обслуговування, що запитуються. Маршрутизація з QoS використовує дві різні цільові функції для оптимізації мережної продуктивності: найкоротший тракт має бути обраний для мінімізації часових втрат, а мінімально завантажений тракт має бути обраний для розподілу навантаження [18].

Існує чіткий взаємозв'язок між маршрутизацією із забезпеченням QoS у реальному масштабі часу та захисними механізмами мережі GMPLS. Механізми захисту впливають на маршрутизацію, пропонуючи різні шляхи та нові тракти LSP для її здійснення з урахуванням забезпечення необхідних вимог QoS. Зокрема для швидкого надання захисних механізмів потрібно заздалегідь маршрутизувати резервний тракт LSP. Тим не менш, топологічні зміни або вимоги нових ресурсів змушує LSR у реальній мережі вибирати нові робочі та резервні LSP. Резервні LSP мають бути встановлені статично (з використанням засобів явної маршрутизації), але така ситуація може призвести до неефективного використання ресурсів. Отже, алгоритми маршрутизації, що працюють у реальному масштабі часу, мають застосовуватися для встановлення нових трактів LSP [19].

У разі застосування на мережі механізмів багаторівневого захисту використання маршрутизації в реальному масштабі часу більш очевидне. Різні рівні такого захисту використовують динамічну маршрутизацію для організації резервних трактів різних типів в різні проміжки часу. Тим не менш, шляхи відновлення можуть бути створені від вузла, що реалізує перемикання шляхів, так званий комутатор шляху (Path Switch LSR, PSL) до вузла, що забезпечує об'єднання шляхів (Path Merge LSR, PML). Таким чином, існуючі маршрутні алгоритми можуть бути покращені у схемі багаторівневого захисту за допомогою розгляду не лише вузлів «вхід-вихід», але також усіх можливих вузлів PSL/PML. На рис. 3.2 представлена типова схема організації багаторівневого захисту GMPLS. Відповідно у таблиці 3.1, наведені призначення локальних (LRP) та глобальних (GRP) шляхів захисту (відновлення) [17].

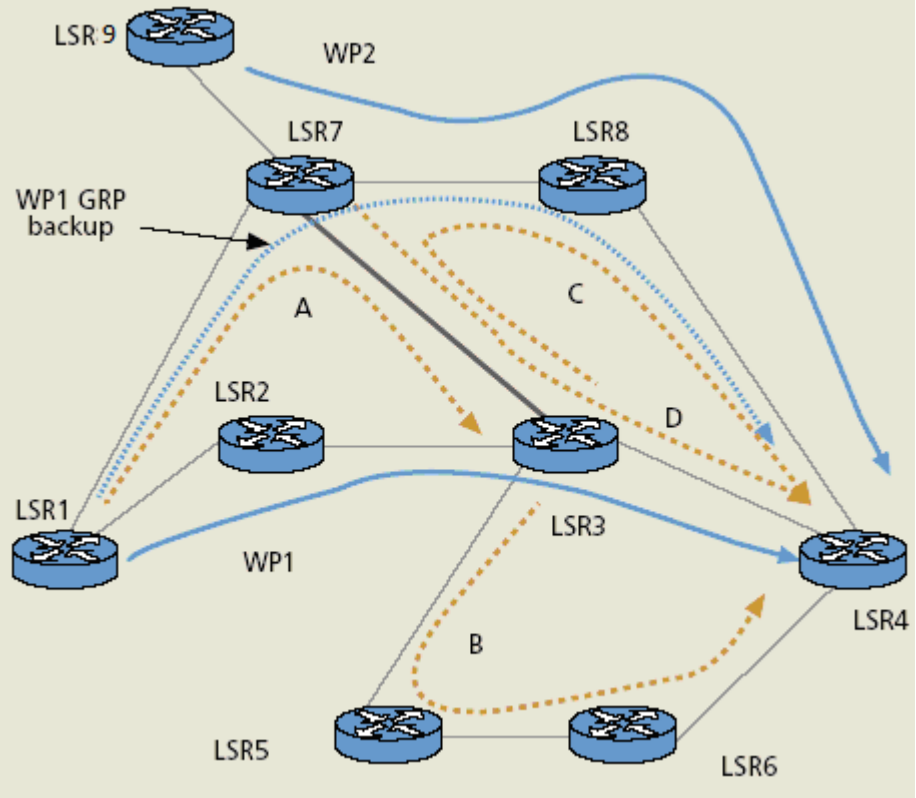

Рисунок 3.2 – Типова схема організації багаторівневого захисту GMPLS

Таблиця 3.1 – Призначення шляхів відновлення

Working path	Elements links and nodes	Recovery path
	(1-2)	LRP A (1-7-3)
	LSR2	
WP1	(2-3)	
	LSR3	WP1 GRP (1-7-8-4)
	(3-4)	LRP B (3-5-6-4) LRP C (3-7-8-4)
	(9-7)	None
	LSR7	
WP2	(7-8)	
	LSR8	LRP D (7-3-4)
	(8-4)	

Припустимо (див. рис. 3.2 та табл. 3.1), що в мережі GMPLS організовані два робочі шляхи LSP – WP1 та WP2, для яких необхідно забезпечити захист. Якщо шлях WP1, який проходить через маршрутизатори LSR1, LSR2, LSR3,

LSR4, був первісно організований, то алгоритм маршрутизації може вибрати резервний (backup) шлях GRP, який організований маршрутизаторами LSR1, LSR7, LSR8, LSR4. А шлях WP2, що охоплює маршрутизатори LSR9, LSR7, LSR8, LSR4 не може бути організований, тому що для нього не можна знайти резервний шлях. Причина полягає в тому, що різні маршрутні алгоритми в реальному масштабі часу не дозволяють резервним і робочим шляхам спільно використовувати будь-який сегмент LSP, а в даному випадку сегмент, організований маршрутизаторами LSR9-LSR7, є єдиним шляхом для досягнення маршрутизатора LSR9. У разі використання механізмів багаторівневого захисту жоден глобальний резервний шлях GRP не може бути маршрутизованим для робочого шляху WP2, але основна частина його трактів та вузлів може бути захищена, з використанням локальних резервних шляхів відновлення [17].

Так із рис. 3.2 та таблиці 3.1 можна бачити, що тракт, який утворений маршрутизаторами LSR3-LSR4, має подвійний захист локальними резервними шляхами LRP B (LSR3, LSR5, LSR6, LSR4) і LRP C (LSR3, LSR7, LSR8, LSR4). Зазначимо також, що пропускна здатність може бути розділена між локальними резервними шляхами LRP A (LSR1, LSR7, LSR3) та LRP D (LSR7, LSR3, LSR4) в тракті LSR7-LSR3. Цей новий сценарій для повного захисту відкриває велику кількість можливих рішень для захисту шляхів. Проте повне відновлення може призвести до надмірного споживання мережних ресурсів. Тоді слід запропонувати обмежити захист на основі класу типу трафіку та ненадійності тракту. Ці обмеження будуть використовуватись для відповідного покращення динамічних маршрутних алгоритмів з QoS [17].

Іншим аспектом збільшення ефективності маршрутизації з QoS є використання концепції класів трафіку для аналізу ймовірності та/або чутливості різних типів трафіку у разі відмов з урахуванням різних параметрів, таких як: втрати пакетів, затримки на відновлення тощо. Тобто маршрутний алгоритм може працювати по різному залежно від типу трафіку. Наприклад, якщо WP1 має більш високий пріоритет захисту, ніж WP2, то можливо маршрутний алгоритм намагатиметься знайти всі можливі локальні резервні шляхи для WP1 (резервні шляхи A, B, C на рис. 3.2) [17].

Пропонуються різні механізми організації відповідних схем захисту залежно від класу трафіку. У цій роботі акцент робиться на застосування сценарію диференційованого обслуговування (Differentiated Service, DiffServ), у якому визначено чотири класу трафіку (див. табл. 3.2) [20]:

- клас термінової передачі (Expedited Forwarding, EF) для транспортування трафіку у реальному масштабі часу;

- два типи гарантованої передачі (AF1 і AF2) використовуються трафіком з двома різними різновидами втрат;

- клас негарантованої доставки для трафіку без вимог QoS (Best Effort, BE).

Таблиця 3.2 – Стратегії захисту для класів трафіку DiffServ

Traffic class	QoS requirements	Protection domain	LSP setup	Resource allocation	Bandwidth
EF	Real-time	Local recovery	Pre-established	Prereserved	Equivalent
AF1	Very low losses	Reverse recovery	Pre-established	Reserved on demand	Equivalent
AF2	Low losses	Global/local	On demand	Reserved on demand	Limited
BE	No requirements	Global/local	On demand	Reserved on demand	Limited

Відповідно до вимог QoS, у таблиці 3.2 представлені різні стратегії захисту. Локальне відновлення захисту (Local recovery) призначається класу трафіку EF відповідно з обмеженням часу відновлення, яке має бути менше трафіку в реальному масштабі часу (Real-time). У випадку передачі трафіку AF1 вимогою QoS є досягнення дуже низьких втрат (Very low losses). Область захисту класів трафіку AF2 і BE може бути глобальною чи локальної (Global/local), в залежності від надійності [17, 20].

Наступні три колонки: установка LSP (LSP setup), розподіл ресурсів (Resource allocation) та смуга пропускання (Bandwidth) – є необхідними параметрами захисту та відновлення. Установка LSP стосується ініціалізації установки відновлення: у разі попередньої установки, шлях відновлення організується перш, ніж буде відмова тракту; у разі установки LSP за запитом, шлях відновлення організується після виникнення відмови. Схема попередньої установки швидша і, отже, підходить для класів трафіку EF та AF1. Розподіл ресурсів (наступна колонка в табл. 3.2) показує, як розподіляються мережні ресурси (як правило, мається на увазі смуга пропускання) по LSP до виникнення відмови (тобто здійснюється попереднє резервування (Prereserved)) або після виникнення відмови, тобто LSP може бути організований без розподілу смуги пропускання з можливістю резервування за запитом (Reserved on demand). Як показано в останній колонці таблиці 3.2 (Bandwidth), існують дві стратегії розподілу смуги пропускання тракту LSP: еквівалентний (Equivalent) розподіл

(однаково з робочим трактом) або обмежений (Limited) розподіл (тобто виділяється менша смуга, ніж робочий шлях) . Для EF та AF1 розподіляється еквівалентна смуга пропускання, що не позначається на погіршенні якості обслуговування. Розглянуті стратегії та параметри захисту можуть бути об'єднані в одну характеристику, під назвою «рівень ефективності захисту» (Performance Level, PL) [17, 20].

Таким чином, у цьому розділі ми проаналізували два важливі аспекти забезпечення працездатності мереж GMPLS, що пов'язані з організацією та управлінням динамічним багаторівневим захистом, а також маршрутизацією в реальному масштабі часу за допомогою необхідних параметрів QoS. Крім того, в процесі проведеного аналізу показана важливість спільного використання багаторівневого захисту GMPLS з маршрутизацією такого типу. Також показано, що для зменшення ймовірності відмов та збільшення використання ресурсів організація нових LSP залежить від маршрутизації з QoS у реальному масштабі часу. Зокрема варіант захисту та відновлення GMPLS передбачає організацію резервних LSP. Резервні шляхи можуть бути маршрутизовані різними способами залежно від рівня захисту. Якщо розглядається динамічне середовище та параметри QoS, то одночасно повинні застосовуватися управління відмовами GMPLS та алгоритми маршрутизації з QoS у реальному масштабі часу. Розглянута типова схема для організації багаторівневого захисту GMPLS (з різними типами резервних шляхів LSP).

4 ІМІТАЦІЙНЕ МОДЕЛЮВАННЯ МЕРЕЖІ GMPLS ТА ТИПОВИЙ РОЗРАХУНОК ПАРАМЕТРІВ ТРАФІКУ

4.1 Імітаційна модель маршрутизації трафіка в мережі GMPLS

Для моделювання мереж GMPLS було використано систему моделювання мережної архітектурно-топологічної структури NetCracker. Імітаційні блоки, що реалізують функції пристроїв та елементів MPLS, поєднуються у мережу з використанням графічного інтерфейсу. Функціонування системи демонструється на прикладі моделювання мережі GMPLS, що передає інформацію по паралельні маршрути [14].

На рис. 4.1 показано схему маршрутизації трафіку в GMPLS по чотирьох шляхах LSP [14].

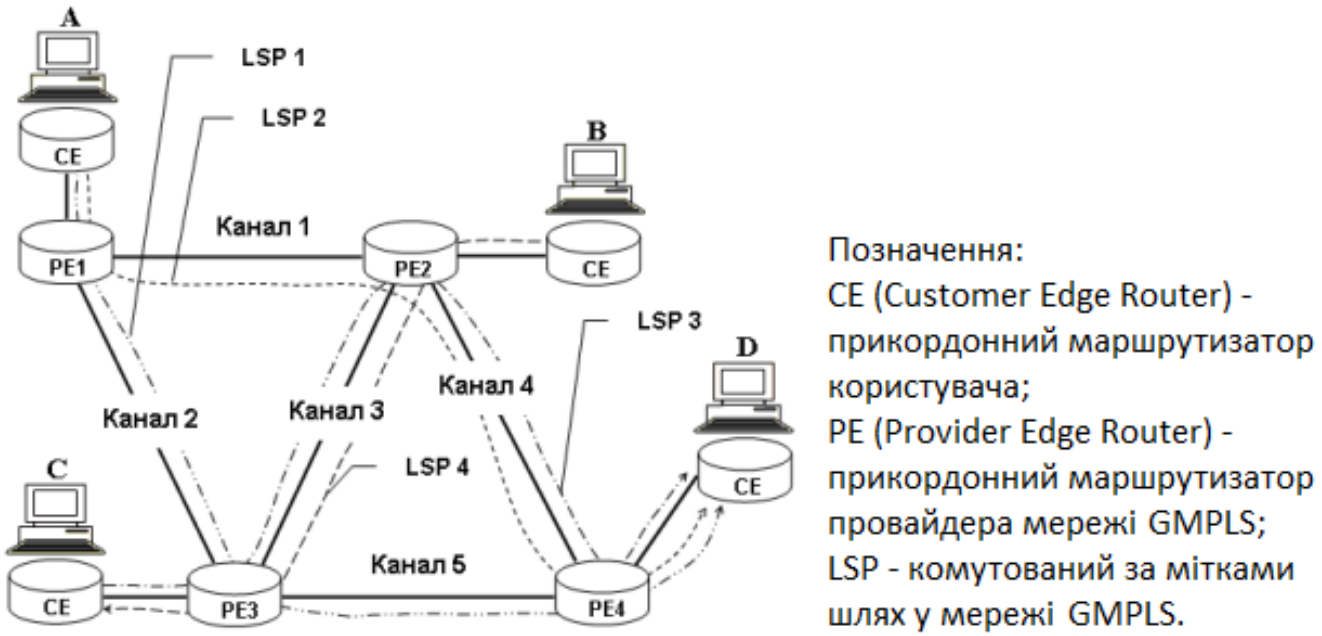

Рисунок 4.1 – Схема здійснення маршрутизації трафіку в GMPLS

Будемо досліджувати тракт передачі пакетів від абонента A до абонента D. Для маршрутизації пакетів у маршрутних таблицях прописані наступні LSP-шляхи [14]:

- шлях 1: Користувач A - PE1 - Канал 2 - PE3 - Канал 5 - PE4 - Користувач D;
- шлях 2: Користувач A - PE1 - Канал 1 - PE2 - Канал 4 - PE4 - Користувач D;
- шлях 3: Користувач C - PE3 - Канал 3 - PE2 - Канал 4 - PE4 - Користувач D;
- шлях 4: Користувач B - PE2 - Канал 3 - PE3 - Користувач C.

Маршрутизатори PE мають загальну вхідну чергу, яка переповнюється у разі збільшення трафіку, що надходить з різних напрямків. Передача пакетів від інших абонентів відбивається на затримках передачі пакетів для Користувача А. Задачею моделювання процесу є оцінка швидкодії GMPLS під час передачі пакетів від Користувача А до Користувача D у випадках:

а) використання лише одного LSP1;

б) передачі пакетів послідовно, використовуючи різні шляхи LSP.

Моделювання з використанням програмного пакета NetCracker проводилося за таких припущень: Користувачі А, В, С генерують по 100 пакетів. Користувач А генерує пакети з інтервалом 3 мкс. Пакети від Користувача А мають адресу призначення Користувача D. Пакети від Користувача В мають адресу від Користувача С і генеруються з інтервалом в 10 мкс. Користувач С генерує пакети з адресою призначення Користувача D через кожні 10 мкс. Результати цього моделювання наведено у таблицях 4.1 - 4.2 та на рис. 4.2 - 4.4 та [14].

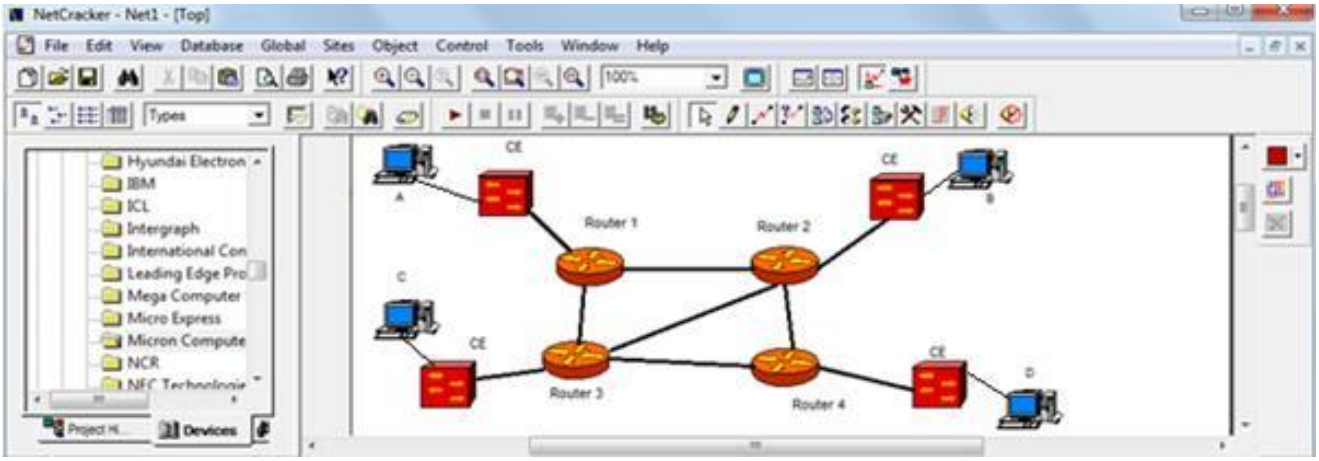

Рисунок 4.2 – Вікно моделювання мережі GMPLS в програмному пакеті NetCracker

Таблиця 4.1 – Результати, що отримані при моделюванні довжини черги у разі використання одного LSP

Час, мкс	0	50	100	150	200	250	300	350	400	450	500	550	600	650	700
Довжина черги, пакет	0	0	2	7	12	15	16	20	28	33	34	40	46	51	53

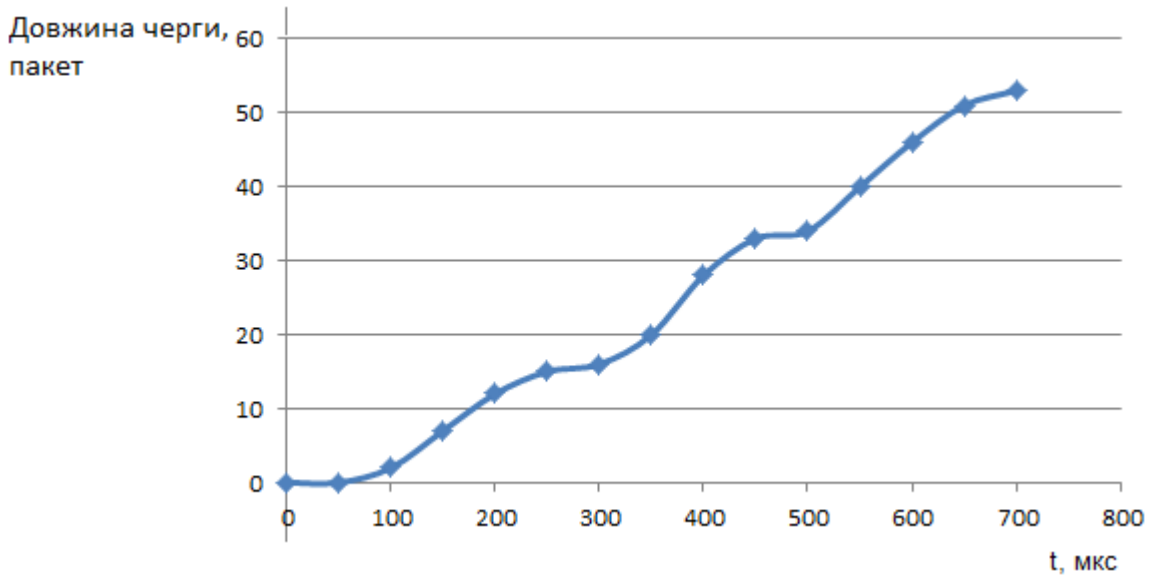

Рисунок 4.3 – Графічна залежність за отриманими результатами моделювання довжини черги у разі використання одного LSP

Таблиця 4.2 – Результати, що отримані при моделюванні довжини черги у разі використання двох LSP

Час, мкс	0	25	50	75	100	125	150	175	200	225	250	275	300	325	350	375
Довжина черги, пакет	0	3	0	5	7	12	9	5	8	3	4	3	2	1	3	10

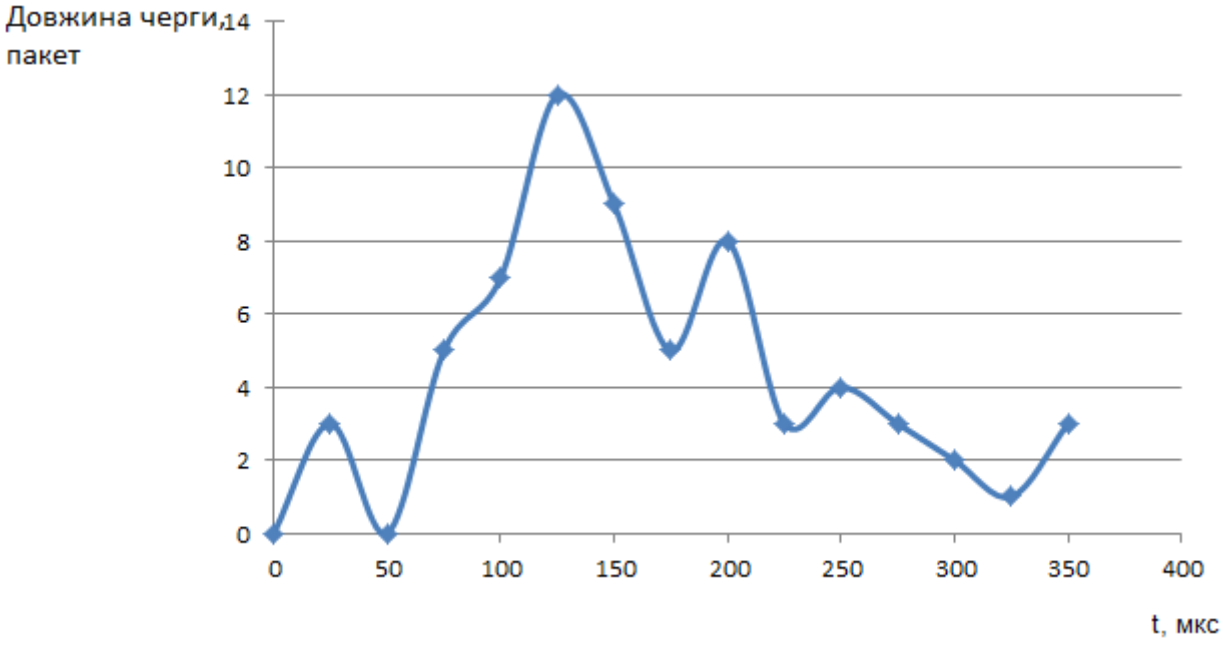

Рисунок 4.4 – Графічна залежність за отриманими результатами моделювання довжини черги у разі використання двох LSP

З результатів імітаційного моделювання видно, що навантаження, яке створюється трафіком на мережу з використанням одного LSP, перевищує навантаження, яке створюється трафіком на мережу з використанням двох LSP. При досягненні обсягу трафіку певної критичної точки відбувається невелике перенавантаження, що відбивається на продуктивності. Якщо така ситуація відбувається в лінійному режимі, це не призведе до великих проблем. Однак у пікові значення часу, коли трафік у мережі досягає певного рівня, пропускна здатність сильно зменшиться у відповідності до серйозності навантаження та збільшення числа пакетів у черзі на вхідних інтерфейсах маршрутизаторів. Щоб уникнути цього, можна використовувати два LSP. Другий LSP, крім того, можна використовувати як резервний шлях у разі можливої відмови першого на основі механізму перемаршрутизації. Окрім того, що механізм швидкої перемаршрутизації зможе забезпечити додаткову надійність при передачі трафіку, він також є дуже добре масштабованим рішенням, оскільки всі LSP, що проходять через пошкоджений тракт, можуть бути зведені в один резервний тунель, який створюється з урахуванням тих же обмежень, що і при розрахунку захищених LSP.

4.2 Типовий розрахунок параметрів трафіка в мережі GMPLS

В якості фізичної мережі, на базі якої було здійснене розгортання GMPLS взята оптична мережа, яка організована відповідно до технології Gigabit Ethernet (GE). Міжкадровий інтервал (Inter Packet Gap, IPG) для GE становитиме 0,096 мкс. Під час проведення розрахунку враховується час кадру, що переведене у надмірну інформацію. Швидкість фізичного середовища GE становить 1 Гбіт/с (тобто B_t = 1073741824 біт/с). Окремо потрібно зазначити, що ми звикли вважати 1 Гбіт рівним 1000000000 біт, проте комп'ютери використовують двійкову систему обчислення (у якій числа представляються ступенями числа 2), а не десятичну, як люди у повсякденному житті. Тому, в двійковій системі обчислення, 1 Гбіт дорівнює 230 біт (тобто 1024 · 1024 · 1024 біт), що дорівнює 1073741824 біт. Таким чином, якщо IPG подати в бітах або байтах для того, щоб зв'язати з кадром GE, то отримаємо [6]:

$$IPG = B_t \cdot 0{,}096 \cdot 10^{-6} = 1073741824 \cdot 0{,}096 \cdot 10^{-6} \approx 103 \text{ біт або 13 байт.} \quad (4.1)$$

Максимальний розмір пакета дорівнює 1526 байт з урахуванням кількості корисних даних (Maximum Segment Size, MSS). У кадрі GE 18 байт займає службова інформація (заголовок GE), та 8 байт складає преамбула [6].

Максимальний розмір кадру GE у каналі (Maximum Transmission Unit, MTU) з урахуванням міжкадрового інтервалу розраховується за формулою [21]:

$$MTU = 1526 + IPG = 1539 \text{ байт.} \quad (4.2)$$

Частка інформації користувача відносно інформації в кадрі, який сформований за технологією GE, розраховується за формулою [6, 21]:

$$\gamma_{GE} = (1526 - 18 - 8)/MTU = 1500/1539 = 0{,}975. \quad (4.3)$$

Далі необхідно зарезервувати місце для міток GMPLS ($N_{міт}$) та заголовка TCP/IP ($N_{заг}$). Будемо використовувати стек із двох міток по 32 біти ($N_{міт}$ = (2·32)/8 = 8 байт), де верхня мітка визначає маршрут проходження, а нижня використовується для вибору необхідної мережі VPN. Заголовок TCP/IP займає по 20 байт, як для протоколу IP, так і протоколу TCP ($N_{заг}$ = 2·20 = 40 байт) [6, 21].

Отже, кількість корисних даних в оптичній мережі GE з використанням технології GMPLS визначимо за формулою [21]:

$$MSS = 1526 - 18 - 8 - 2 \cdot 4 - 2 \cdot 20 = 1452 \text{ байти.} \quad (4.4)$$

Таким чином, кадр GE, що передається по фізичних сегментах мережі з урахуванням використання GMPLS, буде включати наступні елементи (табл. 4.3) [6].

Максимальна пропускна здатність, у разі ідеальних умов для даних користувача ($C_П$), дорівнюватиме [21]:

$$C_П = \frac{MSS}{MTU} \cdot B_t, \quad (4.5)$$

$$C_П = \frac{1452}{1539} \cdot 1073741824 = 966{,}1 \text{ Мбіт/с.}$$

Таблиця 4.3 – Складові кадру технології Gigabit Ethernet

Преамбула	8 байт
Заголовок Gigabit Ethernet	18 байт
Стек із двох міток	8 байт
Заголовок IP	20 байт
Заголовок TCP	20 байт
Міжкадровий інтервал (IPG)	13 байт

Частка інформації з урахуванням інформації пакету GMPLS розраховується за формулою [21]:

$$\gamma_{GMPLS-CE} = MSS/MTU \ , \tag{4.6}$$

$$\gamma_{GMPLS-CE} = \frac{1452}{1539} = 0{,}943.$$

Визначимо кількість MTU-пакетів, що передається:

$$P = \frac{B_t}{8 \cdot MTU}, \tag{4.7}$$

$$P = \frac{1073741824}{8 \cdot 1539} = 87211 \text{ пакетів/с.}$$

Розрахуємо затримку MTU-пакета ($T_П$) [21]:

$$T_{\text{П}} = \frac{8 \cdot MTU}{B_t}, \tag{4.8}$$

$$T_{\text{П}} = \frac{8 \cdot 1539}{1073741824} = 11{,}5 \text{ мкс.}$$

При розрахунках не враховувався час, який необхідний для отримання підтверджень про доставку пакетів, а також не враховувався час встановлення та розриву з'єднань, затримки мережі GE (0,01-0,4 мс), а також службовий трафік (протоколи управління, маршрутизації і т.ін.) [14].

ВИСНОВКИ

У цій кваліфікаційній роботі були проаналізовані основні механізми захисту та відновлення, що надаються технологією GMPLS з метою забезпечення постійної працездатності та необхідної якості обслуговування в оптичних транспортних мережах типу ASON, які, у свою чергу, є базовою платформою для розгортання GMPLS.

Інфраструктура транспортних мереж ASON формується з урахуванням поточного та перспективного трафіку послуг. При цьому в таких мережах переважає трафік IP, що дозволяє реалізувати послуги в реальному та відносному масштабі часу, а самі мережі зобов'язані реагувати на запити обслуговування з мінімальними часовими затримками. Це і зумовило впровадження в таких мережах технології GMPLS, яка дозволяє помітно покращити їх якість експлуатації, адміністрування та обслуговування. GMPLS у мережах ASON є основою організації їх сигнальної системи. Якщо класична технологія MPLS використовує мітки, що фізично додаються до пакетів, то в GMPLS ця концепція забезпечується шляхом впровадження нових типів міток, що відносяться до різних оптичних елементів, таких як: віртуальні контейнери SDH, лямбди волокна, лямбди канальних інтервалів DWDM, кадри Gigabit Ethernet, і елементи інших оптичних технологій, що відносяться до класу мереж ASON. Ці елементи представлені у вигляді міток у керуючій площині протоколів мережі та використовуються оптичними комутаторами та маршрутизаторами для встановлення з'єднання GMPLS, що дозволяє змінювати процес комутації за мітками для врахування відмінностей у способах призначення міток, а також поширення повідомлень сигналізації і взаємодії з вхідними та вихідними пристроями [3, 5].

У роботі зазначено, що у мережах ASON, які організуються на базі сучасних високошвидкісних технологій (Gigabit Ethernet, SDH, DWDM, та ін.), особлива увага приділяється надійності та стабільності роботи. Показано, що мережі такого типу мають високу продуктивність каналів, але при цьому слабко пов'язані. В результаті вони є вразливими для відмов і, як наслідок, можуть призвести до втрати величезної кількості трафіку. Тому дослідження, аналіз та впровадження механізмів захисту/відновлення в оптичних мережах на базі GMPLS є актуальним завданням.

До таких механізмів захисту/відновлення належать місцеве відновлення, захисна комутація, швидка перемаршрутизація та механізми багаторівневого захисту.

В ході аналізу було виявлено, що при використанні захисту типу місцеве відновлення, втрата встановленого з'єднання LSP відновлюється за рахунок формування нового LSP з урахуванням ситуації на мережі, що змінилася. Цей вид місцевого відновлення називається відновленням від джерела. Воно є найповільнішим серед розглянутих механізмів. Процедуру місцевого відновлення можна прискорити, якщо розірване з'єднання LSP відновлюватиметься не від джерела, а локально в місці виявлення пошкодження, яке називається точкою відновлення (PLR) [5, 20].

Але у підсумку аналіз механізмів захисту та відновлення мереж GMPLS показав, що найбільш дієвим є способи, що відносяться до механізму «швидкої перемаршрутизації». Зазначено, що застосування даних способів захисту в GMPLS дозволить уніфікувати складову, що відповідає за управління оптичними транспортними мережами. Це в свою чергу сприятиме ширшому впровадженню та поширенню технології GMPLS, як єдиного стандарту сигналізації для сучасних високошвидкісних технологій мереж ASON [5, 20].

Також у роботі для мереж GMPLS запропонована концепція застосування механізму багаторівневого захисту, в якому реалізується управління кількома захисними системами, кожна з яких організовує різні захисні рівні залежно від типу класу трафіку. Показано, що сценарії багаторівневого захисту динамічно встановлюються, використовуючи основні особливості підходів до забезпечення маршрутизації з підтримкою QoS у реальному масштабі часу. Зокрема, механізми захисту впливають на маршрутизацію, пропонуючи різні шляхи та нові тракти LSP для її здійснення з урахуванням забезпечення необхідних вимог QoS. Зазначено, що найповніше переваги використання багаторівневого захисту реалізується у сценаріях із множинними відмовами [5].

У практичній частині магістерської кваліфікаційної роботи було проведено імітаційне моделювання мережі GMPLS та запропоновано методики розрахунку параметрів трафіку. Для моделювання GMPLS була використана система моделювання мережної структури NetCracker. Імітаційні блоки, що реалізують функції пристроїв та елементів MPLS, з'єднуються у мережу з використанням графічного інтерфейсу.

Результати імітаційного моделювання показали, що при досягненні обсягу трафіку певної критичної точки відбувається невелике перевантаження, що відбивається на продуктивності. Якщо така ситуація відбувається в лінійному режимі, то це не призведе до великих проблем. Однак під час, коли трафік у мережі досягне певного рівня, пропускна здатність сильно зменшиться у відповідності до більш серйозного перевантаження та збільшенням пакетів у черзі до серверів. Щоб цього уникнути можна використовувати два LSP. Другий LSP крім того можна також використовувати як резервний шлях у разі відмови першого на основі механізму швидкої перемаршрутизації. Цей механізм забезпечить додаткову надійність під час передачі трафіку і, крім того, він є дуже добре масштабованим рішенням.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Росляков А.В. Сети следующего поколения NGN / А.В. Росляков, С.В. Ванюшин и др. – М.: Эко-Трендз, 2008. – 424 с.

2. Барков Игорь Некоторые аспекты технологий IP-телефонии [Електронний ресурс] / ixbt.com. – Режим доступу: https://www.ixbt.com/comm/ip-aspects.html.

3. Гольдштейн А.Б., Гольдштейн Б.С. Технология и протоколы MPLS / А.Б. Гольдштейн, Б.С. Гольдштейн. – С-Пб.: БХВ-Санкт-Петербург, 2005. – 304 с.

4. Бубенцова Л.В. Технология MPLS: уч. пособ. / Л.В. Бубенцова – Одесса: ОНАС им. А.С. Попова, 2010. – 44 стр.

5. Будылгина Н.В. Технологии глобальных компьютерных сетей: уч. пособ. / Н.В. Будылдина. – Екатеринбург: УрТИСИ ГОУ ВПО «СибГУТИ», 2006-264с.

6. Олифер В.Г. Компьютерные сети: принципы, технологии, протоколы / В.Г. Олифер, Н.А. Олифер. – 4-е изд. – СПб.: Питер, 2010. – 944 с.

7. Xtera Communications Inc. Компоненты DWDM систем и их характеристики // LightWave Russian Edition. – №2. – 2005.– С. 50 - 56.

8. Фокин В.Г. Оптические системы передачи и транспортные сети: уч. пособ. / В.Г. Фокин – М.: Эко-Трендз, 2008. – 271 с.

9. Рахматулин А.М. Анализ оптимальности применения обобщенной многопротокольной коммутации в отказоустойчивых решетчатых оптических транспортных сетях связи / А.М. Рахматулин // Спецвыпуск T-Comm «Технологии информационного общества». Часть1. – 2009. – С. 35 - 37.

10. Ильтаф В. Эффективный механизм передачи данных в опорных IP-сетях с использованием технологии MPLS / Валид Ильтаф // Беспроводные технологии . – №2. – 2017. – С. 14 - 20.

11. Francesco Palmieri. VPN scalability over High Performance Backbones Evaluating MPLS VPN Against Traditional Approaches. Eighth IEEE International Symposium on Computers and Communication (ISCC’03). – 2003.

12. Rissal Efendi. A Simulation Analysis of Latency and Packet Loss on Virtual Private Network through Multi Virtual Routing and Forwarding // International Journal of Computer Applications. 2012. Vol. 60. № 19.

13. Гулевич Д.С. Сети связи следующего поколения: учеб. курс [Електронний ресурс] / Д. С. Гулевич // НОУ «ИНТУИТ» – 2007. – Режим доступу до ресурсу: http://www.intuit.ru/studies/courses/1150/157/info.

14. Курятніков П.І. Механізми забезпечення постійної працездатності транспортних мереж GMPLS / П.І. Курятніков, Ю.М. Колтун // матеріали 13-ої міжнародної науково-технічної конференції «Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління». – Баку – Харків – Жиліна, 26 -27 квітня, 2023 р. – С. 79.

15. Ролич М.Л. Технология обобщенной коммутации в MPLS сетях / М.Л. Ролич, А.Ю. Болдоев // Международный научно-исследовательский журнал. – №10 (17). – 2013 (Часть 2). – С. 76 – 77.

16. RSVP-TE [Електронний ресурс]. – Доступ здійснено 08.05.2023. – Режим доступу до ресурсу: https://linkmeup.gitbook.io/sdsm/10.-base-mpls/03.-label_distribution/01.-protocols/02.-rsvp-te

17. P. Nilsson And M. Pi´oro. Solving dimension in gtasks for proportionally fairnet works carrying elastic traffic. Performance Evaluation, 49 (1–4): 371–386, September 2002.

18. Сатовский Б.Л. MPLS - технология маршрутизации нового поколения сетей общего пользования/ Б.Л. Сатовский // Сети и системы связи. 2001. № 3. С. 57 - 65.

19. Лузгачев М.В. Задача маршрутизации трафика на графе сети MPLS с одноадресными соединениями [Електронний ресурс] / М.В. Лузгачев, К.Е. Самуйлов // Вестник РУДН. Серия Математика. Информатика. Физика. – №1. – 2009. – С. 23 – 33. – Режим доступу до ресурсу: https://cyberleninka.ru/article/n/zadacha-marshrutizatsii-trafika-na-grafe-seti-mpls-s-odnoadresnymi-soedineniyami/viewer.

20. Алленов О.М. Технология GMPLS: методы защиты и восстановления/ О.М. Алленов // Вестник связи. – 2017. – № 9. – С. 72-78.

21. Решение проблем, связанных с фрагментацией IP, а также с MTU, MSS и PMTUD, при помощи протоколов GE и IPSEC [Електронний ресурс] / Cisco Systems, Inc. – 2010. – Режим доступу до ресурсу: http://www.justogroup.ru/dokumentacija/cisco/kommutiruemye_seti/reshenie_problem,_svyazannih_s_fragmentaciey_ip.pdf.