Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

Інститут телекомунікаційних систем
(повне найменування інституту, факультету)

Кафедра телекомунікацій
(повна назва кафедри)

До захисту допущено

В.о. завідувача кафедри

_____ Валерій ЯВІСЯ
(підпис) (Ім'я, прізвище)

"04" червня 2020 р.

Дипломна робота

на здобуття освітнього ступеня "бакалавр"
(назва ОС)

Спеціальність 172 Телекомунікації та радіотехніка,
(код і назва)

на тему: Побудова базової телекомунікаційної мережі на основі технології MPLS

Виконав (-ла): студент (-ка) 4 курсу, групи ТМ-61
(шифр групи)

Литовченко Костянтин Анатолійович _____
(прізвище, ім'я, по батькові) (підпис)

Керівник професор, к.т.н. Романов Олександр Іванович _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Консультант _____ _____ _____
(назва розділу) (посада, вчене звання, науковий ступінь, прізвище, ініціали) (підпис)

Рецензент доцент, к.т.н. Созонник Галина Дмитрівна _____
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище та ініціали) (підпис)

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

Студент _____
(підпис)

Київ – 2020 року

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

Інститут телекомунікаційних систем
(повна назва)

Кафедра телекомунікацій
(повна назва)

Освітній ступінь бакалавр
Спеціальність 172 Телекомунікації та радіотехніка
(код і назва)

ЗАТВЕРДЖУЮ
В.о. завідувача кафедри
____ Валерій_ЯВІСЯ
(підпис) (ім'я, прізвище)
"_22 "_січня_2020 р.

ЗАВДАННЯ
НА ДИПЛОМНУ РОБОТУ СТУДЕНТУ

Литовченко Костянтин Анатолійович
(прізвище, ім'я, по батькові)

1. Тема роботи Побудова базової телекомунікаційної мережі на основі технології MPLS

керівник роботи професор кафедри ТК, д.т.н. Романов О.І.
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом по університету від 30 березня 2020 р. № 924-с

2. Термін подання студентом роботи__
3. Вихідні дані до роботи

4.Зміст роботи: 1). Обгрунтування актуальності теми. Розглянути основні компоненти мережі MPLS, їх призначення та функції. 2). Проаналізувати роботу основних протоколів у мережі MPLS; 3). На основі дослідженої інформації побудувати базову телекомунікаційну мережу, використовуючи технологію MPLS.

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо)
Слайд №1 План доповіді.
Слайд №2 Вступ. Актуальність, мета та практична цінність роботи.
Слайд №3 Структура мітки. Основні поля.
Слайд №4 Інкапсуляція міток.
Слайд №5 LSP тракти. Робота та утворення трактів.
Слайд №6 Протоколи OSPF та BGP.
Слайд №7 Протоколи LDP та RSVP.
Слайд №8 Базова мережа MPLS.
Слайд №9 Сервіси, які працюють на технології MPLS.
Слайд №10 GMPLS.
Слайд №11 Висновки до роботи, напрями подальшого вивчення.
Слайд №12 Публікації, тези, участь в конференціях і т.п.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання 04.09.2019

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів роботи	Примітка
1	Отримання завдання. Аналіз поставлених задач. Початок пошуку інформації.	04.09.2019 – 01.10.2019	
2	Історичні умови появи технології MPLS.	01.10.2019 – 05.10.2019	
3	Аналіз технології MPLS. Перелік компонентів, їх призначення та функції.	05.10.2019 – 16.10.2019	
4	Розгляд мітки як головного компонента технології MPLS. Її структура, завдання та застосування.	16.10.2019 – 16.11.2019	
5	Розгляд LSP тракту. Умови створення, принцип роботи.	20.11.2019 – 20.02.2020	
6	Аналіз видів, призначення та роботи FEC.	20.02.2020 – 24.02.2020	
7	Розгляд структури основних протоколів технології MPLS: OSPF, BGP, RSVP, LDP. Їх використання в мережі MPLS.	24.02.2020 – 10.03.2020	
8	Розробка телекомунікаційної мережі на базі технології MPLS. Аналіз їх основних функції, взаємодії елементів MPLS мережі з базовою мережею IP.	10.03.2020 – 30.04.2020	
9	Аналіз роботи сервісів, які працюють на технології MPLS.	30.04.2020 – 08.05.2020	
10	Опис роботи технології GMPLS в телекомунікаційній мережі майбутнього.	09.05.2020 – 25.05.2020	
11	Оформлення пояснювальної записки дипломної роботи, підготовка до захисту.	25.05.2020 – 01.06.2020	

Студент _____ Литовченко К.А.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Романов О.І.
(підпис) (прізвище та ініціали)

РЕФЕРАТ

Дипломна робота містить: 85 сторінок, 32 рисунків, 2 таблиці, 13 посилань

Метою даної роботи є аналіз технології MPLS, висунення пропозиції щодо побудови базової телекомунікаційної мережі на основі технології MPLS та аналіз роботи такої мережі.

В дипломній роботі проведено аналіз та порівняння сучасних мереж, які використовуються. Розгляд принципів формування MPLS мережі, взаємодії MPLS мережі з IPv4 мережею. Також було проведено аналіз мережі GMPLS, її побудова.

Ключові слова: MPLS, LDP, OSPF, BGP, LSP, мітки, LSP тракти, LSR.

ABSTRACT

The diploma work consists of 85 pages, 32 figures, 2 tables, 13 references

The purpose of this work is to analyze the MPLS technology, make a proposal to build a basic telecommunications network based on MPLS technology and analyze the operation of such a network.

The thesis analyzes and compares modern networks that are used. Consideration of the principles of formation of MPLS network, interaction of MPLS network with IPv4 network. GMPLS network analysis and construction were also performed.

Keywords: MPLS, LDP, OSPF, BGP, LSP, tags, LSP paths, LSR.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

1. MPLS Multiprotocol Label Switching – багатопротокольна комутація міток
2. GMPLS Generalized Multiprotocol Label Switching – узагальнена багатопротокольна комутація міток
3. TE Traffic Engineering – інжиніринг трафіку
4. FEC Forwarding Equivalence Class — це класи трафіка
5. LER MPLS edge router — це крайовий вузол MPLS мережі, який з'єднує домен MPLS з вузлом поза цим доменом.
6. LSP Label Switched Path — шлях проходить через один або більше LSR тракт, по якому йдуть пакти одного і того ж FEC.
7. ER-LSP Explicitly routed LSP — тракт LSP, який організований у спосіб, відмінний від традиційної маршрутизації пакетів IP.
8. LSR Label Switching Router - маршрутизатор, здатний пересилати пакети за технологією MPLS.
9. IP Internet Protocol – інтернет протокол, міжмережний протокол
10. RSVP Resource ReSerVation Protocol – протокол резервування мережевих ресурсів
11. LDP Label Distribution Protocol – протокол розподілу міток
12. OSPF Open Shortest Path First – протокол динамічної маршрутизації
13. BGP Border Gateway Protocol – протокол граничного шлюза
14. IBGP Internal Border Gateway Protocol – протокол внутрішнього кордону шлюзу
15. EBGP Exterior Border Gateway Protocol – протокол зовнішнього кордону шлюзу
13. FRR Fast ReRoute – швидке перенаправлення
14. LIB Label Information Base – інформаційні база міток
15. CE Customer Edge – кордонний маршрутизатор користувача
16. PE Provider Edge – кордонний маршрутизатор провайдера
17. VPN Virtual Privet Network – віртуальні приватні мережі

ВСТУП

Виникнення комп'ютерних мереж спричинило бум у революції передачі повідомлення на великі відстані. З самого початку виникнення перед комп'ютерними мережами були поставлені наступні задачі: передача даних на великі відстані, задоволення потреб у швидкості і якості передачі цих даних та основне і найголовніше – це з'єднання окремих вузлів між собою в одну мережу. Саме передача даних була основною причиною виникнення таких мереж та їх розвитку. Проте корпорації шукали шляхи для вирішення таких задач: збільшення швидкості передачі даних в межах одного офісу, а потім між віддаленими філіалами, які можуть знаходитися в різних частинах світу.

Сьогодні мережі вже перестали просто бути частиною компанії, і стали однією з важливих аспектів, на які спираються новостворені корпорації, компанії або менші по розмірах бізнеси. Ні одна організація не може функціонувати і здійснювати свою діяльність без побудови комп'ютерної та телекомунікаційної мережі.

Крім того, стає гостре питання виділення інтернет-ресурсів: адреси IPv4, кількість яких з кожним роком стає все менше, а IPv6 поки що не дуже розповсюджений. Також виникає потреба надання якості цих послуг або як ще називають QoS. Рішення першої частини питання полягає у тому, що за допомогою транспортних каналів офіси з'єднуються з центральним або між собою, а передача даних у зовнішній світ відбувається через одну точку. Таке рішення є достатньо непоганим, у випадку, якщо не потрібний додатковий захист або надійність. Рішення другої частини питання це створення технологій та пристроїв, які забезпечують швидку передачу на рівні 2 та 3. Поява нових пристроїв комутації на рівні 2, а також нових маршрутизаторів на рівні 3, які використовують таблиці маршрутизації для швидкого оброблення та передачі даних.

Поява таких технологій як ATM та Free Relay, які були розроблені в 90-ті роки, зробили прорив у передачі пакетів. З'явилися засоби забезпечення обслуговування такі як DiffServ та IntServ, протоколи маршрутизації та

резервування. Проте всі вони програють у таких параметрах як затримка, джиттер, перевантаження і т.п., багатопротокольній комутації по мітках MPLS.

MPLS є універсальним розв'язанням проблем якості обслуговування (QoS), які стоять перед пакетними мережами на сьогоднішній день. MPSL забезпечує високу швидкість передачі даних, масштабованість, оптимізацію розподілу трафіку та ефективну маршрутизацію в пакетних мережах IP. Проте чому саме MPLS є протоколом-лідером на цей час? Які ще він має переваги, крім вище перерахованих? Це безумовно оптимальне відображення наскрізного трафіку третього рівня від вихідного мережевого вузла до вхідного вузла в трафіку на другому рівні мережевої ієрархії. Можна сказати, що технологія MPLS – є гібридом рівнів 2 і 3 OSI.

В даній роботі буде проведено аналіз роботи базової телекомунікаційної на основі технології MPLS та побудова мережі з використання MPLS.

1. Аналіз технології MPLS. Перелік компонентів, їх призначення та функції

1.1. Історичні умови появи технології MPLS.

Традиційно основними вимогами до технології опорних мереж були висока пропускна здатність, низька затримка та хороша масштабованість. Однак сучасний стан ринку диктує нові правила гри. Тепер постачальника послуг недостатньо просто надавати доступ до своєї магістралі IP. Зміни потреби користувачів включають доступ до інтегрованих мережевих служб, організацію віртуальних приватних мереж (VPN) та ряд інших інтелектуальних послуг.

Багатопротокольна комутація міток (MPLS) - це метод маршрутизації в телекомунікаційних мережах, який здійснює маршрутизацію даних від одного вузла до іншого на основі міток короткого шляху, а не довгих мережевих адрес, що дозволяє уникнути складних пошуків у таблиці маршрутизації та прискорює потоки трафіку.

За інформацією Infocellar, MPLS у тому вигляді, в якому ми це знаємо сьогодні, був створений у 1997 році інженерною робочою групою в Інтернеті і став альтернативою багатошаровому перемиканню IP через банкомат. Банкомат через IP, один з найбільш ранніх протоколів маршрутизації, використовував функцію 3 рівня, але використовувався лише на кордонах мережі. Зі зростанням вимог споживачів та корпоративних мереж постачальники послуг незабаром усвідомили обмеження IP та ATM, особливо коли мова йде про масштабованість. Ще однією проблемою була маршрутизація IP-пакетів через мережі банкоматів. Всі запропоновані технології спрямовані на поєднання переваг маршрутизації IP та комутації ATM, залишаючись при цьому орієнтованими на використання IP-мереж, і таким чином дозволяють мультисервісної мережі еволюційно розвиватися до спрощення своєї інфраструктури шляхом інтеграції функцій другого

(комутаційного) та третій (маршрутизаційний) рівень. Ця перешкода призвела до створення MPLS у 1997 році, який став галузевим стандартом для сумісної багатошарової комутації. IETF працював над створенням MPLS, підтримуючи функціональність IP, виключаючи протоколи ATM та використовуючи комутацію міток MPLS. MPLS почав масове використання з 2001 року. Багатопротокольна комутація міток (MPLS) отримала свою назву завдяки тому, що ця технологія могла взаємодіяти з будь-яким видом протоколів мережевого рівня, тобто MPLS - це інкапсулюючий протокол, який може передавати дані з декількох протоколів нижніх шарів OSI модель. Представники найбільших постачальників мережевих рішень та обладнання беруть активну участь у діяльності групи. Ця архітектура виросла із системи Tag Switching, запропонованої Cisco Systems, проте деякі ідеї були запозичені у конкуруючої технології комутації IP від Ipsilon та проєкту ARIS IBM. Архітектура MPLS містить найуспішніші елементи з усіх згаданих розробок, і незабаром вона повинна перетворитися на Інтернет-стандарт завдяки зусиллям IETF та компаній, зацікавлених у швидкому просуванні цієї технології на ринок. Cisco у своїй системі перемикання тегів відійшов від концепцій, які запропонували Ipsilon та ARIS, а саме запропонував створити таблицю переадресації в комутаторі, що не грунтується на потоці трафіку, і було визначено для технологій рівня 2. Технологія від Cisco була близькою до технології MPLS; крім того, MPLS запозичила механізми, які використовуються в перемиканні тегів. Механізм перемикання тегів був розроблений для роботи з низкою протоколів нижчого рівня і включав протокол розподілу ключових слів (протокол розподілу тегів, TDP), як у MPLS, механізм комутації тегів підтримував формування стека тегів. Окрім швидшого пошуку адреси, нові маршрутизатори можуть обслуговувати дзвінки різними способами залежно від необхідної якості обслуговування (при передачі голосу, відео та зображення). Крім того, всі маршрутизатори

Cisco, які впровадили Tag Switching, пізніше були оновлені та змогли підтримувати MPLS.

Ще одна технологія, яка передувала MPLS, - це технологія IP-навігатора, запропонована Cascade. Потім Каскад придбав компанію Ascend, яка, своєю чергою, стала частиною Lucent Technologies. Технологія IP-навігатора використовувала багато ідей для комутації IP-мереж, розроблених раніше Toshiba, Ipsilon, Cisco та IBM.

Після опублікування першої серії проектів стандартів перемикання тегів 9–13 грудня 1996 року в Сан-Дієго, штат Каліфорнія, BETF прийняв рекордну відвідуваність IETF, на якій Cisco Systems, IBM та Toshiba виступили з презентаціями своїх технологій. Такий інтерес, а також той факт, що так багато провідних компаній багато технічно розробили технічні пропозиції щодо вирішення проблеми, дозволили зробити очевидний висновок про необхідність створення спеціальної групи для стандартизації механізму перемикання етикетки. У квітні 1997 року в Мемфіс Тенісі було проведено перше засідання робочої групи МПЛС. Сама назва Multiprotocol Label Switching була прийнята, насамперед, з тієї причини, про яку ми вже згадували, що назви IP Switching та Tag Switching пов'язувались з продуктами, що випускаються конкретними компаніями, і потрібен був нейтральний термін. Зараз технологія MPLS працює в симбіозі з маршрутизацією IP, будучи її невід'ємною частиною, працює над IP.

1.2. FEC

Робочі групи визначили три основні елементи технології MPLS: FEC – клас переадресації еквівалентності – клас еквівалентності переадресації; LSR – Lable Switching маршрутизатор – маршрутизатор перемикання міток; LSP – мітка комутованого шляху – шлях перемикання міток. Цей пункт буде стосуватися FEC.

Заголовок пакета містить набагато більше інформації, ніж потрібно для вибору наступного маршрутизатора. Цей вибір можна організувати простіше - виконавши дві функції. Один з них – це поділити весь набір пакетів, що надходять, на класи, які називаються переадресаційними класами еквівалентності (FEC). При використанні багатопротокольної комутації міток MPLS пакет присвоюється лише певному класу FEC
раз, коли він потрапляє в мережу. Цьому FEC присвоюється мітка - ідентифікатор фіксованої довжини, який передається разом з пакетом, коли він пересилається до наступного маршрутизатора. Кожен мережевий маршрутизатор MPLS створює таблицю, яка визначає, як слід пересилати пакет. Ця таблиця, яка називається інформаційною базою міток LIB, містить набір використаних міток, і для кожної з них є прив'язка "мітка FEC". Мітки, які використовуються LSR для прив'язки тегів FEC, поділяються
в наступні категорії:

• на платформі, коли значення мітки є унікальними на всьому шляху LSP; Мітки вибрані із загального пулу міток, і жодна дві мітки, розподілені по різних інтерфейсах, не мають однакового значення.

• на основі інтерфейсу, коли значення міток пов'язані з інтерфейсами: для кожного інтерфейсу визначається окремий пул міток, з якого вибираються мітки для цього інтерфейсу. При цьому мітки, присвоєні різним інтерфейсам, можуть
бути однаковим.

1.3. Мітки

Поєднання пов'язане з тим, що той самий мережевий пристрій, який називається маршрутизатором мітки (LSR), виконує функції як маршрутизатора IP, так і комутатора віртуальної схеми. Мало того, це не механічне поєднання двох пристроїв, а тісна інтеграція, коли функції кожного

пристрою доповнюють один одного і використовуються разом. Важливо зауважити, що побудова мережі MPLS або формування LSP здійснюється заздалегідь, до отримання робочих пакетів у мережі. LSP генеруються автоматично на запит або вручну мережевим адміністратором. Саме з мітками виконуються процедури їх розподілу через маршрутизатори LSR та процедури створення LSP-шляхів, по яких будуть слідувати пакети MPLS. Після розподілу міток та створення шляхів LSP можна виконати основну функцію MPLS - пересилання мічених пакетів мережею MPLS. Комутація міток виконується за наступними кроками:

Крок 1. Створення та розповсюдження міток. Перед тим, як розпочнеться передача мережею MPLS, маршрутизатори LSR здійснюють відповідність між мітками та FEC у своїх таблицях. Крім того, характеристики трафіку та функціональні можливості MPLS узгоджуються до передачі даних (крива 2 на рис. 1), або генеруються як пакети, що належать певному потоку даних або трафіку певного класу, що входить у мережу MPLS (крива 1).

Крок 2. Створення таблиці в кожному LSR. Після отримання інформації про прив'язку міток для FEC кожен маршрутизатор LSR створює записи в таблиці LIB. Вміст таблиці показує відповідність між мітками та FEC і пов'язує кожну пару "вхідний інтерфейс, вхідна мітка" з парою "вихідний інтерфейс, вихідний мітка". З будь-якими новими узгодженнями, прив'язки мітки до записів FEC у таблиці оновлюються. Таблиці міток, згідно з якими кожен пакет спрямовується по відповідному шляху LSP, завжди встановлюються перед тим, як пакет розпочинає свій шлях через мережу. Окрім того, шлях з комутацією міток завжди є одностороннім. Якщо ви хочете, щоб пакетний трафік між двома прикордонними LSR рухався у зворотному напрямку, з`являється необхідність створення двох шляхів.

Крок 3. Створення мічених LSP шляхів. Як показано лінією 1 на рис.1, шляхи LSP створюються у зворотному напрямку до створення записів у таблицях LIB. Кожен LSR отримує мітку від нижчестоячого маршрутизатора.

LSP створюється послідовною маршрутизацією по секціях, і якщо потрібна оптимізація розподілу трафіку, для визначення шляху використовується протокол CR-LDP, який гарантує відповідність вимогам QoS / CoS, або протокол RSVP-TE.

Крок 4. Табличний пошук та інкапсуляція міток у пакеті. Маршрутизатор на вході (LSR1 на рис. 1), визначивши, до якого FEC належить отриманий ззовні пакет, використовує таблицю LIB для пошуку потрібного зв'язування "FEC label" та інкапсулює цю мітку таким чином, що підходить для технологій, що використовується на рівні 2, як це буде показано нижче.

Крок 5. Пересилання пакету. Розглянемо потік пакетів від вхідного маршрутизатора LSR1 до вихідного маршрутизатора LSR5. Зауваження, що LSR1 може не мати мітки для цього пакета. У цьому випадку він знаходить наступний роутер за IP-адресою. Нехай наступним маршрутизатором для LSR1 буде LSR2. Маршрутизатор LSR1 ініціює запит мітки від LSR2. Отримана мітка LSR1 вставляється в пакет і пересилає його до LSR2. Кожен наступний LSR (в цьому випадку LSR3 та LSR4) аналізує мітку, що міститься в отриманому пакеті, замінює її вихідною міткою та передає пакет далі. Коли пакет досягає LSR5, він видаляє мітку з пакета, оскільки пакет залишає домен MPLS і доставляє пакет до місця призначення. Шлях LSP, через який проходить пакет,
показаний пунктирними лініями 2.

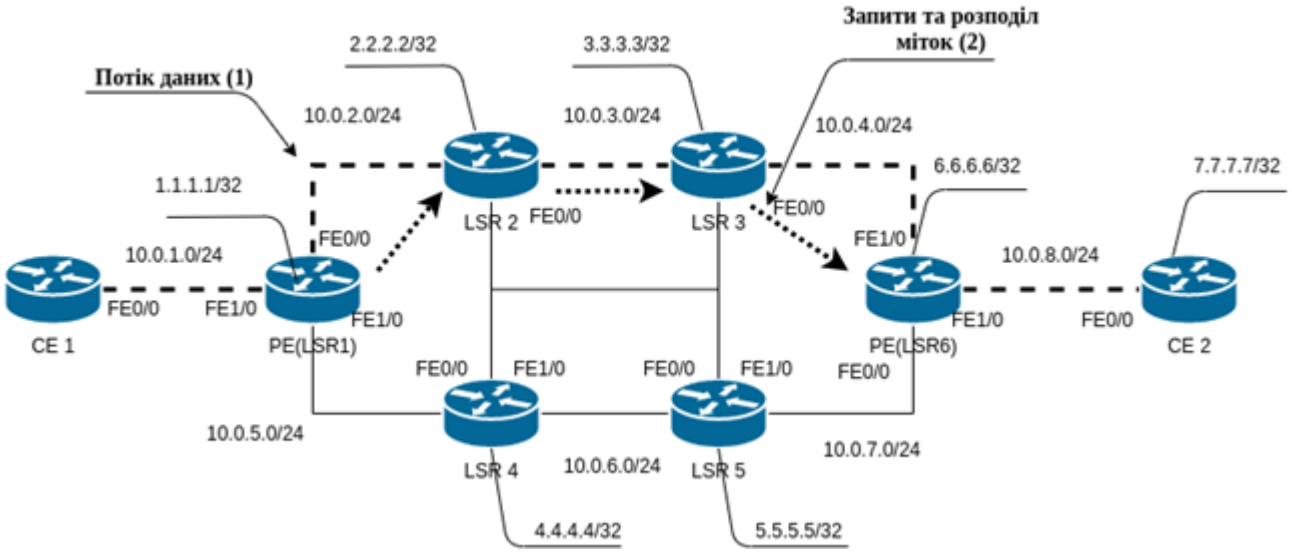

Рис. 1. Комутація по міткам MPLS

Після отримання пакету маршрутизатор LSR отримує з нього мітку і використовує її як індекс у своїй таблиці переадресації. Як тільки буде знайдено запис, в якому значення вхідної мітки дорівнює значенню мітки, вилученої з пакета, маршрутизатор замінює вхідну мітку в пакеті вихідною міткою і пересилає пакет через вказаний вихідний інтерфейс у під рекорді до наступного LSR, також зазначеному в цьому під записі. Якщо під запис записує конкретну вихідну чергу, маршрутизатор ставить пакет у цю чергу. Якщо LSR підтримує не одну, а декілька таблиць (по одній для кожного з її інтерфейсів), то єдиною зміною алгоритму є те, що після отримання пакету LSR попередньо вибирає таблицю, яка буде використана для обробки пакету. Таблиця вибирається відповідно до ідентифікатора інтерфейсу, через який був отриманий пакет. Розглянемо крок 5 більш докладно: маршрутизатор вхідного кордону PE (LSR1) визнає, що прийнятий пакет від CE1 повинен бути переданий відповідно до FEC, переданий через LSP 1-2-3-6, додає мітку з номером 1 до пакету і пересилає його на транзитний маршрутизатор LSR2, де за допомогою таблиці переадресації вхідна мітка замінюється міткою з номером 2 і пакет передається далі по вищезгаданому маршруту до LSR3. LSR3 замінює мітку №2 міткою №3. Потім LSR 3 через вихідний інтерфейс, в

цьому випадку FE0 / 0, передає пакет на крайовий маршрутизатор LSR6. У маршрутизаторі LSR6 видаляє мітку 3, і пакет передається на CE2, який має адресу 7.7.7.7/32, використовуючи звичайну передачу пакету через мережу IP.

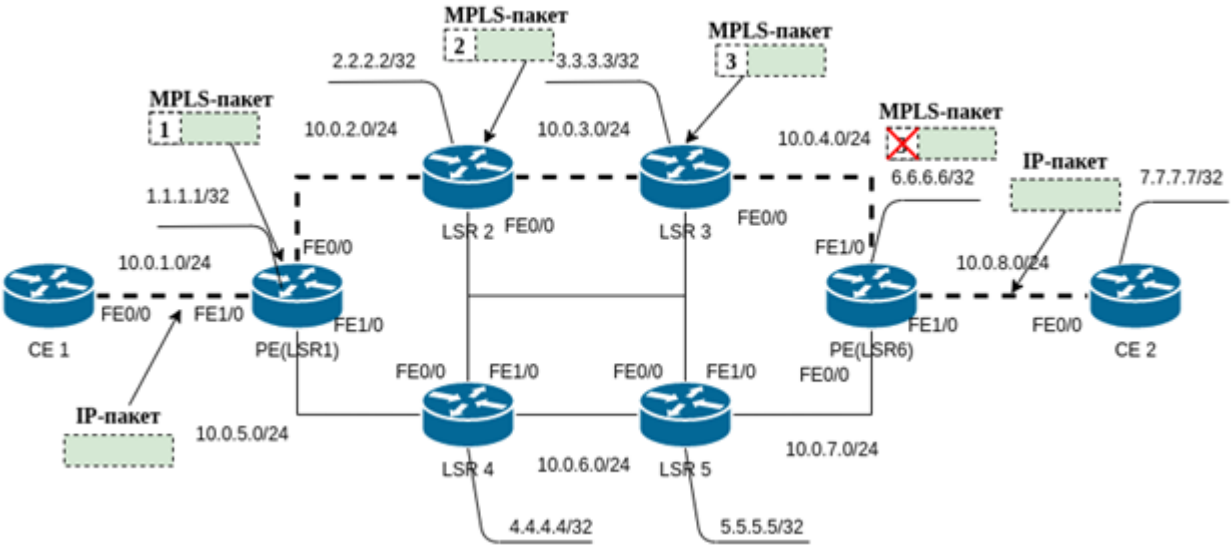

Рис. 2. Проходження мітки по мережі MPLS

1.3.1. Структура мітки, стек міток

На рисунку 3 показані формати заголовків взаємодії технології MPLS з технологіями канального рівня PPP та Ethernet. Це не означає, що під шаром MPLS є повністю функціональна мережа з технологією на канальному рівні, наприклад, мережею Ethernet, але лише те, що передача обов'язково використовує формати кадрів цих технологій для розміщення IP-пакету (рівень 3) в кадр канального рівня. Сучасні маршрутизатори часто мають оптичний інтерфейс, але це не означає, що протокол IP (третій рівень моделі OSI) безпосередньо взаємодіє з фізичним рівнем, тобто з технологією DWDM (нижній підрівень першого, фізичний рівень моделі OSI). Фактично, у цьому випадку обладнання, що реалізує ту чи іншу технологію канального рівня (PPP або Ethernet), а також обладнання, що реалізує функції електричного

фізичного шару, наприклад, технологія PoS (Packet over SDH), яка реалізується використовуючи вбудовані (вбудовані) мультиплексори SDH в IP-роутери.

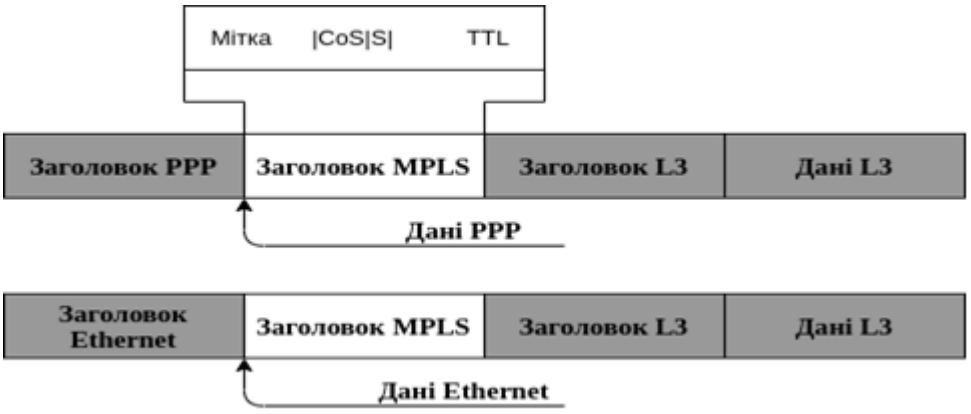

Рис.3. Схема розміщення MPLS мітки

Мітка - це елемент фіксованої довжини, який використовується для локальної ідентифікації класу еквівалентності пересилання FEC. Довжина мітки — 32 біта (4 байти): 12 біт — заголовок і 20 біт — значення мітки. Заголовок мітки складається з трьох полів: 3-бітове поле Exp, яке може бути використане для вказівки класу обслуговування, S-біт атрибута "нижнього" стека та 8-бітний TTL (Time-to-Live) поле. 20-бітове поле мітки містить значення MPLS-мітки, яке може бути будь-яким числом в діапазоні від 0 до $2^{20} - 1$, за винятком значень резерву (0, 1, 2, 3 і т.д.) . Схема MPLS-кадра показана на рис. 4.

Рис. 4. Структура MPLS-мітки

Експериментальне бітове поле (EXP) містить три біти, які зарезервовані для подальших досліджень та експериментів. В даний час ведеться робота

над створенням узгодженого стандарту використання цих бітів для підтримки диференційованого обслуговування різних типів трафіку та ідентифікації класу обслуговування. При наданні диференційованих послуг мережі MPLS це поле може вказувати на певний клас сервісу, наприклад, аналогічний класам DiffServ. Щоб забезпечити якість IP-послуг в кінці, на межі мережі MPLS ви можете скопіювати поле пріоритету IP в поле CoS, враховуючи, що поле CoS у заголовку MPLS містить лише 3 біти, і лише 3-розрядне IP-поле може передаватися в ньому пріоритетно, а 6-бітове диференційоване поле коду обслуговування (DSCP - Differentiated Service Code Point) не є. При необхідності, інформація CoS може також передаватися як одна з міток стеку MPLS, оскільки поле мітки має розмір 20 біт і може вміщувати як поле пріоритету IP, так і поле DSCP.

Біт S є засобом підтримки ієрархічної структури стека міток MPLS. В заголовку останньої (тобто найглибшої чи найнижчої) мітки біти є S = 1, а у всіх інших мітках у стеці біти S = 0.

Поле часу життя (TTL) в заголовку MPLS працює аналогічно полю TTL в IP-дейтаграмі; це поле є механізмом, який перешкоджає можливості нескінченної циркуляції пакетів через мережу внаслідок утворення закільцьованих маршрутів. Байт TTL знаходиться в кінці заголовка мітки і, як показано на рис. 4, займає біти 24 - 31. Діапазон цього поля становить від 0 до 255.

Можна використовувати теги MPLS у вигляді стеку, які показані на рис. 5. MPLS може виконувати такі операції зі стеком: помістити мітку на стек, вийняти мітку зі стека та замінити мітку. Функціонал стека MPLS дозволяє поєднувати кілька LSP в один. До стека мітки кожного з цих LSP зверху додається загальна мітка, що призводить до агрегованого шляху MPLS. У кінцевій точці такого шляху він розгалужується на свої окремі LSP. Так можуть об’єднувати тракти, які мають загальний маршрут. Отже, MPLS здатний забезпечити ієрархічну переадресацію, що може стати важливою і

необхідною особливістю. При його використанні не потрібно передавати глобальну інформацію про маршрутизацію, що робить мережу MPLS більш стабільною та масштабованою, ніж мережа з традиційною маршрутизацією. Тег MPLS повинен завжди супроводжуватися заголовком рівня.

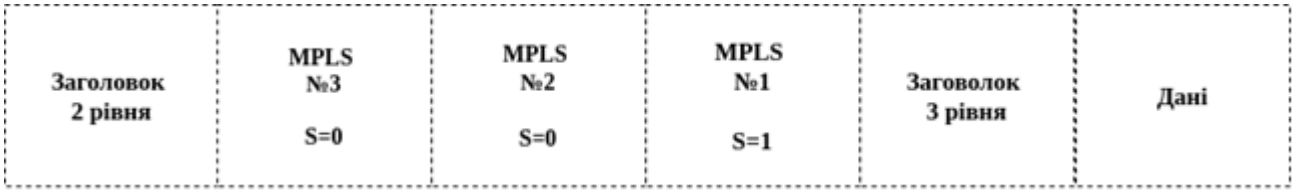

Рис. 5. Приклад трьохрівневого стека міток MPLS

Кожна мітка має власні значення полів Exp, S-біта и TTL.

Механізм інкапсуляції містить один або більше протоколів верхнього рівня в межах корисного набору дейтаграми інкапсульованого протоколу. Загальна модель інкапсуляції показана на рис. 6.

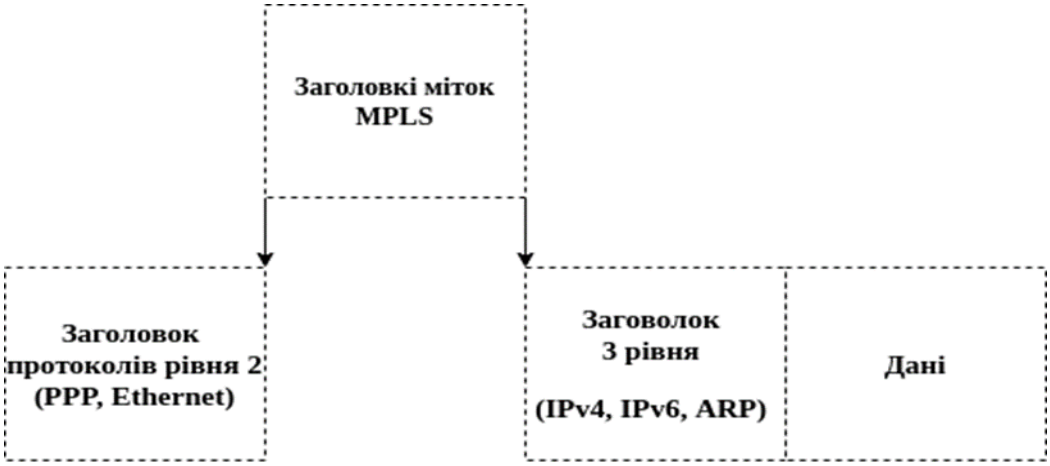

Рис. 6. Інкапсуляція MPLS міток

Мітка MPLS може бути розміщена в існуючому форматі заголовка рівня 2. Однією з сильних сторін технології MPLS є те, що вона може використовуватися спільно з різними протоколами рівня 2. Серед цих протоколів є ATM, Frame Relay, PPP та Ethernet, FDDI та інші, передбачені документами MPLS.

Інформація про теги може передаватися кількома способами:

- у складі заголовка другого рівня ATM , коли інформація про теги передається в ідентифікаторах віртуального каналу VCI та віртуальної контури VPI.
- як частина кадру AAL5 (ATM Adaptation Layer 5) рівня адаптації ATM перед сегментацією та компіляцією SAR (Segmentation and Reassembly), яка виконується в ATM-середовищі, коли ця інформація містить дані стека міток (кілька полів міток MPLS);
- як частина заголовка другого рівня Frame Relay, коли інформація мітки передається в ідентифікаторах DLCI (Data Link Connection Identifier);
- як нова 4-байтова мітка, що називається клином або прокладкою (shim), яка вставляється між заголовками другого та третього рівнів;

Отже, мітка може бути поміщена в пакет різними способами - вміститись у спеціальний заголовок, розміщений або між заголовками рівня 2 та рівня 3, або у вільне та доступне поле заголовка одного з цих двох рівнів, якщо, звичайно, є одна. Очевидно, питання про те, де розмістити заголовок, що містить мітку, повинен відповідати об’єктам, які його використовують.

1.3.2. Таблиці пересилань

Інформаційна база з інтегрованою таблицею міток називається Next Hop Laward Forwarding Entry (NHLFE) і, згідно з RFC 3031, вона містить таку інформацію:

• операція, яка повинна виконуватися зі стеком міток пакетів (замініть верхню мітку стека, видаліть верхню мітку, помістіть нову мітку на поверх стека);

• наступний маршрутизатор в LSP, з наступним
бути тим самим LSR;

• інкапсуляція на рівні зв'язку даних, що використовується в передачі пакетів;

• спосіб кодування стека міток при передачі пакету;

• інша інформація, що стосується переадресації пакету.

Вхідна мітка	Перший підзапис	Другий підзапис
Значення вхідної мітки	Вихідна мітка	Вихідна мітка
	Вихідний інтерфейс	Вихідний інтерфейс
	Адреса наступного LSR	Адреса наступного LSR

Таблиця 1. Записи в таблиці LIB

Додаткова інформація вказує, куди слід переслати пакет — наступний відрізок маршруту або наступний маршрутизатор — запис у таблиці також може містити інформацію, яка вказує, які ресурси має можливість використовувати пакет, наприклад, певну вихідну чергу. LSR може підтримувати одну загальну таблицю або окремі таблиці для кожного з її інтерфейсів. У першому варіанті обробка пакету визначається виключно міткою, що міститься в пакеті. У другому варіанті обробка пакетів визначається не тільки міткою, але й інтерфейсом, до якого пакет надійшов. LSR може використовувати або перший варіант, або другий варіант, або комбінацію обох. У MPLS найважливішою властивістю алгоритму переадресації є те, що вся інформація, необхідна для переадресації пакета та вирішення, якими ресурсами пакет може користуватися, LSR може отримати лише одним доступом до пам'яті.

1.3.3. Прив’язка «FEC-мітки»

Існує два типи прив'язки міток до FEC: перший тип - мітка для зв'язування вибирається та призначається локально в LSR. Це зв'язування називається локальним. Другий тип полягає в тому, що LSR отримує інформацію про зв'язування мітки від якоїсь іншої LSR, яка відповідає зв'язуванню, створеному на цій іншій LSR. Це прив'язка називається віддаленою.

Перший варіант називається зв'язуванням мітки «знизу», тому що в цьому випадку прив'язка мітки, перенесеної пакетом до FEC, до якого належить цей пакет, створюється підпорядкованим LSR, тобто LSR, які ближче до місця призначення пакету, ніж LSR які поміщають мітку на пакет. Зауваження, що при прив’язуванні «знизу» пакети, які несуть певну мітку, передаються у напрямку, протилежному напрямку передачі інформації про прив'язку цієї мітки до FEC.

Другий варіант називається прив’язкою мітки до FEC «зверху» (upstream label binding), тому що в цьому випадку прив’язка переносимої мітки до того FEC, якому належить цей пакет, створюється тим же LSR, який поміщає мітку до пакета. Тобто творець прив'язки розташований «вище» (ближче до відправника пакета), ніж LSR, до якого пересилається цей пакет. При прив'язці «зверху» пакети, які переносять певну мітку, передаються в тому ж напрямку, що й інформація про прив'язку цієї мітки до FEC.

LSR створює або знищує прив'язку міток до FEC через певну подію. Така подія може бути ініційована або пакетами даних, які слід пересилати маршрутизатором LSR, або керуючими (маршрутизуючими) інформаціями (наприклад, інформацією про маршрутизацію протоколу OSPF), які повинні оброблятися LSR. Коли створення або знищення прив'язки ініціюється пакетами даних, це називається прив'язкою до даних. Коли створення або знищення прив'язки ініціюється керуючою інформацією, воно називається прив'язкою під впливом керуючої інформації (control-driven).

LSR також підтримує пул "вільних" міток (тобто мітки без прив'язки). Після первинного встановлення LSR пул містить усі мітки, які LSR може використовувати для локального їх розташування до FEC. Саме потенціал цього пулу визначає, зрештою, скільки пар «label-FEC» можуть одночасно підтримувати LSR. Коли маршрутизатор створює нову локальну прив'язку, він бере мітку з пулу, коли маршрутизатор знищує раніше створену прив'язку, він повертає мітку, пов'язану з цією прив'язкою, назад до пулу.

1.3.4. Операції над мітками

FEC формується шляхом аналізу адресних префіксів, які розподіляються за внутрішнім протоколом маршрутизації та використовуються для створення шляхів LSP по секціях, є два можливі режими маркування:

• незалежне призначення (тобто незалежне створення шляхів LSP);

• впорядковане призначення (тобто впорядковане створення LSP-шляхів).

Незалежне призначення. При незалежному призначенні мітки кожен LSR, незалежно від інших подій, вирішує прив’язати мітку до виявленого FEC та повідомити LSR, який знаходиться вище, про цю прив'язку. Ця ситуація схожа на традиційну маршрутизацію, яка виконується в звичайних мережах IP при виявленні нових маршрутів. Якщо LSR налаштований на незалежне маркування, то повідомлення Label Mapping протоколу LDP, передається цим LSR, коли виникає будь-яка з наступних ситуацій:

• LSR розпізнає новий FEC за допомогою таблиці переадресації та призначає мітку донизу за власною ініціативою;

• LSR отримує повідомлення від вищерозташованого маршрутизатора про запит мітки для FEC, який міститься в таблиці пересилань;

• наступний маршрутизатор для FEC замінюється іншим одноранговим вузлом сеансу LDP і активується механізм виявлення закільцьованих маршрутів;

• змінюються атрибути прив'язки "label-FEC";

• інформація про зв'язування міток була отримана від нижчестоячого маршрутизатора в ситуації, коли не було створено верхнього зв’язування, або було активовано механізм виявлення зворотного зв'язку, або змінили атрибути прив'язки мітки-FEC.

Упорядкований прийом. Цей метод присвоєння міток має більше обмежень, ніж попередній, у тому сенсі, що прив'язка мітки до певного FEC відбувається лише тоді, коли LSR або виступає в якості вихідного вузла для цього FEC, або вже отримав інформацію про зв'язування мітки-FEC з нижчестоячого маршрутизатора. Якщо LSR використовує впорядкований режим маркування, повідомлення Label Mapping надсилається підлеглими LSR, при виникнені будь-якої з наступних ситуацій:

• LSR розпізнає новий FEC за допомогою таблиці переадресації і є для цього вихідним маршрутизатором FEC;

• LSR отримує повідомлення про запит мітки від маршрутизатора вихідного потоку для FEC, присутнього в його таблиці переадресації, або є вихідним маршрутизатором для цього FEC, або прив'язка мітки, призначена йому знизу;

• наступний маршрутизатор для FEC замінюється іншим одноранговим вузлом сеансу LDP і активується механізм виявлення циклу;

• змінюються атрибути прив'язки "мітка-FEC";

• інформація про зв'язування міток була отримана від маршрутизатора нижчестоячого, коли не було створено верхнього зв’язування, або активовано механізм виявлення зворотного зв'язку, або змінили атрибути прив'язки мітки-FEC.

Технологія MPLS використовує два режими розподілу міток: нижчестоячим LSR по запиту вищестоячого або нижчестоячим LSR за власною ініціативою. Режим розподілу нижчесточим за запитом вищестоячого потоку використовується для створення шляхів LSP на секції.

Це дозволяє вищестоячому LSR явно вимагати прив'язування мітки до певного FEC від сусіднього нижчестоячого LSR. Режим розповсюдження міток нижчестоячого за власною ініціативою застосовується тоді, коли нижчестоячому LSR потрібно "поширювати" мітки вищестоячим LSR, хоча вони не запитували у нього це в явному вигляді.

Режими збереження міток. Ще одна характеристика використання міток - режим їх збереження. Коли LSR вищого рівня отримує ярлик від LSR нижчого рівня, який наразі не суміжний з ним з точки зору цього FEC, він повинен визначитися з цією міткою: або використовувати її (тобто "тримати" її прив'язку до FEC) або відмовитися. MPLS використовує два основні режими зберігання міток:

• ліберальний режим,

• консервативний режим.

У ліберальному режимі вищестоячий LSR зберігає будь-які прив'язки до міток FEC, які він отримав від несуміжних нищестоячих LSR (за течією, тобто мітки, що надходили до нього транзитом). У консервативному режимі вищестоячий LSR відкидає такі мітки, тобто викидає їх. Перевага ліберального режиму полягає в тому, що якщо нищестоящий LSR стає сусіднім маршрутизатором з точки зору FEC, вам не потрібно змінювати прив'язку мітки-FEC. Це дозволяє набагато швидше реагувати на зміни маршруту.

Фіксовані значення міток приведено нижче:

• 0 - «IPv4 Explicit NULL Label». Ця мітка повинна знаходитися на дні стека міток. Вона вказує, що стек повинен бути витягнутий з пакета, і подальша маршрутизація цього пакета повинна грунтуватися на заголовку IPv4.

• 1 - «Router Alert Label». Ця мітка може знаходитися в будь-якому місці стека міток за винятком його дна. Коли приходить пакет, що містить таку мітку нагорі стека, він доставляється місцевому програмному модулю для

обробки. Подальша маршрутизація буде проводитися або по нищележачий мітці, або на основі інформації, що міститься в заголовку протоколу мережевого рівня або інкапсульованих в нього протоколів. При пересиланні пакета мітка Router Alert Label повинна бути знову поміщена наверх стека міток. Використання цієї мітки регламентовано в RFC 2113 і аналогічно використанню опції Router Alert в IP-пакетах.

• 2 - «IPv6 Explicit NULL Label». Ця мітка повинна знаходитися на дні стека міток. Вона вказує, що стек повинен бути витягнутий з пакета, і подальша маршрутизація пакету повинна грунтуватися на заголовку IPv6.

• 3 - «Implicit NULL Label». Ця мітку LSR може привласнювати і поширювати, але пакети їй ніколи не позначаються. Коли LSR, згідно LIB, повинен замінити (swap) мітку, що знаходиться вгорі стека, а нова мітка є Implicit NULL Label, то замість заміни, LSR видаляє (pop) стек міток.

• 4 - 15 - Значення зарезервовані для подальшого використання.

• 16 - 1023 - використовуються для статичних LSP.

1.4. LSP тракт

Побудова мережі MPLS або формування LSP здійснюється заздалегідь, до отримання робочих пакетів у мережі. LSP генеруються автоматично на запит або вручну мережевим адміністратором. LSP організовуються перед сеансом передачі даних або коли виявляється певний потік даних. Протокол LDP займається призначенням міток LSP. Основним завданням розподілу міток є організація та підтримання LSP-шляхів, включаючи визначення кожної мітки FEC у кожному LSR шляху LSP. LSR використовує протокол розподілу міток для інформування вищестоячого LSR про призначення "мітка FEC".

Нищестоячий LSR може безпосередньо повідомляти про зв'язування мітки-FEC до вищестоячого LSR, що називається прив’язкою по ініціативі нищестоячого (unsolicited downstream). Крім цього, можливе оповіщення про прив’язку, передане нищестоячим за вимогою (downstream on demand), коли

вищестоячий LSR запитує прив’язку у нищестоячого LSR. Організований LSP завжди є одностороннім. Трафік зворотного напрямку йде по іншому LSP. Технологія MPLS підтримує наступні два варіанти створення LSP:

• послідовна маршрутизація через ділянки маршруту (hop-by-hop route) - кожен LSR самостійно вибирає наступну ділянку маршруту для цього FEC. Ця методологія аналогічна тій, що зараз використовується в мережах IP. LSR використовує існуючі протоколи маршрутизації, такі як, наприклад, OSPF;

• явна маршрутизація (ER) - аналогічно методу маршрутизації відправника. Вхідний LSR (тобто LSR, з якого потік даних надходить у мережу MPLS) вказує ланцюг вузлів, через які проходить ER-LSP. Вказаний шлях може бути не оптимальним. Уздовж шляху ресурси можуть бути зарезервовані для забезпечення QoS вказаного трафіку даних. Це сприяє оптимальному розподілу трафіку по всій мережі та дозволяє надавати диференційовані послуги потокам трафіку різних класів, сформованим на основі прийнятих правил та методів управління мережею.

Висновок по розділу 1:

В розділі було розглянуто умови, які привели до появи такої як технології MPLS, основні компоненти мережі та їх функціональні можливості. Технологія MPLS на даний момент часу є перспективним та прогресивним рішенням для розподілення ресурсів системи, для забезпечення менеджменту трафіку.

2. Аналіз протоколів технології MPLS

2.1. Протокол OSPF

2.1.1. Метрики OSPF-протокола

OSPF (Open Shortest Path First) - це динамічний протокол маршрутизації, який базується на технології стану зв’язку і використовує алгоритм Дійкстра, щоб знайти найкоротший шлях.

Open в імені протоколу означає, що специфікація протоколу маршрутизації вільно поширюється, і ви можете самостійно змінювати функції протоколу, його реалізацію, вдосконалювати та змінювати. Міжнародна спільнота IETF розробила дві специфікації протоколу OSPF - RFC 1131 та RFC 2328.

Протокол OSPF реалізує принцип вартості шляху (принцип стану каналу), метрика представлена у вигляді ефективності зв'язку в каналі: чим менша метрика, тим ефективніша передача даних по каналах зв'язку. Для обчислення показників для передачі інформації через мережеві канали OSPF доступна наступна формула:

метрика = 10^8 /швидкість передачі в бітах в секунду.

За цією формулою обчислені, наприклад, такі метрики:

• Канал зі швидкістю ≥ 100 Мбіт / с відповідає метриці 1.

• Мережа Ethernet / 802.3 відповідає метриці 10.

• Тракт E1 2.048 Мбіт / с відповідає метриці 48.

• Тракт T1 1.544 Мбіт / с відповідає метриці 65.

• Канал 64 Кбіт / с відповідає метриці 1562.

• Канал 56 Кбіт / с відповідає метриці 1 785.

• Канал 19.2 Кбіт / с відповідає метриці 5208.

• Канал 9.6 Кбит/с відповідає метриці 10416.

OSPF будує окрему таблицю маршрутизації для кожної метрики. OSPF вибирає маршрут на основі пропускної здатності каналу. Інша можлива метрика — затримка — визначає час у мікросекундах, необхідний маршрутизатору для обробки, встановлення черги та передачі пакетів. Коли існує декілька маршрутів з однаковим метричним значенням, маршрутизатори можуть використовувати всі ці маршрути для передачі пакетів, забезпечуючи балансування навантаження. Маршрутизатор OSPF розміщує всі маршрути з однаковими значеннями метрики в таблиці маршрутизації, і балансування навантаження між маршрутами відбувається автоматично. Використовуючи OSPF, LSR відображає графік видимої для нього граф домену MPLS, де для кожної пари сусідніх вершин графа (маршрутизаторів) вказується ребро (канал), що з'єднує їх, і метрика цього ребра.

2.1.2. Алгоритм Дійкстра

Алгоритм Дейкстри був введений Едсгером Дійкстра в 1956 р. Використовуючи цей алгоритм, в мережі MPLS OSPF обчислює найкоротші шляхи між заданим LSR — вершиною графа — та всіма іншими вершинами. Результатом алгоритму є таблиця, де для кожної вершини графа мережі MPLS вказується перелік ребер, що з'єднують його з усіма іншими вершинами цього графа по найкоротшому шляху. Приклад роботи цього алгоритму представлений на рис. 7.

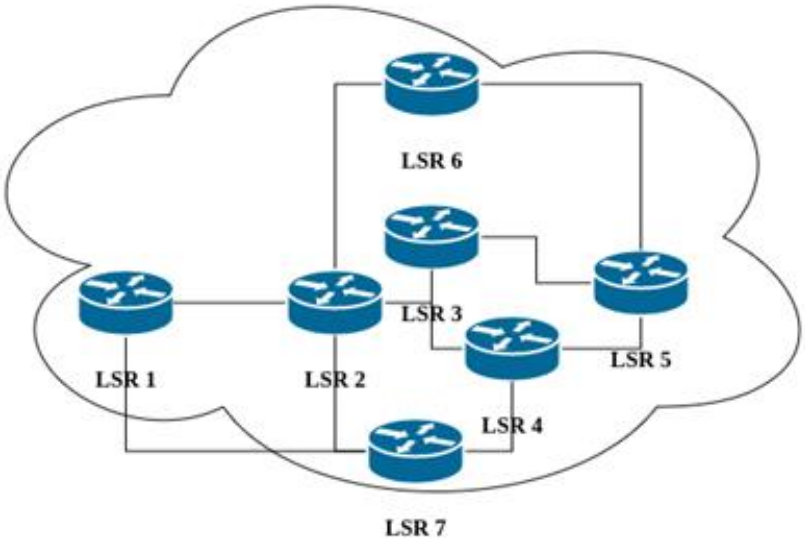

Рис. 7. Ілюстрація роботи алгоритма Дійкстри

Нехай A — безліч оброблених вершин, тобто вершин, найкоротший шлях до яких від заданої вершини LSR4 вже знайдений; B — безліч залишилися вершин графа (тобто безліч вершин графа за вирахуванням безлічі A); C — упорядкований список шляхів.

Крок 1. Визначити A = {LSR4} і B = {всі вершини графа, крім LSR4}. Помістити в список C всі односигментні (довжиною в одне ребро) шляхи, що починаються з LSR4, в порядку зростання їх метрик.

Крок 2. Якщо C порожній або перший шлях в C має нескінченну метрику, то відзначити все вершини безлічі N як недосяжні і закінчити роботу алгоритму.

Крок 3. Розглянемо l - найкоротший шлях в списку C. Видалити l з C. Нехай LSR * - останній вузол в l. Якщо LSR * ∈ A, перейти до кроку 2; інакше l є найкоротшим шляхом з LSR4 в LSR *; перенести LSR * з B в A.

Крок 4. Побудувати набір нових шляхів, які розглядатимуться, шляхом додавання до шляху l всіх односегментной шляхів з LSR * в B. Метрика кожного нового шляху дорівнює сумі метрики l і метрики відповідного односегментной відрізка, що починається в LSR *. Додати нові шляхи в

упорядкований список С, помістивши їх на потрібні місця у відповідності зі значеннями метрик. Повернення до кроку 2.

Якщо між двома вузлами мережі існує декілька маршрутів з близькими за значенням метриками, протокол OSPF дозволяє розподіляти трафік по цих маршрутах в пропорції, відповідної значенням метрик.

2.1.3. Структура OSPF-пакета

IP - транспортний протокол для OSPF. Пакети OSPF мають однаковий 24-байтовий заголовок (рис. 8) із такими полями:

Номер версії (Version Number). Вказує номер версії протоколу OSPF, який використовується маршрутизатором, який генерував цей пакет.

Тип пакету (Packet Type). Один з п’яти типів пакунків, обговорених у наступному параграфі.

Довжина пакета (Packet Length). Довжина пакету OSPF в байтах, включаючи заголовок та вміст.

Ідентифікатор маршрутизатора (Router ID). Ідентифікує вихідний маршрутизатор пакету. Кожному маршрутизатору в межах області присвоюється унікальний 32-розрядний ідентифікатор, і OSPF використовує ці ідентифікатори для вибору маршрутизаторів DR та BDR. Адміністратор може встановити ці значення вручну або вони будуть встановлені автоматично.

Ідентифікатор області (Area ID). Ідентифікує область, звідки прийшов пакет OSPF. Зона 0 завжди має ідентифікаційний номер 0,0.0.0.

Контрольна сума (Checksum). Використовується для контролю цілісності пакету OSPF. Стандартна контрольна сума IP для всього вмісту пакету OSPF, за винятком 64-бітного поля аутентифікації, обчислюється як сума 16-бітових пакетних слів в додатковому коді.

Тип аутентифікації (AuType). Визначає процедуру аутентифікації, яку слід використовувати для цього пакету. Серед можливих варіантів: відсутність аутентифікації, простий пароль, шифрування. Якщо включена проста функція пароля, маршрутизатор формуватиме суміжні стосунки лише з тими маршрутизаторами, які мають той самий пароль. Поле типу аутентифікації становить 16 біт.

Дані аутентифікації. 64-бітове поле, яке використовується процедурою аутентифікації.

Рис. 8. Заголовок OSPF-пакета

Протокол OSPF використовує пакети 5 типів:

• Тип 1. Привітання (Hello).

• Тип 2. Опис бази даних DD (Database Description).

• Тип 3. Запит відомостей про стан каналів (Link State Request).

• Тип 4. Коригування відомостей про стан каналів (Link State Update).

• Тип 5. Підтвердження отримання відомостей про стан каналів (Link State Acknowledgement).

2.2. Протокол BGP в MPLS

На сьогодні BGP - єдиний динамічний протокол маршрутизації, який використовується для обміну маршрутами між автономними системами (AS).

Побудова будь-яких корпоративних мереж, і навіть досить простих, супроводжується впровадженням внутрішніх протоколів динамічної маршрутизації.

Його головне призначення полягає саме в передачі інформації від одного маршрутизатора BGP до інших маршрутизаторів BGP про наявність інших автономних мереж та їх структури, тим самим формуючи ієрархічну схему маршрутизації, що з'єднує різні вузли та автономні мережі в єдину мережу MPLS / IP і дозволяє вільно встановлювати зв’язок між невідомими одна одній системам. Необхідність розділення глобальної мережі на автономні пов'язана з тим, що якщо велика кількість маршрутизаторів намагатиметься взаємодіяти один з одним, трафік буде перевантажувати пропускну здатність мережі і глобальна мережа вийде з ладу. BGP задається як сеанс зв'язку між двома вузлами, і оскільки паралельно буде виконуватися багато BGP-сеансів, що працюють в мережі, один маршрутизатор може бути залучений до декількох таких сеансів. Під час сеансу BGP повідомлення обмінюються через TCP-з'єднання між одноранговими протоколами BGP. Версія 4 протоколу BGP суттєво відрізняється від попередньої реалізації BGP і фактично включає два окремих протоколи: протокол EBGP - External Border Gateway Protocol, - використовуваний для маршрутизації між автономними системами, і протокол IBGP - Internal Border Gateway Protocol, - використовуваний для маршрутизації всередині автономної системи. Протоколу BGP показаний на рис. 9.

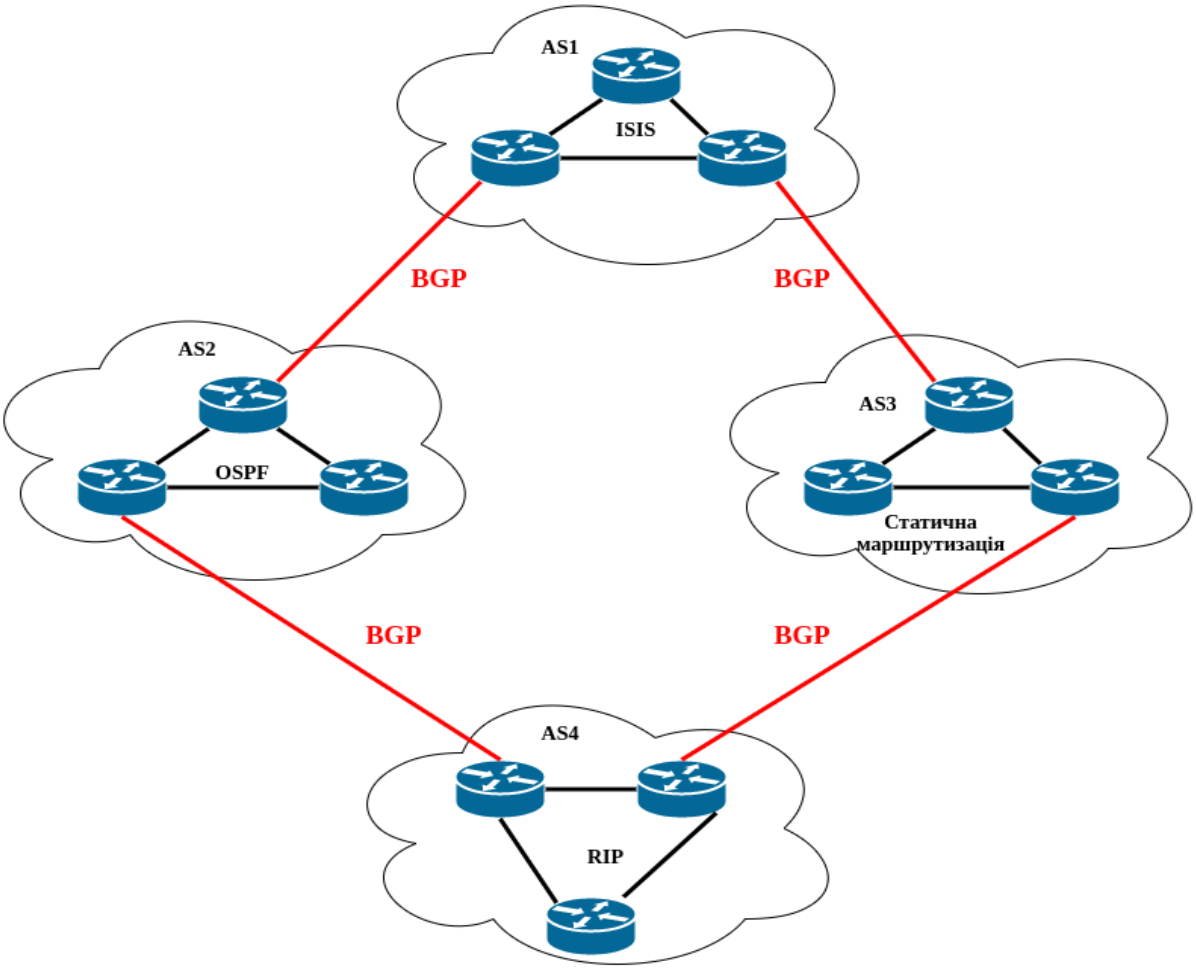

Рис. 9. Протокол BGP

BGP нерозривно пов'язаний з концепцією автономної системи (AS — Autonomous System). Тому невід'ємною частиною є нумерація автономних систем, яка є основним структурним підрозділом протоколу BGP. У контексті BGP доцільно додати до цього те, що визначення автономної системи тісно пов'язане з концепцією точок доступу до мережі PoP IP (точка присутності), якої автономна система зазвичай має дві або більше для балансування навантаження та надійність. Діапазони чисел AS описані в інструкційному документі RFC 1930. У більшості випадків ASN призначається постачальником послуг Інтернет з підмножини його номерів, що становить від 1 до 65535. Існує три класи автономних систем АС:

• системи з множинною адресацією (multihomed),

• тупикові, що мають тільки один вихід в Інтернет (single-homed),

• багатоканальні транзитні мережі (multihomed transit).

Є три типи маршрутизаторів BGP: спікери, прикордонні шлюзи і рівноправні маршрутизатори BGP.

Спікери — це роутери автономної системи BGP. Під час налаштування цих маршрутизаторів їм слід присвоїти номер автономної системи, до якої вони належать. Під час однорангового спілкування спікери BGP обмінюються повними копіями таблиць маршрутизації під час початкового двостороннього сеансу, включаючи повторні запуски.

Спікери BGP, які з’єднують два або більше автономних систем, називаються прикордонними шлюзами (Border Gateways). Вони потрібні автономним системам у випадку, коли автономна система зв’язується з іншими АС MPLS/IP мережі за допомогою протоколу EBGP.

Відповідно до принципів мережевої маршрутизації, під час сеансів зв’язку спікери BGP обмінюються інформацією про маршрутизацію, про топологію та метричні характеристики відповідних ділянків мережі. Такий обмін відбувається між одноранговими маршрутизаторами (BGP peers) автономної системи. Рівноправні маршрутизатори BGP не повинні бути безпосередньо підключені один до одного, однак, між двома спікерами BGP завжди повинен бути стандартний метод зв'язку, щоб вони могли ініціювати сеанс зв'язку. Коли BGP встановлює сеанс зв'язку між двома рівноправними маршрутизаторами, між якими немає прямого зв'язку, це з'єднання називається одноранговим зв’язком із пересиланням по протоколу EBGP (EBGP multihop peering).

Зовнішній протокол прикордонного шлюзу (EBGP — Exterior Border Gateway Protocol) використовується для встановлення зв'язку між спікерами BGP різних автономних систем, включаючи зв’язок між постачальниками послуг Інтернету та точками доступу POP, а також між великими корпоративними мережами та постачальниками послуг. Для того, щоб будь-який спікер, який перебуває за межами АС, міг успішно обмінюватися

інформацією з цим АС, він повинен знати про його місцезнаходження та знати свою адресу. Запис маршруту BGP містить інформацію про те, як передавати інформацію з однієї точки в іншу, призначену для адреси xxx.xxx.xxx.xxx. Маршрути вказують мережеву IP-адресу (якщо мережа не знаходиться в автономній системі, до якої належить передавальний пристрій) та адресу маршрутизатора, яка буде використана для наступного переадресації. Коли у спікера є інформація про маршрут, якою потрібно ділитися з іншими спікерами BGP (внутрішніми або зовнішніми), він повідомляє їх про цей маршрут. Повідомлення про маршрут або сповіщення - це метод, за допомогою якого один спікер надає іншим спікерам інформацію про маршрут або корекцію маршруту, який показує динаміків BGP один про одного та про мережі. Динамічний маршрут - це маршрут, про який спікер дізнається в результаті обміну інформацією про коригування з іншими маршрутизаторами. Цей процес обміну забезпечує динамічний перерозподіл маршрутів BGP.

IBGP — Internal Border Gateway Protocol (протокол шлюзу внутрішнього кордону) використовується для встановлення зв'язку в автономній системі. Різниця між IBGP та EBGP полягає в повідомленні маршруту сусіднього маршрутизатора, який знаходиться в тому ж АС. При переведенні на номери зі списку АС можуть виникати циклічні шляхи. Щоб уникнути цього, IBGP не додає номер АС до списку AS_Path. Створюється також граф зв’язків IBGP між прикордонними маршрутизаторами тієї ж автономної системи.

Необхідно також розглянути таке поняття та методологію як карта маршруту. Карта маршруту дає вам можливість вибрати, які маршрути будуть перерозподілятися між спікерами. Карти маршрутів працюють лише на рівні сповіщень про коригування і не фільтрують маршрути, що надходять на маршрутизатор. Карта маршруту містять метрики, за допомогою яких виконується алгоритм маршрутизації. Використовуючи карти маршрутизації,

адміністратор мережі може змінювати метрики та змінювати алгоритм передачі даних між АС та всередині неї.

Структура загального заголовку протокола BGP показана на рис. 10.

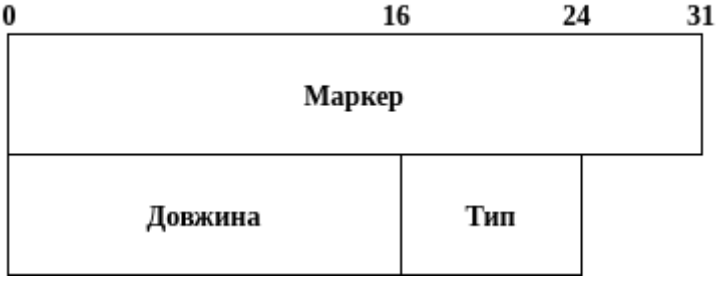

Рис. 10. Структура загального заголовку BGP

Загальний заголовок містить чотири поля:

Довжина (Length), розміром в 2 байта, визначає загальну довжину пакета BGP в байтах.

Тип (Type) - однобайтовое поле, яке вказує тип повідомлення.

Є змінне число байтів, що пересилаються. Максимальний розмір повідомлення BGP складає 4096 байт. Протокол BGP має повідомлення чотирьох типів: запит з'єднання OPEN, повідомлення про оновлення UPDATE, повідомлення NOTIFICATION, повідомлення підтвердження зв'язку Keepalive.

Запит з'єднання OPEN: його передає маршрутизатор, якому потрібно організувати сеанс зв'язку з іншими BGP-маршрутизаторами. Прийняв це повідомлення маршрутизатор підтверджує встановлення з'єднання, передаючи повідомлення KEEPALIVE. На рис. 11 показана структура заголовка повідомлення OPEN.

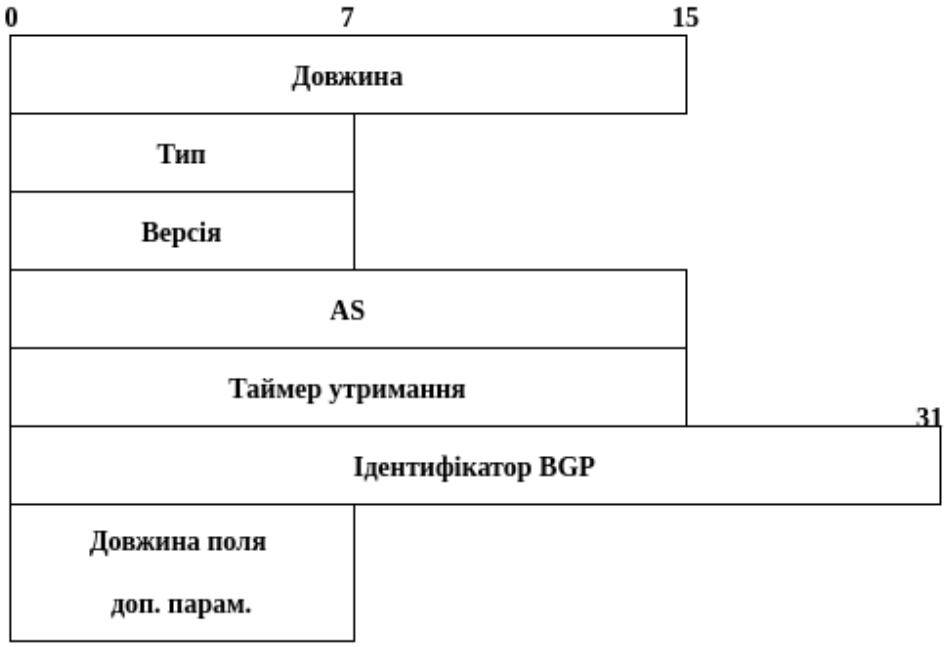

Рис. 11. Заголовок повідомлення OPEN

Поле версія (Version), довжиною 1 байт, вказує застосовувану відправником версію протоколу BGP. Поле автономна система (AS), довжиною 2 байта, містить унікальний номер тієї AS, в яку входить спікер-відправник. Поле таймер утримання (hold-time), теж 2-байтовое, визначає максимальний інтервал часу між прийомом повідомлень KEEPALIVE і UPDATE. Поле ідентифікатор BGP, довжиною 4 байта, однозначно визначає відправника і зазвичай містить MAC-адреса маршрутизатора і його ASN.

Повідомлення про оновлення UPDATE: Повідомлення UPDATE розсилається маршрутизаторів BGP з метою внесення змін до таблиці маршрутизації. На рис. 12 представлена структура цього повідомлення, в яке входять три блоки: інформація мережевого рівня про досяжності (NLRI - Network Layer Reachability Information), атрибути маршрутів і недосяжні маршрути.

Рис. 12. Структура заголовку повідомлення про оновлення

Повідомлення NOTIFICATION: таким видом повідомлення обмінюються при виникненні помилки. Структура такого заголовка представлена на рис. 13.

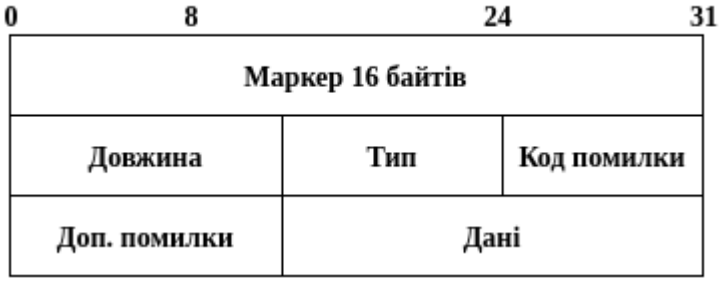

Рис. 13. Структура заголовку повідомлення NOTIFICATION

Повідомлення про підтвердження зв'язку: повідомлення підтвердження зв'язку KEEPALIVE відправляється, щоб підтвердити прийом повідомлення OPEN, переданого маршрутизатором AS. Повідомлення KEEPALIVE містить тільки заголовок і забезпечує скидання таймера утримання з'єднання.

2.3. Протокол сигналізації RSVP

RSVP - це протокол сигналізації, який забезпечує резервування ресурсів, управляє ними з метою надання інтегрованих послуг і емулює тим самим виділені канали в IP-мережах.

Протокол резервування ресурсів (RSVP) був розроблений у дослідницькому центрі Xerox в Пало-Альто. Резервація в моделі IntServ виконується за допомогою вже згаданого протоколу резервування ресурсів (RSVP). Це протокол сигналізації, як і протоколи сигналізації телефонних мереж. Однак специфіка пакетних мереж дейтаграм природно залишає свій слід. Так, параметри комутації в мережах IP не є атрибутом резервування, оскільки IP-пакети в будь-якому випадку (при резервуванні або без нього) будуть передаватися маршрутизаторами на основі записів у таблиці маршрутизації.

Є два способи впорядкування шляху LSP: незалежно або упорядковано. У першому випадку LSR приймає рішення про те, як прив’язати мітку до конкретного FEC: він вибирає мітку та повідомляє про її прив’язку вищестоящому LSR, який запрошує мітку. У другому випадку прив'язка мітки до FEC запускає вихідний LSR, і процедура прив’язки послідовно рухається вгору до вхідного LSR. Впорядкований метод кращий для запобігання закольцьованих маршрутів. Запит на бронювання RSVP включає два варіанти, один з яких описує метод бронювання, а другий описує вибір відправника, який визначає напрямок потоків. RSVP визначає три стилі резервування:

• роздільне, з фіксованим фільтром - стиль Fixed Filter (FF),

• спільне явне - стиль Shared Explicit (SE),

• спільне, з довільною фільтрацією - стиль Wildcard Filter (WF).

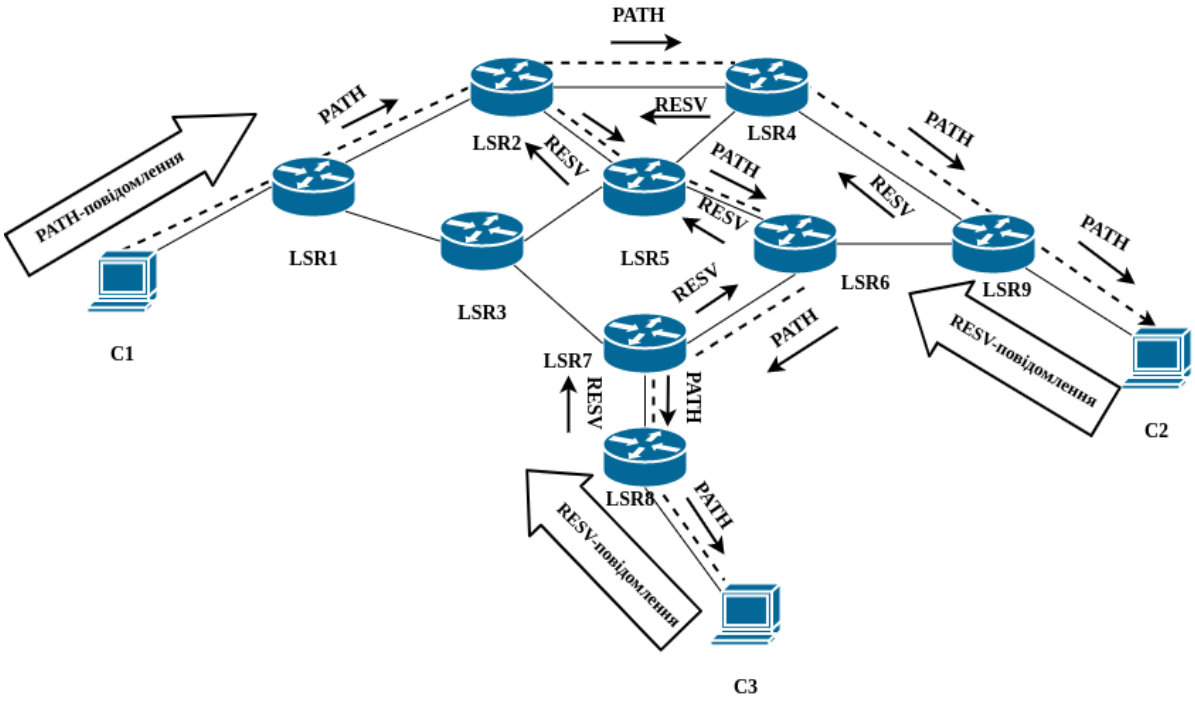

Рис. 14. Резервування ресурсів проколом RSVP

1. Джерело даних (комп'ютер C1 на рис. 14) надсилає одержувачам за унікальною або груповою (як на малюнку) адресою спеціальне повідомлення PATH, яке вказує рекомендовані параметри для якісного прийому трафіку: верхня та нижня межі пропускної здатності, затримки та варіації затримок. Ці параметри складають специфікацію трафіку джерела. PATH-повідомлення передається маршрутизаторами мережі в напрямку до всіх зазначених в груповій адресі одержувачам. Крім того, максимально допустима швидкість і максимальні розміри пакетів потоку можуть бути додатково вказані.

2. Кожен маршрутизатор, який підтримує протокол RSVP, отримавши PATH-повідомлення, фіксує «стан шляху», яке включає попередній адресу джерела PATH-повідомлення, тобто останній за часом крок у зворотному напрямку (що веде до джерела). Це необхідно для того, щоб відповідь приймача пройшов по тому ж шляху, що і PATH-повідомлення.

3. Після отримання PATH-повідомлення приймач відправляє в зворотному напрямку маршрутизатора, від якого він отримав це повідомлення, запит на резервування ресурсів, тобто RESV-повідомлення. На рис. 14 показано два

приймача, комп'ютери С2 і С3. На додаток до специфікаціям трафіку джерела С1 (які містять параметри для якісного прийому його трафіку: верхні і нижні межі пропускної здатності, затримки і варіації затримки) RESV-повідомлення додатково включає специфікацію запиту приймача, в якій вказуються необхідні приймача параметри якості обслуговування, і специфікацію фільтра , яка визначає, до яких пакетам сеансу застосовувати дане резервування (наприклад, по типу транспортного протоколу і номеру порту). Разом специфікації запиту і фільтра є дескриптор потоку, для якого виконується резервування. Запитувані параметри QoS в специфікації запиту можуть відрізнятися від зазначених в специфікації трафіку. Наприклад, якщо приймач вирішує приймати не всі посилаються джерелом пакети, а тільки їх частина (що вказується в специфікації фільтра), то йому потрібна, відповідно, менша пропускна здатність.

4. Кожен маршрутизатор, лоддержівающій протокол RSVP уздовж висхідного шляху, отримавши RESV-повідомлення, перевіряє, по-перше, чи є у маршрутизатора ресурси, необхідні для підтримки запитуваної рівня QoS, а по-друге, чи має користувач право на резервування ресурсів. Якщо запит не може бути задоволений (через нестачу ресурсів або помилки авторизації), маршрутизатор повертає повідомлення про помилку відправнику. Якщо запит приймається, то маршрутизатор посилає RESV-повідомлення далі вздовж маршруту наступного маршрутизатора, а дані про необхідний рівень QoS передаються тим механізмам маршрутизатора, які відповідальні за управління трафіком.

5. Прийом маршрутизатором запиту на резервування ресурсів означає також передачу параметрів QoS на опрацювання до відповідних блоки маршрутизатора. Конкретний спосіб обробки параметрів QoS маршрутизатором в протоколі RSVP не описується, але зазвичай вона полягає в тому, що маршрутизатор перевіряє наявність вільної пропускної спроможності і ємності пам'яті для нового резервування. При позитивному

результаті перевірки маршрутизатор запам'ятовує нові параметри резервування і віднімає їх з лічильників відповідних вільних ресурсів.

6. Коли останній в зворотному напрямку маршрутизатор отримує RESV-повідомлення і приймає запит, то він посилає повідомлення про підтвердження вузлу-джерелу. При груповому резервування враховується той факт, що в точках розгалуження дерева доставки кілька резервних потоків зливаються в один. Так, в маршрутизаторі LSR2 в розглянутому прикладі зливаються RESV-повідомлення від приймачів С2 і С3. Якщо для всіх резервуються потоків запитується однакова пропускна здатність, то вона потрібна і для загального потоку, а якщо запитуються різні величини пропускної здатності, то для загального потоку вибирається максимальна.

7. Після встановлення стану резервування в мережі джерело починає відправляти дані, які обслуговуються на всьому шляху до приймача (приймачів) із заданою якістю обслуговування.

2.3.1. Роль RSVP в MPLS

Мета введення протоколу сигналізації RSVP в MPLS полягає в тому, щоб LSR аналізуючи їх мітки, а не IP-заголовки, могли розпізнавати пакети, що належать тим потокам, для яких було зроблено резервування ресурсів. Таким чином, RSVP стає інструментом для розподілу міток MPLS. Коли маршрутизатору LSR потрібно передати повідомлення Resv для нового потоку, він вибирає зі свого пулу вільну мітку, створює запис у своїй таблиці LFIB, визначаючи вибрану позначку як вхідну, і потім передає повідомлення Resv, що містить цю мітку в об'єкті LABEL. При отриманні повідомлення Resv з об'єктом LABEL, що містить цю входить мітку, вищестоящий LSR вносить її в свою таблицю як вихідну для пересилки до нижчому LSR, який передав повідомлення Resv. Потім він призначає нову мітку, яка буде

використовуватися ним як вхідна мітка, і вставляє цю нову мітку в повідомлення Resv, передане наступному вищестоящому LSR.

Протокол RSVP, розширений об'єктом LABEL, підтримує пересилання пакетів по мережі MPLS (тракт LSP) тільки уздовж маршруту, обчисленого схемою традиційної маршрутизації пакетів IP. Протокол RSVP розширюється новим об'єктом - Explicit Route Object (ERO). Об'єкт переноситься в повідомленні Path і містить явно заданий маршрут, по якому має йти повідомлення. Пересилання такого повідомлення маршрутизатором визначається не адресою одержувача, що містяться в заголовку IP пакета, а змістом об'єкта ERO. Ця функція дозволяє автоматично ремаршрутизувати LSP в обхід аварійних ділянок, перевантажених областей і вузьких місць мережі.

Оскільки трафік, що проходить по LSP, визначається міткою, присвоєної у вхідному маршрутизаторі, то з точки зору протоколу IP LSP можна вважати своєрідним тунелем, що знаходиться під рівнем IP-маршрутизації. Для підтримки функцій такого тунелю (тобто вже звичного як LSP) в RSVP специфіковані нові C-типи для об'єктів SESSION, SENDER_TEMPLATE і FILTER_SPEC. Ці нові типи називаються LSP_TUNNEL_IPv4 і LSP_TUNNEL_IPv6. Так як об'єкти обох типів функціонально ідентичні і розрізняються лише форматом адреси, з яким вони працюють.

2.4. LDP-протокол

У специфікації LDP на цей момент встановлено два типи елементів, за допомогою яких може визначатися FEC:

• Address Prefix - адресний префікс будь-якої довжини від нуля до повної адреси.

• Host Address - повна адреса хоста.

Специфікація ж протоколу LDP визначає правила, за якими встановлюється відповідність між вхідним пакетом і його LSP. Для розподілу міток можуть використовуватися різні методи:

• метод на основі топології (topology-based method) використовує стандартну обробку протоколів маршрутизації (наприклад, OSPF і BGP);

• метод на основі запитів (request-based method) використовує обробку керуючого протоколу на основі запитів (наприклад, протоколу RSVP);

• метод на основі трафіку (traffic-based method) запускає процедуру присвоєння і розподілу міток при отриманні пакету.

2.4.1. Робота протокола LDP

Протокол розподілу міток LDP - це набір процедур та повідомлень, які дозволяють LSR організовувати шляхи комутації міток, обмінюючись інформацією про прив’язки міток для FEC з LSR, а також починає, підтримує та закінчує сеанси LSP. Діалог між взаємодіючими одноранговими вузлами LSR називається сеансом LDP, під час якого кожен з взаємодіючих LSR отримує інформацію, що зв'язує мітки для FEC в інших LSR. При обміні інформацією, що стосується зв'язування «мітки-FEC» між LSR, використовуються чотири категорії повідомлень LDP:

• повідомлення виявлення (discovery messages), які використовуються для того, щоб оголосити і підтримувати присутність LSR в мережі;

• сеансу повідомлення (session messages), призначені для створення, підтримки та припинення LDP-сеансів між LSR;

• повідомлення-оголошення (advertisement messages), які використовуються для створення, зміни та скасування прив'язки мітки до FEC;

• повідомляючі повідомлення (notification messages), що містять допоміжну інформацію та інформацію про помилки.

Інша основна мета протоколу LDP - виявлення циклу для запобігання циклів два поля використовуються в повідомленнях Label Request та Label Mapping, а саме: Path Vector та Hop Count.

Повідомлення Hello: повідомлення Hello надсилається маршрутизатором через усі інтерфейси, на яких включений LDP, кожні 15 секунд на адресу 224.0.0.2, порт 646, транспортний протокол UDP. Повідомленням Hello також можуть обмінюватися між LSR, не підключеними безпосередньо. У цьому випадку повідомлення надсилається за унікальною адресою. Повідомлення Hello містять таку інформацію: Holddown Timer (таймер затримки) - період часу, протягом якого сусіди повинні надсилати щонайменше одне повідомлення Hello. Якщо сусіди пропонують різні значення, то вони повинні прийняти мінімальне. Оскільки UDP не гарантує доставку, рекомендується надсилати повідомлення Hello із періодом, тричі коротшим, ніж таймер затримки. Якщо таймер затримки дорівнює 0, то приймаються наступні значення за замовчуванням:

• 15с - для звичайних hello повідомлень на адресу all-routers;

• 45с - для повідомлень посилаються на конкретну адресу (Targeted Hello).

Встановлення LDP сесії: LDP встановлюється поверх TCP / IP. LSR1 і LSR2 при обміні повідомленнями hello дізнаються транспортні адреси один одного. Якщо транспортний адресу LSR1 більше ніж транспортна адреса LSR2, то LSR1 ставати "активним" сусідом, а LSR2 "пасивним", інакше, навпаки. Далі, LDP сесія встановлюється за наступним сценарієм:

1. Активний сусід встановлює TCP / IP сесію.

2. Активний сусід посилає повідомлення Init, що включають в себе свої параметри LDP сесії.

3. Пасивний сусід перевіряє параметри LDP сесії в повідомленні Init на предмет сумісності з локальними налаштуваннями LDP.

4. Пасивний сусід відповідає повідомленням Init, що включає в себе параметри LDP сесії.

5. Активний сусід перевіряє параметри LDP сесії в повідомленні Init на предмет сумісності з локальними налаштуваннями LDP.

6. Сесія встановлена.

Якщо на якомусь етапі відбувається щось не передбачене (приходить не той тип пакета, очікуване повідомлення не спадає взагалі, або не збігаються параметри LDP сесії в повідомленні Init і т.п.), то сесія вважається невстановленої. LSR, який знайшов помилку посилає повідомлення Shutdown або Reject своєму сусідові.

Повідомлення Init: містить наступні дані Protocol Version - версія протоколу; Keep Alive Time - максимальний час між службовими повідомленнями. A-bit, Label Advertisement Discipline - режим обміну інформацією про мітки. Можливе використання двох режимів обміну інформацією про мітки:

• 1 - Downstream on Demand;

• 0 - Downstream Unsolicited.

D-but, Loop Detection - механізм запобігання Циколія LSP. 0 - вимкнено, 1 - включений.

PVLim, Path Vector Limit - Змінна використовується для роботи механізму запобігання циклів.

Max PDU Length - LDP повідомлення групуються в PDU (Protocol Data Units) і передаються в одному пакеті TCP / IP. Max PDU Length - означає максимально можливу довжину суміщених повідомлень LDP в байтах. Сусіди можуть пропонувати різні значення, але обидва повинні вибрати мінімальне. Зауважимо, що навіть одне повідомлення упаковується всередину PDU.

Receiver LDP Identifier - Ідентифікатор простору міток (або Label Space Identifier).

Приклад обміну мітками за допомогою протоколу LDP показаний на рис. 15.

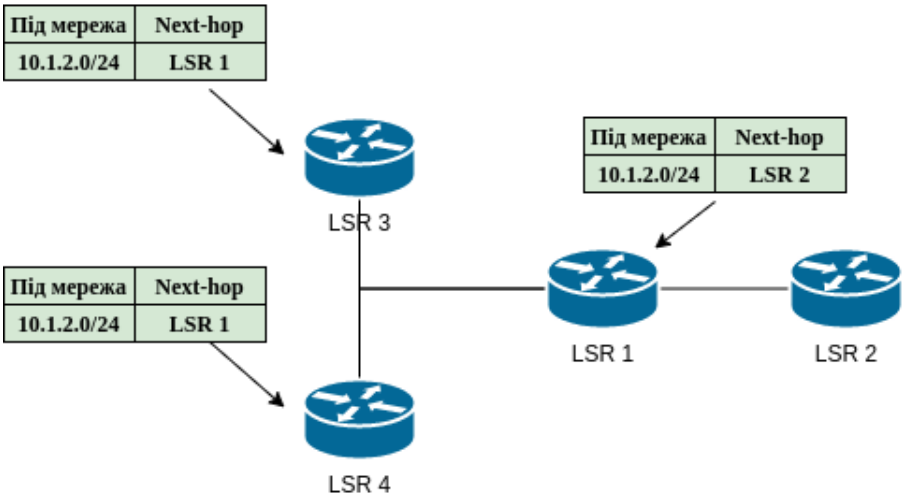

Рис. 15. Обмін мітками

2.4.2. Формат повідомлення LDP

Формат повідомлення LDP зображен на рис. 16.

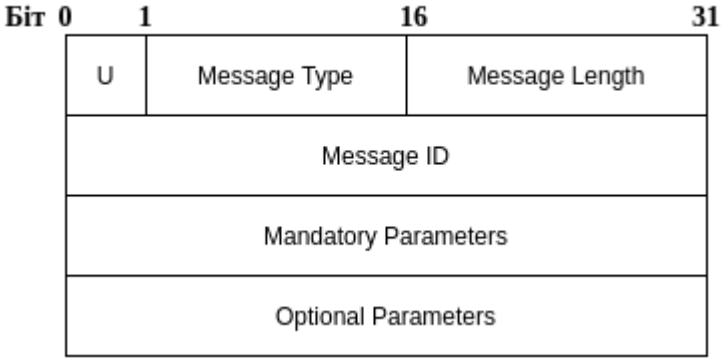

Рис. 16. Формат LDP повідомлення

Біт U - біт невідомого повідомлення. Якщо він має значення 0, то відправнику передається повідомлення про те, що тип повідомлення при вході, якщо ж біт U має значення 1, то повідомлення просто ігнорується.

Поле Message Type - ідентифікує тип повідомлення.

Поле Message Length визначає загальну довжину повідомлення в байтах, починаючи з поля Message ID і включає обов'язкові і необов'язкові параметри.

Поле Message ID має довжину 32 біта і використовується для того, щоб однозначно ідентифікувати повідомляючі повідомлення протоколу LDP.

Поле Mandatory Parameters є список обов'язкових параметрів повідомлення. Деякі повідомлення протоколу не вимагають ніяких параметрів. Якщо в повідомленні передбачені обов'язкові параметри, вони повинні бути вказані в тому порядку, в якому вони слідують у цьому повідомленні.

Поле Optional Parameters містить необов'язкові параметри. Вони, на відміну від обов'язкових параметрів, можуть з'являтися в повідомленнях в довільному порядку або не з'являтися взагалі.

2.4.3. Параметри функціонування LDP

Існує кілька параметрів функціонування LDP:

• режим обміну інформацією про мітки (Label Distribution Mode)

• режим контролю над розповсюдженням міток (Label Distribution Control)

• режим збереження міток (Label Retention Mode)

Режим обміну інформацією про мітки: між сусідами можливо використання двох режимів обміну інформацією про мітки:

• Downstream On Demand - із запитом;

• Downstream Unsolicited - без запиту.

При режимі Downstream On Demand LSR повинен запитувати мітку для створення LSP (для FEC) від сусіднього LSR, який є next-hop-му для цього FEC. При режимі Downstream Unsolicited LSR для кожного FEC знаходиться у нього в таблиці IP-маршрутизації призначає мітку і розсилає її всім своїм сусідам. Якщо для сусіднього LSR вихідний LSR є next-hop-му, то мітка встановлюється в таблицю комутації.

Режим контролю над поширенням міток: існує кілька механізмів над контролем розповсюдження влучний:

• Independent Label Distribution Control - незалежний контроль;

• Ordered Label Distribution Control - упорядкований контроль.

При використанні незалежного контролю над поширенням міток LSR може виділяти мітки для FEC своїм сусідам навіть у разі, якщо LSR не має вихідний мітки для себе від наступного LSR. Якщо використовується упорядкований контроль над поширенням міток, то LSR не виділятиме мітки своїм сусідам, поки сам LSR не отримає вихідну мітку для заданого FEC від NH-LSR-а. При цьому режимі перший відсилає мітку той LSR, до якого безпосередньо приєднано FEC.

Режим збереження (Label Retention Mode):

• Conservative Label Retention Mode (стриманий режим збереження міток);

• Liberal Label Retention Mode (вільний режим збереження міток).

При використанні стриманого режиму збереження міток при знищенні маршруту на FEC мітка видаляється. Для відновлення LSP необхідно, що б мітка була заново виділена сусіднім NH-LSR-му. Якщо використовується вільний режим збереження міток, то при знищенні маршруту на FEC мітка не видаляється, а лише позначається як неактивна. І в разі, якщо маршрут на FEC відновлюється через той же NH-LSR, то мітка не вимагається, а використовується стара, статус якої змінюється на активний.

2.4.4. Сигналізація LDP-протокола

Якщо ми поєднаємо режим "нищестоячим по запиту" з упорядкованим способом розповсюдження мітки, то їх розподіл відбуватиметься наступним чином. Вхідний LSR надсилає повідомлення із запитом на мітку нищестоячому LSR, і це повідомлення поширюватиметься через мережу до вихідного LSR. Вихідний LSR відповідає сусідньому вищестоячому LSR повідомленням Label Mapping. Цей верхній LSR запам'ятовує мітку FEC для свого вихідного інтерфейсу, створює нову мітку FEC для свого вхідного інтерфейсу та інформує наступний LSR висхідного потоку про цю прив'язку

за допомогою власного повідомлення Label Mapping. Процес триває, поки вхідний LSR не отримає повідомлення Label Mapping у відповідь на його початковий запит. Сценарій сигналізації для цього випадку показаний на рис. 17.

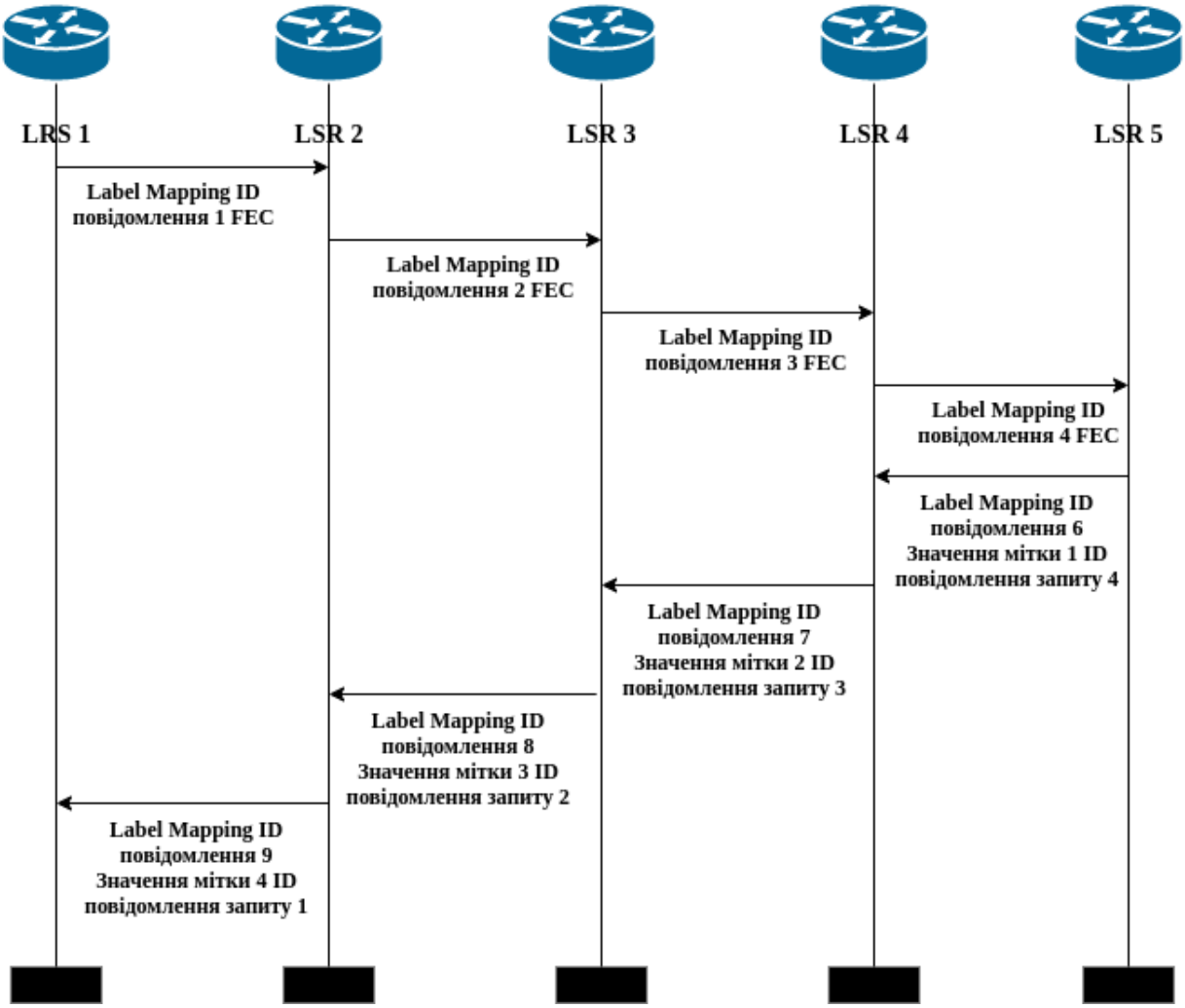

Рис 17. Режим «нищестоячий по запиту» з впорядкованим розподіленням міток

Висновок по розділу 2

В даному розділі було проаналізовано роботу таких протоколів як OSPF, BGP-4, RSVP та основного протоколу технології MPLS LDP. Перелічені вище протоколи забезпечують максимальну ефективність роботи технології MPLS за рахунок оптимізації, аналізу та побудови маршрутів ще на початку

підготовчих робіт передачі даних. Поступова робота протоколів дає можливість контролювати етапи створення, підготовки та пересилання повідомлення. OSPF – протокол, який забезпечує початкову оптимізацію мережі для маршрутизації трафіку. Протокол BGP-4 потрібен для взаємодії між автономними системами, налаштування прикордонних маршрутизаторів як всередині АС так і зовні за допомогою таких похідних протоколі BGP як EBGP та IBGP. Протокол LDP, вже безпосередньо після налаштувань зі сторони протоколів OSPF та BGP, починає пошук сусідів для створення LSP та передачі даних за допомогою міток. Протокол RSVP займається резервуванням мережевих ресурсів.

3. Структура мережі. Всі елементи, функціональна схема та принципи їх роботи. Сервіси в мережі MPLS.

Мережа, побудована за технологією MPLS (наприклад, мережа, представлена на рис. 18), є ієрархічною і являє собою дворівневу архітектуру. Структура мережі з технологією MPLS поділяє вузли IP-мережі на три типи:

• внутрішні, звані LSR або P (в мережах VPN / MPLS позначає маршрутизатор всередині мережі оператора);

• граничні, звані LER (Edge LSR - граничний LSR) або PE (Provider Edge - в мережах VPN / MPLS);

• призначені для користувача термінали, звані в мережах MPLS CE (Customer Edge).

На прикладі архітектури телекомунікаційної мережі, яка показана на малюнку 18, буде проведено аналіз роботи основних протоколів технології MPLS, такі як OSPF, BGP-4 (IBGP, EBGP), LDP. Протокол прикордонного шлюзу (BGP) встановлює зв'язок між PE-PE (IBGP / EBGP) і PE-CE (EBGP), налаштовуючи ці прикордонні маршрутизатори для взаємодії мережі клієнта і мережі провайдера, далі після роботи протоколу BGP, в мережі провайдера

побудована на MPLS, буде прокладений, вигідний з точки зору метрик, маршрут передачі даних за допомогою протоколу OSPF. Слідом включається основний протокол розподілу і передачі міток LDP на побудованих маршрутах протоколом OSPF.

Маршрутизатор LSR (або в нашому прикладі P) отримує топологічну інформацію про мережі, беручи участь в роботі алгоритму маршрутизації - OSPF, BGP. До надходження пакета в маршрутизатор P від маршрутизатора PE, починає роботу протокол OSPF. Логіка роботи протокол OSPF наступна: 1. Всі маршрутизатори в домені MPLS обмінюються HELLO-пакетами. 2. Обмінявшись пакетами, вони встановлюють сусідські відносини, додаючи кожен один одного в свою локальну таблицю маршрутизації. 3. Маршрутизатор збирають стану всіх своїх лінків (зв'язків з сусідами), що включають в себе id-маршрутизатора, id-сусіда, мережа і префікс між ними, тип мережі, вартість линка (метрику) і формують пакет, званий LSA (Link State Advertisement) . 4. LSR-маршрутизатор розсилає LSA своїм сусідам, ті поширюють LSA далі. 5. Кожен маршрутизатор, який отримав LSA додає в свою локальну табличку LSDB (Link State Database) інформацію з LSA. 6. Після обміну LSA, кожен маршрутизатор знає про все лінки, на підставі пар будується повна карта мережі, що включає всі маршрутизатори та всі зв'язки між ними. 7.На підставі цієї карти кожен маршрутизатор індивідуально шукає найкоротші з точки зору метрики маршрути в усі мережі та додає їх в таблицю маршрутизації. Потім він починає взаємодіяти з сусідніми маршрутизаторами, розподіляючи мітки, які в подальшому будуть застосовуватися для комутації. 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 в таблиці маршрутизації, яке використовується при традиційній маршрутизації.

Як видно з рис. 18, клієнтське обладнання підключено до маршрутизаторів PE. Прикордонні маршрутизатори PE виконують присвоєння мітки пакетам, які надходять від вузлів клієнта CE. Для взаємодії з різними типами клієнтських мереж маршрутизатори PE зазвичай оснащені шлюзами. Центральна частина мережі (основна мережа) включає P-роутери (літера P означає провайдера). P-роутери виконують функції комутації та управління MPLS. Передача здійснюється шляхом аналізу та заміни міток у кожному вузлі P, а управління (встановлення та зміна міток) - за допомогою протоколу розподілу міток LDP (Label Distribution Protocol). Таким чином, технологія MPLS, використовуючи заздалегідь задану послідовність міток у проміжних вузлах, передає кожен пакет у певному напрямку, тобто організований шлях комутації міток (LSP). Шляхи LSP є віртуальними, оскільки в IP-мережах методом комутації пакетів фізичні шляхи з фіксованою пропускною здатністю не можуть бути організовані. Бронювання пропускної здатності для шляхів LSP виконується статистично з урахуванням кількості трафіку, навантаження на лінію та ймовірності наявності вільного ресурсу потрібного розміру.

Структура, показана на рис. 18, описує плоску мережу, що складається з одного домену MPLS і керується протоколом внутрішнього шлюзу (IGP). Маршрутизатори PE повинні присвоїти мітку запуску пакету при надходженні в основну мережу MPLS і видалити цю мітку, коли пакет покине мережу. Маршрутизатори PE спілкуються між собою через BGP-4 для обміну інформацією про створені шляхи LSP. Роутери P виконують набагато простіші функції, ніж маршрутизатори PE. P-маршрутизатори не знають віртуальних маршрутів LSP, створених маршрутизаторами PE, і не беруть участі в обміні за допомогою протоколу кордону шлюзу (BGP), який відбувається на прикордонних маршрутизаторах PE при створенні LSP.

Особливість протоколу BGP полягає в тому, що маршрутизатор PE приймає і передає свої повідомлення про маршрутизацію не всім

маршрутизаторам, пов'язаним з ним, а лише тим, які в конфігурації вказані як його "сусіди", до того ж маршрутизатори, розташовані на багатьох кроках можуть бути «сусідами» (хоп). Якщо маршрутизатор PE, в принципі, повинен організовувати маршрутизовані маршрути LSP з комутацією міток до будь-якого маршрутизатора PE, то всі вузли PE повинні вважатися його сусідами. Це ускладнює розширення мережі. Коли вводиться новий PE, воно повинно бути «зареєстровано» у всіх існуючих PE, а кількість зв’язків між PE зросте як квадрат від числа цих вузлів. Тому можна сказати, що плоска мережа MPLS, показана на рис. 18, має погану масштабованість. Кожен LSP у такій мережі організований від одного граничного вузла PE до іншого граничного PE вузла, всі LSP є незалежними, і загальна кількість LSP, створених у великій мережі, може бути дуже великою.

Важливим недоліком плоскої мережі є поява великої кількості службової інформації у разі пошкодження мережі та при зміні маршрутів. Усунення цих недоліків забезпечується встановленням в мережі MPLS спеціальних маршрутизаторів, званих Route Reflectors (RRs), з'єднаних за принципом кожен з кожним, до яких підключені граничні маршрутизатори PE, перетворюючи плоску мережу MPLS в ієрархічна.

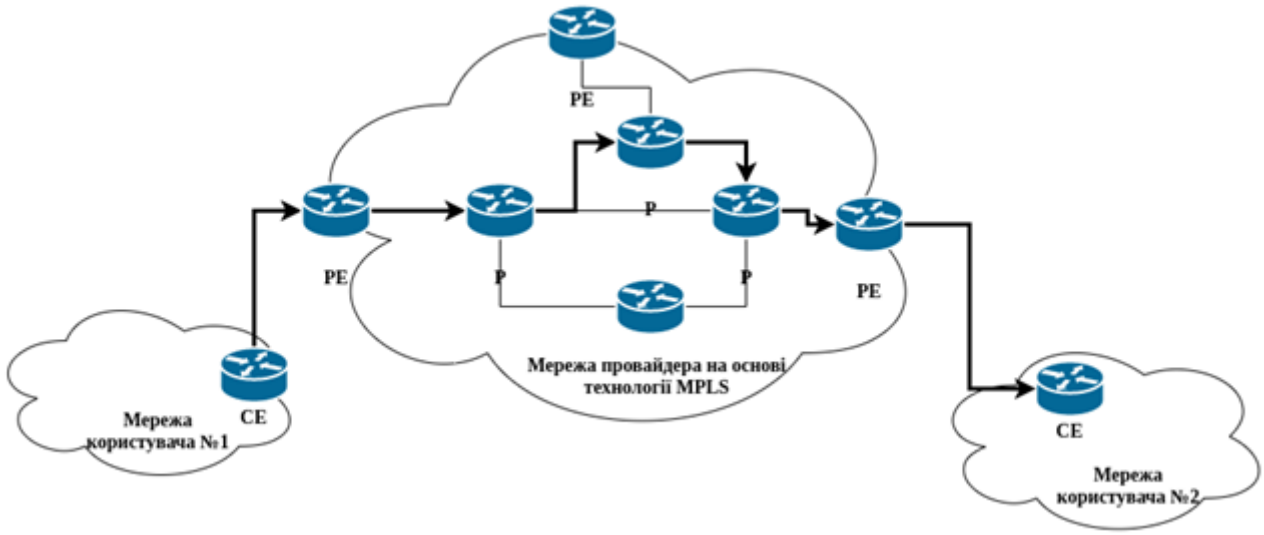

Рис. 18. Загальна мережа, яка побудована на технології MPLS

Ієрархічна побудова мережі MPLS має більш складну багатодоменну структуру, але надає ряд переваг, особливо в майбутньому, використовуючи мережу MPLS для передачі мультисервісного трафіку. В даний час концепції побудови сучасних мереж MPLS-мереж операторського класу. Провідні виробники обладнання для мереж MPLS пропонують нові мережеві архітектури, орієнтовані на надання послуг відповідно до вимог NGN. Доцільно будувати мережі MPLS у вигляді багатодоменної ієрархічної структури. Наприклад, у структурі мережі MPLS з декількох доменів маршрутизацію, засновану на принципі «OSPF області», коли маршрутні зміни за протоколом OSPF не поширюються по всій мережі, а зосереджуються лише в одному домені. З метою побудови ієрархічної мережі MPLS в мережу вводяться транзитні граничні вузли TPE, які одночасно служать також відбивачем маршруту (RR-вузли).

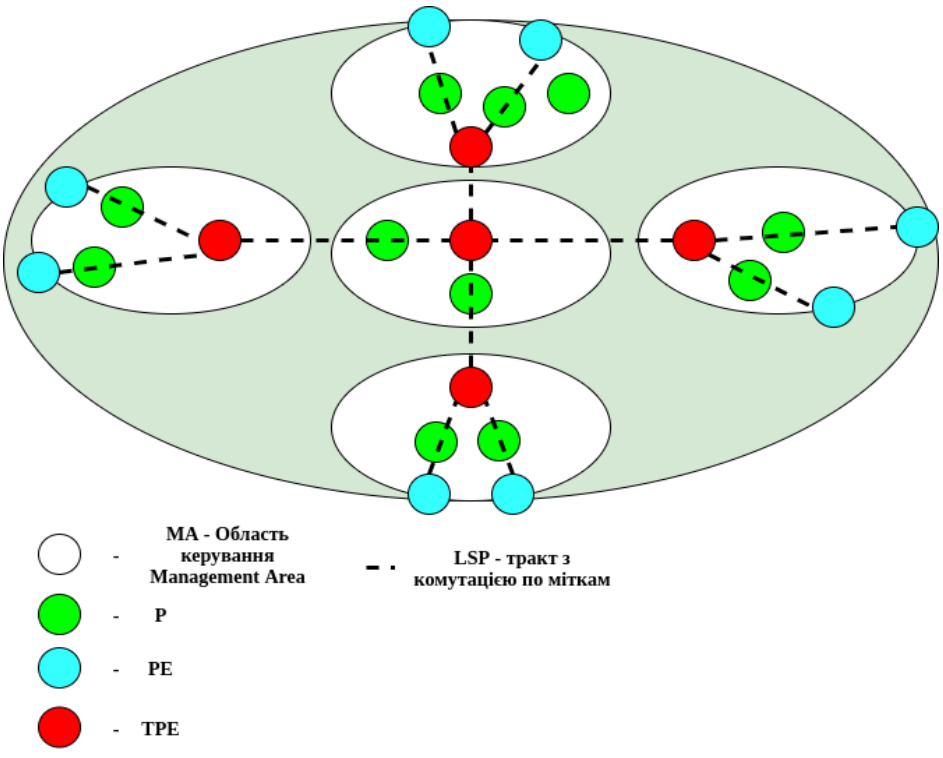

Рис. 19. Структура ієрархічної мережі MPLS

Перший IP-пристрій на вході магістральної IP- мережі — це прикордонний маршрутизатор PE, встановлений на кінцевій станції магістральної мережі та виконує деякі аналогічні функції з АМТС (в сенсі

підключення периферійних клієнтських мереж). Як зазначено, ієрархічна мережа MPLS додатково вмикає транзитні маршрутизатори (TPE), підключені на основі "кожен до кожного", які служать ВАК (вузол автоматичного комутації) з точки зору концентрації трафіку та організації зв’язків між різними територіями. У мережі MPLS без TPE потрібно встановити LSP між маршрутизаторами PE по типу "кожен з кожним", кількість яких (пропорційна квадрату кількості вузлів PE) у великій мережі буде дуже великою. За наявності транзитних вузлів кількість з'єднань різко зменшується, оскільки кожен PE переходить до власного транзитного вузла TPE, який з'єднаний з усіма іншими TPE, внаслідок чого кожен вузол PE може підключитися до будь-якого іншого вузла PE в ні більше двох транзитних вузлів ТПЕ. Якщо в структурі мережі MPLS ми вводимо вимогу, щоб кожен вузол PE виходив на два TPE та вводив обмеження кількості транзитів (не більше двох), то мережа MPLS просто вирішує питання бронювання та вирішує проблема циклічного пакету. Незалежно від архітектури, MPLS-мережі, що управляють трафіком з різними класами обслуговування, повинні використовувати технологію MPLS-TE з можливістю резервування ресурсів пропускної здатності при організації LSP, які зазвичай називаються тунелями LSP в технології MPLS-TE. Слід зазначити, що LSP можна організувати кількома способами:

• без резервування смуги пропускання і з резервування смуги;

• з жорстким виділенням смуги пропускання і з динамічним виділенням смуги пропускання (жорсткі і гнучкі LSP, відповідно).

Без використання розширеного протоколу MPLS-TE неможливо резервувати пропускну здатність при організації LSP. Якщо LSP організовані без резервування пропускної здатності, то адміністратор мережі повинен незалежно оцінити можливість завантаження кожного конкретного LSP потоками, щоб не було втрати пакету через перевантаженість мережі. Використовуючи протокол MPLS-TE, що включає модифікований протокол

резервування ресурсів RSVP-TE, можуть бути організовані тунелі LSP з різною пропускною здатністю, побудовані за допомогою багаторівневого стека міток. У технології MPLS ті LSP, які організовані за допомогою міток на різних рівнях стеку міток, називаються багаторівневими LSP. Зазвичай мережі MPLS встановлюють окремі тунелі для потоків з різними класами обслуговування.

З точки зору управління ієрархічна мережа MPLS поділена на кілька областей управління або MPLS-доменів. У кожному домені при обробці міток у вузлах TPE може бути організований перехід до іншого рівня стеку міток, за допомогою якого можна отримати доступ до іншого маршрутизаційного домену, резервувати, агрегувати потоки, змінити пропускну здатність LSP (агрегація або відключення), взаємодіяти з мережами MPLS з іншими операторами, включаючи доступ до міжнародного Інтернету.

Стек міток дозволяє створити агреговану систему шляху LSP з будь-якою кількістю рівнів ієрархії. Для підтримки цієї функції кадр MPLS, який рухається ієрархічно організованому шляху, повинен включати стільки заголовків MPLS, скільки є рівнів ієрархії на шляху. Кожен заголовок MPLS рівня має власний набір полів: label, CoS, TTL та S. Послідовність заголовків організована як стек, так що завжди є ярлик у верхній частині стека, і мітка, яка знаходиться на дні стека, першою завжди обробляється мітка на вершині стеку.

3.1. MPLS/VPN

Існує безліч різновидів віртуальних приватних мереж. Їх спектр варіюється від мереж Інтернет-провайдерів, що дозволяють управляти обслуговуванням клієнтів безпосередньо на їх площах, до корпоративних VPN, що розгортаються і керованих самими корпораціями. Прийнято виділяти три основних види віртуальних приватних мереж:

• VPN з віддаленим доступом (Remote Access VPN),

• внутрішньокорпоративні VPN (Intranet VPN)

• міжкорпоративні VPN (Extranet VPN).

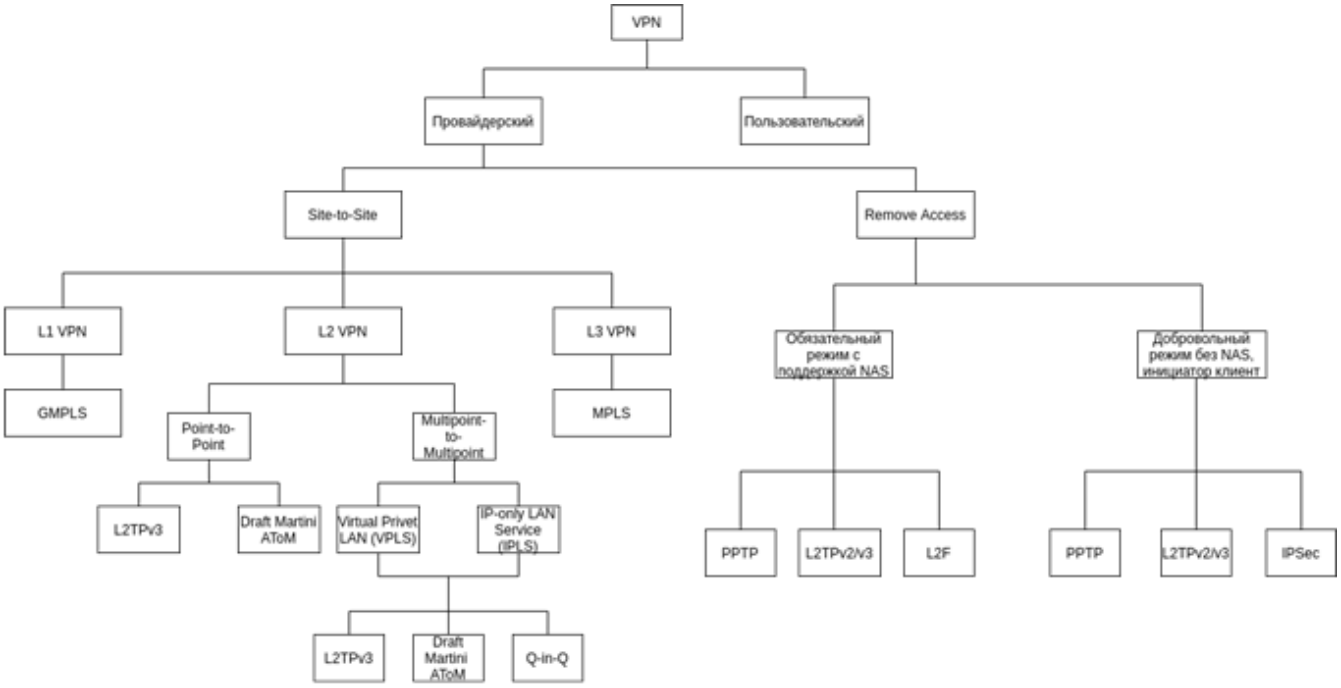

Рис. 20. Види VPN-мереж

Переваги VPN очевидні: витрати на підтримку працездатності мережі майже немає (достатньо абонентської плати за орендовані канали), організація та реструктуризація мережі зручна. Доступ до Інтернет-ресурсів безкоштовний, його може отримати будь-хто з будь-якої точки планети. При організації VPN використовуються спеціальні пристрої та механізми захисту. Для того, щоб отримати доступ до VPN, користувач проходить різноманітні брандмауери, де він має пройти автентифікацію та авторизацію. Крім того, механізми тунелювання та шифрування трафіку використовуються для передачі трафіку VPN через загальнодоступну мережу. Завдяки тунелювання пакети даних передаються через загальнодоступну мережу, як у звичайному з'єднанні "точка-точка". Для кожної пари "відправник-приймач" організований своєрідний тунель — безпечне логічне з'єднання, що дозволяє інкапсулювати дані одного протоколу в пакети іншого.

Internal VPN - це найпростіший варіант VPN: корпорації, яким потрібно організувати доступ до централізованих сховищ інформації для своїх філій та офісів, використовують недорогі інтернет-з'єднання замість орендованих ліній.

Extranet VPN - це мережева технологія, яка забезпечує прямий доступ з мережі однієї компанії до мережі іншої компанії, тим самим підвищуючи надійність комунікацій, встановлених для ділового співробітництва.

Окрім типів технологій, що застосовуються для впровадження VPN, ці мережі поділяються також рівнями моделі OSI, в якій вони працюють. Існують дві основні групи - рівень VPN 2 та рівень VPN 3. Мережеві MPLS-VPN в цій класифікації утворюють новий тип рівня VPN 2.5.

3.2. MPLS L2 VPN

Сучасні реалії такі, що кінцевий споживач телекомунікаційних послуг починає мислити абстрактно і потреби свої висловлює в категоріях Metro (Ethernet) а не WAN (IP). Тому найбільш актуальним стане завдання побудови VPN Layer 2. Використовуючи MPLS, це завдання можна вирішити кількома способами. Розглянемо деякі з них.

3.2.1. Point-to-point VPN (AtoM, EoMPLS)

Для створення VPN Layer 2 по схемі точка-точка (point-to-point) розроблена технологія Any Transport Over MPLS (AToM), що забезпечує передачу Layer 2 фреймів через MPLS мережа. AToM - це інтегральна технологія, що включає Frame Relay over MPLS, ATM over MPLS, Ethernet over MPLS, яка здатна інкопсулювать трафік будь-якого канального рівня. Для споживача мережу провайдера послуг в рамках сервісу AToM виглядає як віртуальний патчкорд.

AToM використовує безпосередні LDP сесії між граничними маршрутизаторами провайдерської мережі (PE) для встановлення і підтримки з'єднань. Безпосереднє просування пакетів відбувається з використанням стекирования міток MPLS, коли одна мітка (Top) з'єднує граничні маршрутизатори, а друга (Bottom) - визначає безпосередньо VPN клієнта (інтерфейс на PE маршрутизатор). Так як найбільш затребуваною в даний час є технологія Ethernet over MPLS (EoMPLS), то деталі функціонування AToM розглянемо на її прикладі.

EoMPLS инкапсулирует Ethernet фрейми в MPLS пакети і використовує стек міток для просування через MPLS мережа. На кожному PE-CLE (Customet Leading Edge) організовується Virtual Circuit (VC). Обов'язково встановлюються прямі LDP сесії між вхідним і вихідним PE-CLE для обміну інформацією про VC. Кожна VC складається з двох односпрямованих LSP.

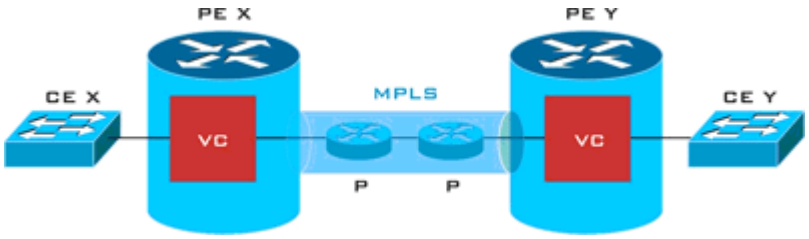

Рис. 21. Мережева структура передачі EoMPLS

Безпосередньо передача пакетів використовує стек міток верхня мітка (Top Label), звана ще Tunnel Label, використовується для досягнення вихідного (Egress) PE-CLE. Нижня мітка (Bottom Label), звана VC Label, використовується для визначення інтерфейсу на PE-CLE. VC Label забезпечується Egress PE-CLE для Ingress PE-CLE для направлення трафіку в потрібний інтерфейс на Egress PE-CLE. VC Label ототожнюється з VC ID і встановлюється на етапі VC setup.

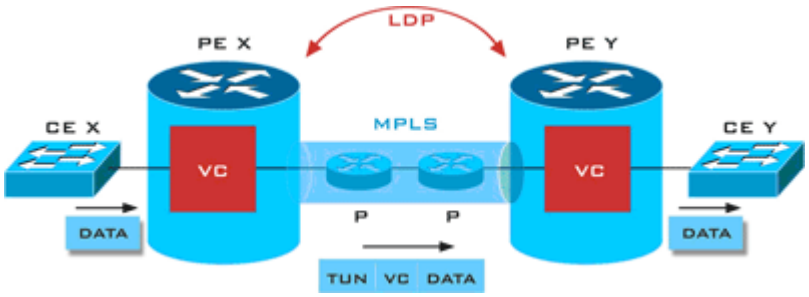

Рис. 22. Передача Ethernet кадров в мережі MPLS

3.2.2. Multi-Point VPN (VPLS)

З метою подолання обмежень point-to-point VPN розроблена технологія Virtual Private LAN Service (VPLS). VPLS - Layer 2 VPN технологія, що забезпечує багатоточкові сполуки (Multipoint Services) поверх пакетної мережевої інфраструктури. VPLS дають можливість об'єднання розподілених локальних мереж в єдину мережу.

Для споживача мережу провайдера послуг виглядає як віртуальний Ethernet свіч. При цьому мережа оператора зв'язку абсолютно прозора і не видно для мережі замовника. На рис. 23 показана логічна структура мережі VPLS.

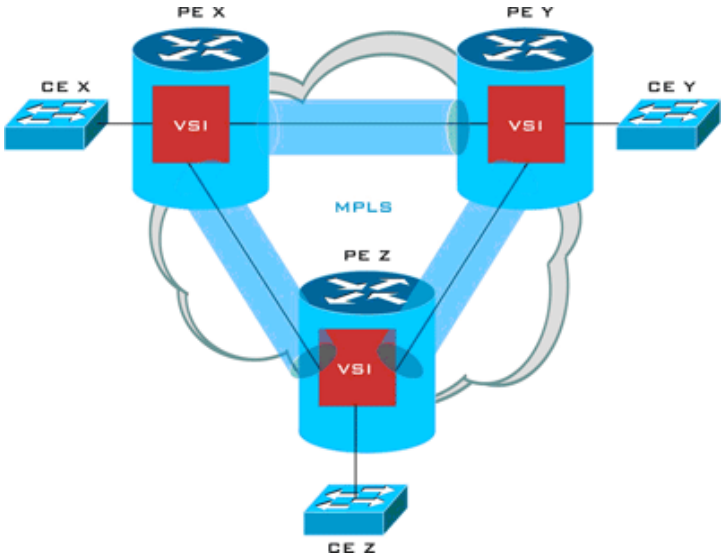

Рис. 23. Логічна структура VPLS

Для кожного VPN на кожному PE виконується Virtual Switching Instance (VSI), яка забезпечує рішення про пересилання для кожної VPLS. Ethernet фрейми коммутируются між PE пристроями, використовуючи VSI. В принципі VPLS розширює модель AToM до багатоточкових з'єднань, використовуючи ті ж методи інкапсуляції. Подальшим розвитком масштабування даної технології є Hierarchical VPLS (H-VPLS). H-VPLS увазі декомпозицію PE пристрою на два User-Facing PE (u-PE) і Network PE (n-PE).

Відмінність VPLS від AToM в тому, що AToM - p-t-p L2 сервіс, а VPLS - multipoint. У той же час MPLS L3 VPN теж multipoint, але обмежений IP трафіком. VPLS ж L2 сервіс і може підтримувати кілька високорівневих протоколів.

3.3. MPLS L3 VPN

Рівень 3: постачальник послуг братиме участь в маршрутизації з клієнтом. Замовник запустить OSPF, EIGRP, BGP або будь-який інший протокол маршрутизації, ці маршрути можуть бути розділені з іншими сайтами клієнта. VPN: інформація про передачу даних від клієнтів повністю відокремлена і захищена від інших клієнтів, не авторизовані користувачів і спрямована по мережі MPLS провайдера.

VPN на базі MPLS 3 рівня використовує однорангову модель, яка базується на протоколі граничного шлюзу (BGP) для передачі інформації. Ця масштабована одноранговая модель дозволяє корпоративним абонентам поширювати дані про маршрутизації інших постачальників послуг, що призводить до значної економії ресурсів і зниження складності операцій. Також система реалізована на протоколі MPLS, не вимагає налаштувань всіх BGP на кожному маршрутизаторі, а лише на граничних роутерах, підключених до інших клієнтів або провайдерів, на відміну від IPv4. В VPN на базі IP використовується екземпляр віртуальної маршрутизації / пересилання наступного покоління (VRF), званий Easy Virtual Network (EVN).

Це спрощує віртуалізацію мережі рівня 3 і дозволяє клієнтам забезпечити поділ трафіку і ізоляцію шляху в загальній мережі інфраструктури, усуваючи необхідність розгортання MPLS в мережі підприємства. EVN повністю інтегрований з традиційним MPLS-VPN або MPLS VPNomGRE.

MPLS дозволяє створювати віртуальні приватні мережі Layer 3, не вдаючись до тунелюванні (GRE) і шифрування (IPsec). MPLS VPN мережу ділить на дві області: IP мережі клієнтів і магістраль провайдера. Класична конструкція MPLS L3 VPN складається з наступних компонентів: граничні маршрутизатори провайдера PE, звернені до клієнтського обладнання CE, з'єднані між собою P маршрутизаторами в MPLS домені. В принципі, P маршрутизаторів може і не бути, необхідно щоб забезпечувалася зв'язність між PE. MPLS L3 VPN інфраструктура (рис.24) передбачає забезпечення ізоляції розподілених клієнтських IP мереж в рамках VPN. Тобто забезпечується тільки обмін пакетами між IP мережами однієї VPN.

У термінах MPLS VPN окреме CE підключення називається сайтом. Кожен сайт являє собою окрему клієнтську підмережа, що входить в ту чи іншу VPN структуру. Кожна VPN логічно пов'язана з одним або більше комплексів маршрутизації і переадресації (Virtual Routing and Forwarding instance — VRF).

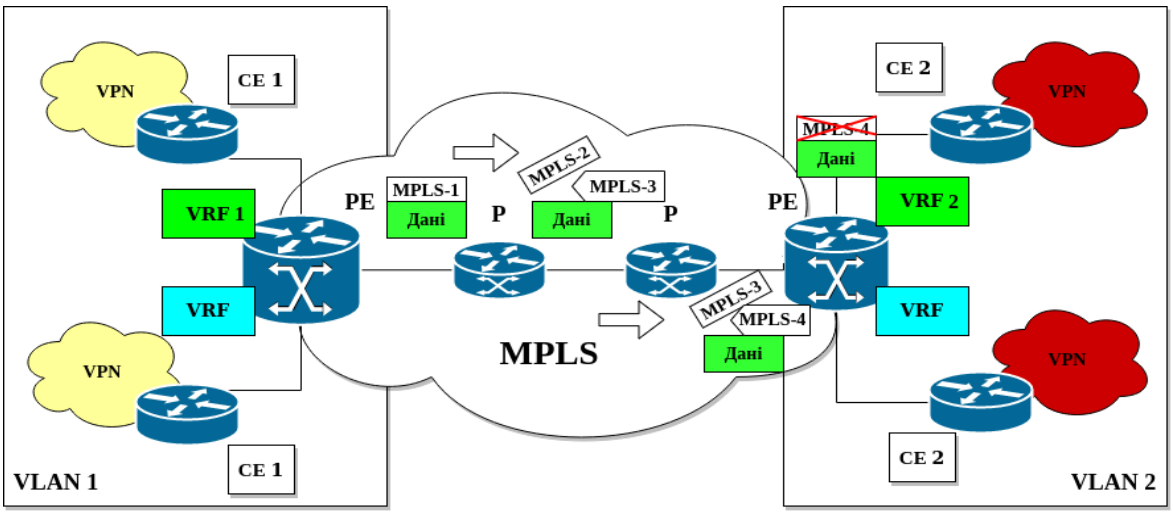

Рис. 24. Схема передачі повідомлення між VLAN1 та VLAN2 за допомогою протокола MPLS

Інтерфейси PE маршрутизаторів, звернені до CE, логічно пов'язані з індивідуальними VRF. Примірник VRF складається з таблиці маршрутизації (IPv4), отримана з неї CEF, набір інтерфейсів, які використовують VRF і побічна інформація. VRF таблиці IP маршрутизації використовуються для обміну інформацією про маршрути тільки всередині VPN мережі, тобто ззовні не можна здійснити пакетизації на маршрутизатор, що знаходиться всередині VPN (цей маршрут просто невідомий).

В рамках MPLS L3 VPN в VPN включається IPv4 клієнтської підмережі. В межах однієї VPN не допускаються рядові IPv4 адреси. Однак в різних VPN це допустимо. Звідси потенційна неоднозначність для PE маршрутизатора: різні VRF можуть містити однакові IPv4 адреси. Для отримання унікальних адрес (і відповідно маршрутів), так званих VPN-IPv4, використовується ідентифікатор VPN-Route Distinguisher (RD). VPN-IPv4 виходить за допомогою додавання до IPv4 ідентифікатора RD. В результаті PE оперує унікальними VPN-IPv4.

Для обміну маршрутною інформацією між VRF різних PE використовується MP-BGP протокол. MP-BGP маніпулює над VPN-IPv4 маршрутами. Таким чином, за допомогою MP-BGP отримуємо віртуальний зв'язок між PE (між VRF однакових VPN). Для задоволення політики експорту / імпорту додатково вводиться поняття адресата маршруту - Route Target (RT).

У підсумку виходить наступна схема. Кожен клієнтський сайт (інтерфейс на PE) має свою VRF (таблицю IPv4 маршрутизації). PE може дізнатися IP приставка клієнта різними способами (статична конфігурація, BGP, RIP, OSPF). PE поміщає IPv4 маршрут клієнта в VRF даного сайту. Крім того, за допомогою заздалегідь обраного ідентифікатора VPN, в які входить даний сайт, IPv4 маршрути (префікси) перетворюються в VPN-IPv4 маршрути і

поміщаються в MP-BGP. MP-BGP відповідно до політики імпорту / експорту пов'язує між собою всі PE маршрутизатори (їх VRF). У підсумку в VRF різних PE, але належать одній VPN, потрапляють всі маршрути по даній VPN. Причому в записах VRF Next-Hopі є PE, який би пов'язаний між собою (віртуально за допомогою MPLS).

Реальна передача пакетів (комутація) відбувається за допомогою MPLS. MPLS мітки використовуються наступним чином: пакет містить два рівня міток (використовується стек). Перша мітка направляє пакет до необхідного PE (next- hop), а друга вказує комплекс VRF, логічно пов'язаний з вихідним інтерфейсом CE маршрутизатора пункту призначення. Розглянемо на прикладі проходження пакетів в MPLS L3 VPN.

Припустимо, CE 1 посилає пакет для CE 2. Від CE 1 до PE 1 приходить пакет з DST = NET 2 (мережа по CE 2) і без міток. Даний пакет приходить з певного інтерфейсу і тому обробляється конкретним VRF 1. У VRF 1 є маршрут до NET 2 з NEXT-HOP - PE 2 і мітка VPN (мітка L1 для потрапляння в необхідну VRF 2 в PE 2). Мітку для досягнення PE 2 PE 1 шукає у своїй глобальній таблиці маршрутизації. Таким чином, PE 1 відправляє в сторону PE 2 пакет зі стеком міток: L2 для досягнення PE 2 як NEXT-HOP і L1 для досягнення потрібної VPN (VRF 2) на PE 2. мітці L2 пакет доходить до PE 2 і вона там буде видалена . PE 2 по мітці L1 з'ясовує який VRF корістовувався для досягнення NET 2. У VRF 2 для NET 2 вказаний інтерфейс PE 2 - CE 2. В сторону CE 2 пакет передається без міток у вигляді IPv4.

3.4. Fast ReRout (FRR)

Швидке перенаправлення FRR (Fast ReRoute). Оскільки з появою потужних та продуктивних маршрутизаторів з можливостю MPLS, що спрощують процес маршрутизації, поступово вимирають, основними перевагами цієї технології є, по-перше, гнучкість управління потоком руху

(насправді, головне завдання TE) та, по-друге, дозволяє тимчасово направляти трафік через запасний канал, обходячи не працююче посилання на ділянці шляху LSP, поки головна частина не зможе змінити весь LSP. Час відновлення порядку 50 мс. FRR забезпечує захист від цих втрат шляхом перенаправлення трафіку, що проходить через LSP, щоб обійти пошкоджену ланку. У цьому випадку рішення про перенаправлення приймається вузлом, який підключений до несправної лінії зв'язку. Це локальне перенаправлення може запобігти подальшій втраті пакету та отримати час для того, щоб повідомити кінцевий вузол та створити новий LSP.

На рисунку 25 показано, як FRR використовується для захисту трафіку в телекомунікаційній мережі, що відбувається між вузлами LSR1 і LSR4 при проходженні через LSR2-LSR3. Мітки 25 і 9 використовуються для LSP від LSR1 до LSR4 через LSR2 і LSR3. Для захисту зв'язку LSR2-LSR3 створюється резервний тунель від LSR2 до LSR3 через вузли LSR5 та LSR6. Мітки 38 і 15 будуть використані в цьому резервному тунелі. Коли LSR2 виявить, що зв’язок між нею та LSR3 вже недоступний, він просто перенаправить трафік, адресований LSR3, до резервного тунелю. Це робиться, розміщуючи мітку 38 поверх стека після виконання звичайної процедури заміни міток (заміни мітки 25 на мітку 9).

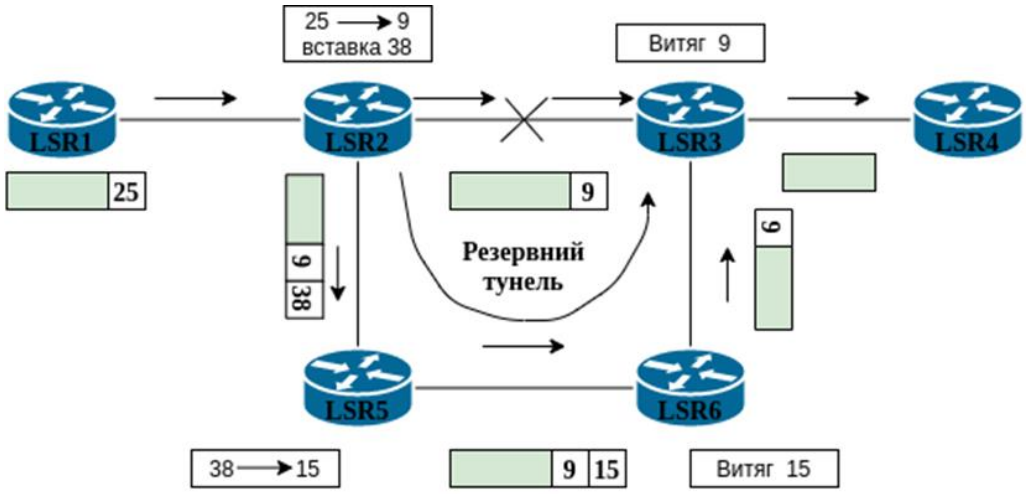

Рис. 25. FRR

3.5. Traffic Engineering

Сучасні комп'ютерні мережі, запропонувавши дешевий трафік, високу продуктивність, суперстабільні і хорошу конвергентность, позбулися таких привабливих якостей старих технологій, як можливість визначати шлях трафіку і забезпечити якість каналу від початку до кінця. Навіщо взагалі може знадобитися інжиніринг трафіку? Конвергенція телекомунікаційної мережі, розділення трафіку за допомогою такої функції MPLS як Traffic Engineering. Інжиніринг трафіку є моніторинг та моделювання потоків трафіку, а також управління трафіком з тим, щоб забезпечити потрібну якість його обслуговування шляхом раціонального використання мережевих ресурсів за рахунок збалансованої їх завантаження. Робота Traffic Engineering представлена на рис. 26.

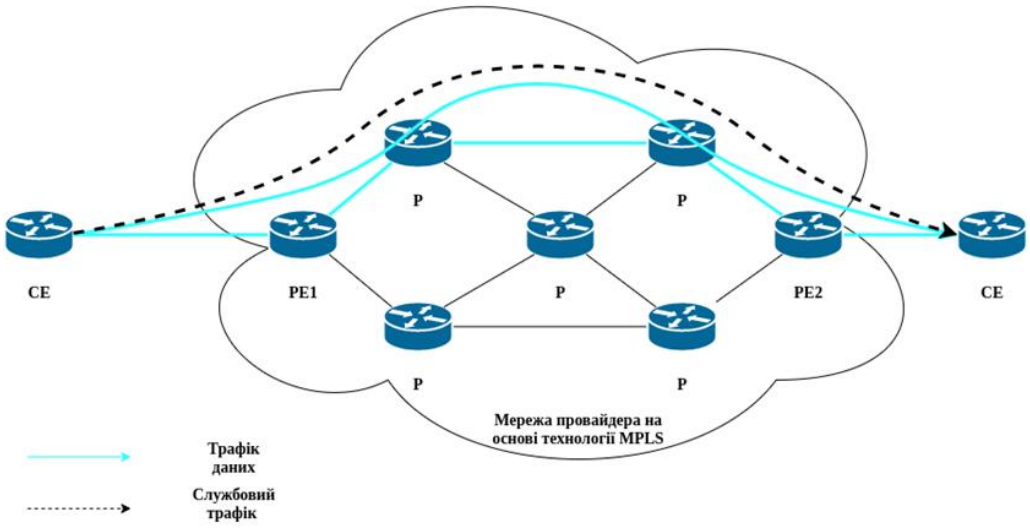

Рис. 26. Робота Traffic Engineering

Крім того, для послуг, які вимагають виконання заданих норм якості обслуговування QoS, наприклад, заданого коефіцієнта втрат пакетів і / або затримки / джиттера, інжиніринг трафіку дозволяє забезпечувати належне QoS шляхом призначення явно певних маршрутів. Адміністратор мережі

може управляти потоками трафіку, що проходять через мережу, і в примусовому порядку направляти по заздалегідь обраному маршруту пакети, які надходять до вхідного маршрутизатора LSRвх тракту LSP і відповідають класу еквівалентності пересилки FEC цього LSP до вихідного маршрутизатора LSRвих. ТЕ важливо, щоб постачальники послуг ефективно використовували свої магістралі і забезпечували високу відмовостійкість. Деякі технології на рівні 2 (L2), такі як ATM, надають можливості ТЕ, які можна використовувати для проектування потоків трафіку між джерелами і одержувачами. Однак це погано масштабується, коли між різними вузлами потрібно повне з'єднання осередків. Оскільки традиційна IP-маршрутизація заснована тільки на адресу призначення, IP-мережі самі по собі не мають механізму ТЕ. Єдиний параметр, який можна використовувати для інженерного трафіку, - це показник, пов'язаний з протоколом внутрішнього шлюзу (IGP), який можна налаштувати для переваги певного шляху. Однак це також погано масштабується в великих мережах. IP може використовуватися через ATM в оверлейной моделі для реалізації ТЕ, але це призводить до проблем з масштабністю.

З іншого боку, MPLS ТЕ забезпечує інтегрований підхід до проектування трафіку, об'єднуючи можливості ATM з проектування трафіку з гнучкістю і диференціацією IP-адрес за класом обслуговування (CoS). Природа MPLS ТЕ дозволяє уникнути проблем, пов'язаних з оверлейной моделлю. Подібно віртуальним каналам ATM або Frame Relay (VC), шлях з комутацією по мітках (LSP), автоматично створюваний MPLS ТЕ, контролює шлях потоку трафіку до конкретного місця призначення, а не чисто переадресацію на основі місця призначення.

MPLS ТЕ працює, вивчаючи топологію і ресурси, доступні в мережі. Потім він відображає потоки трафіку на конкретний шлях на основі ресурсів, які потрібні для потоку трафіку, і доступних ресурсів. MPLS ТЕ створює односпрямовані тунелі від джерела до місця призначення в формі LSP, які

потім використовуються для пересилання трафіку. Точка, де починається тунель, називається головною станцією тунелю або джерелом тунелю, а вузол, де закінчується тунель, називається кінцевою точкою тунелю або місцем призначення тунелю.

Ці компоненти працюють разом, щоб змусити MPLS TE працювати:

Розподіл інформації - це протокол стану каналу, такий як Open Shortest Path First (OSPF) або Проміжна система-проміжна система (IS-IS), який необхідний для виявлення топології. Ці протоколи були розширені для перенесення додаткової інформації, пов'язаної з TE, такий як доступна смуга пропускання та інші пов'язані параметри. IS-IS використовує нові значення довжини типу (TLV), а OSPF використовує для цієї мети оголошення про стан каналу (LSA) типу 10 (непрозорі). Інші IGP не можна використовувати для реалізації MPLS TE.

Розрахунок шляху - це маршрутизація на основі обмежень (CBR), яка використовується для знаходження найкоротшого шляху до конкретної мережі, який відповідає вимогам до ресурсів потоку трафіку. Для цієї функції використовується алгоритм Constrained Shortest Path First (CSPF), який працює на головній станції тунелю.

Налаштування шляху - це протокол сигналізації для резервування ресурсів для потоку трафіку і для установки LSP для потоку трафіку. Протокол резервування ресурсів (RSVP) використовується для цієї мети і був доповнений розширеннями TE для перенесення міток і побудови LSP. Альтернативою RSVP для MPLS TE є обмежена маршрутизація з протоколом розподілу міток (LDP), але пристрої Cisco не підтримують цей протокол.

Пересилання трафіку є компонентом, який відповідає площині пересилання MPLS TE і пересилає трафік через тунель MPLS TE, побудований у вигляді LSP модулем налаштування шляху і заснований на інформації, доступної з інших компонентів.

Можна сказати, що інжиніринг трафіку в MPLS заснований на управлінні наборами атрибутів, значення яких враховуються при виборі маршрутів для створюваних в MPLS мережі LSP і LSP тунелів. Тепер спробуємо описати загальну картину роботи програми TE в MPLS, не заглиблюючись, однак, в подробиці, розгляд яких міг би скласти окрему книгу. Основними компонентами підсистеми TE є:

● призначений для користувача інтерфейс, через який адміністратор може керувати політикою TE;

● IGP компонент, поширює інформацію про топології мережі і відомості про стан мережевих ресурсів;

● маршрутизація на основі обмежень - модуль, який проводить розрахунок маршруту в мережі MPLS на основі інформації, одержуваної від призначеного для користувача інтерфейсу і IGP компонента;

● компонент сигналізації для створення і підтримки LSP (або LSP тунелю), для управління LSP (LSP тунелем) та для бронювання системних ресурсів.

● компонент передачі даних, в якості якого виступає сама мережа MPLS.

Функціональна модель такої LSR TI мережі MPLS представлена на рис. 27.

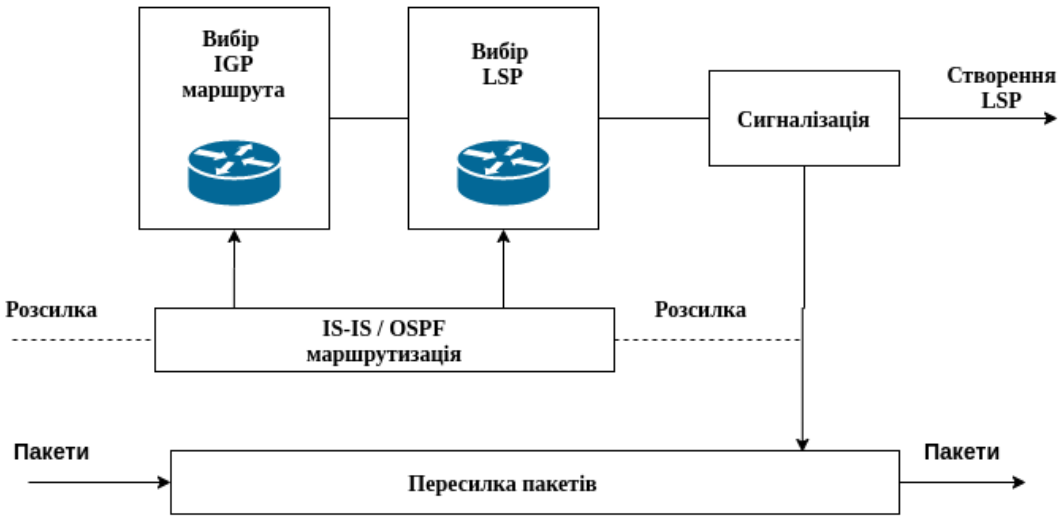

Рис. 27. Модель LSR з підтримкою TE

Примітивні MPLS TE можна досягти, вручну встановивши тунелі, що відповідають необхідним напрямкам руху.

Однак весь спектр заходів MPLS TE виглядає дещо складніше і умовно поділяється на наступні етапи (етапи).

1. Організація домену MPLS.

Існує конкретна мережева топологія, що складається з набору маршрутизаторів і каналів з певними властивостями між ними.

2. Введення обмежень.

У домені MPLS увімкнено механізм TE та описано мінімальні вимоги до мережі: початкові та кінцеві точки потоку трафіку, графіки маршрутів між ними та методи обчислення маршрутів уздовж них (явне або динамічний), необхідну пропускну здатність.

3. Вивчення параметрів мережевого середовища.

Для розповсюдження інформації про канали (атрибути посилань) використовується механізм розширення протоколів маршрутизації (протоколи стану зв'язку: IS-IS, OSPF).

В результаті кожен маршрутизатор отримує розширену топологічну інформацію про мережу, включаючи пропускну здатність кожного каналу зв'язку (ланки). Виявляється база даних посилань та їхні стани (властивості) бази даних посилань.

4. Розрахунок доріг трафіку відповідно до адміністративних вимог та можливостей мережі.

На маршрутизаторах вхідних кордонів (щодо потоку трафіку) працює спеціальний обмежений базовий алгоритм з урахуванням політики вибору найкращого шляху для тунелю LSP (тобто набору маршрутизаторів, через які слід передавати трафік): як можливості каналу, так і адміністративні вимоги (межі домену MPLS, пропускна здатність). Алгоритм перебирає посилання (їх властивості) і, як результат, обчислює маршрути (шляхи) проходження

трафіку відповідно до заходів з урахуванням накладених обмежень. Тобто, як наслідок, потрібні LSP будуються на вхідному маршрутизаторі (head-end) до вихідного маршрутизатора (head-tail) відповідно до накладених вимог щодо проходження трафіку між ними.

5. Встановлення шляхів.

Обчислені шляхи встановлюються в мережі за допомогою спеціального протоколу сигналізації, який може поширювати інформацію про явний маршрут. Сьогодні відомі два такі протоколи: RSVP-ext та CR-LDP.

MPLS підтримує два типи явних шляхів: суворий з визначенням усіх проміжних вузлів і вільний, коли вказана лише частина з них.

За допомогою RSVP ext, LSP (TE Tunnel) встановлюється по обчисленому шляху. Це автоматична установка. RSVP використовує повідомлення PATH та RESV для пересилання LSP по обчисленому шляху. У той же час, параметри пропускної здатності (контроль надходження) також відповідають.

6. Створення маршрутів з урахуванням тунелів TE.

IGP встановлює маршрут на основі наявності тунелів (як інтерфейси тунелю). Як результат, процес маршрутизації на вхідному маршрутизаторі (head-end) просто управляє тунелями LSP як інтерфейси. А в таблиці прямих маршрутів буде маршрут до головного хвоста з наступним тунелем - TE-тунель.

7. Просування пакетів.

За допомогою механізму MPLS (Label Stacking) забезпечується необхідне тунелювання та розповсюдження пакетів.

Висновок по розділу 3

Було запропоновано метод побудови базової телекомунікаційної мережі на основі технології MPLS. Було проведено аналіз роботи такої мережі, порівняння роботи мережі на базі MPLS та мережі IPv4. Також було

проаналізовано роботу технології MPLS в сумісній роботі з мережами VPN L2, VPN L3. VPLS - нова

технологія і одночасно - послуга, яка може надаватися великій кількості корпоративних замовників. Основу концепції VPLS становить ідея передачі пакетів Ethernet з мережі замовника по операторській мережі «прозорим» чином абсолютно без змін. Розглянуто такі можливості технології MPLS як FRR та TE. Перша технологія може надати запасний канал для проходження трафіку. TE дозволяє розділяти службовий та інформаційний трафік, перенаправляючи їх на окремі потоки, які потім можна буде об’єднати та передавати по окремим каналам зв’язку.

4.GMPLS

Узагальнена багатопротокольна комутація по мітках (GMPLS) - це набір протоколів, що розширює MPLS для управління іншими класами інтерфейсів і технологій комутації, відмінних від пакетних інтерфейсів і комутації, таких як мультиплексування з тимчасовим поділом, комутація рівня 2, комутація по довжині хвилі і оптоволокно. Відмінності між MPLS і GMPLS полягає в тому що він розширює підтримку декількох типів комутації, таких як TDM, довжина хвилі і комутація по волокну. GMPLS є площиною управління оптичну мережу з комутацією по довжині хвилі (WSON). Технологія GMPLS є розширенням MPLS для використання тимчасового мультиплексування (наприклад, SONET / SDH, PDH, G.709), поділу по довжинах хвиль (лямбда) і просторової комутації (наприклад, вхідний порт або волокно в вихідний порт або волокно).

Набір затверджених специфікацій Generalized MPLS з'явився в січні 2003 року. GMPLS концептуально аналогічний MPLS, але замість використання явною мітки для розрізнення LSP в кожному LSR використовується деякий фізичне властивість отриманого потоку даних, щоб визначити, до якого LSP

він належить. Архітектура однозначно розділяє компонент, або площину (сукупність функцій) управління (control plane), і компонент (площину) пересилання даних (data plane). Крім цього, площину управління поділяється на дві частини - площину сигналізації, яка включає в себе протоколи сигналізації, і площину маршрутизації, що містить протоколи маршрутизації. GMPLS фокусується на рівні управління системами, де різні технології можуть використовувати фізично відрізняються методи передачі даних і пересилання. При проектуванні технології GMPLS ставилися наступні цілі:

1. Зменшення кількості рівнів комутації та використання уніфікованих функцій управління.

2. Незалежність функцій управління і функцій передачі даних.

3. Використання стеків протоколу MPLS-TE в якості протоколів сигналізації (RSVP-TE або CR-LDP) і протоколів маршрутизації (OSPF або IS-IS) для створення і підтримки нових типів LSP.

4. Узагальнення принципів комутації міток для підтримки різних технологій передачі даних.

5. Розширення механізмів трафік-інжинірингу.

Інтерфейси LSR можна поділити на такі класи:

Інтерфейси з комутацією пакетів (PSC): інтерфейси, які розпізнають кордону пакетів і можуть пересилати дані на основі вмісту заголовка пакета. Приклади включають інтерфейси на маршрутизаторах, які пересилають дані на основі вмісту заголовок IP і інтерфейси на маршрутизаторах, які перемикають дані на основі вміст заголовка "shim" MPLS.

Інтерфейси Layer-2 Switch Capable (L2SC): інтерфейси, які розпізнають кордону кадру / ячейки і можуть перемикатися дані засновані на вмісті заголовка кадру / ячейки. Приклади включають інтерфейси на мостах Ethernet, які перемикають дані на основі вміст заголовка MAC і інтерфейси на ATM-LSR, які пересилати дані на основі ATM VPI / VCI.

Інтерфейси з тимчасовим поділом каналів (TDM): інтерфейси, які перемикають дані на основі тимчасового інтервалу даних в повторюваний цикл. Прикладом такого інтерфейсу є інтерфейс SONET / SDH Cross-Connect (XC), термінальний мультиплексор (TM) або Add-Мультиплексор падаючий (ADM). Інші приклади включають інтерфейси забезпечення можливостей G.709 TDM («цифрова оболонка») і PDH інтерфейси.

Інтерфейси Lambda Switch Capable (LSC): інтерфейси, які перемикають дані на основі довжини хвилі, на якій дані отримані. Прикладом такого інтерфейсу є інтерфейс Фотонне перехресне з'єднання (PXC) або оптичне перехресне з'єднання (OXC), яке може працювати на рівні окремої довжини хвилі. Додатковий приклади включають в себе інтерфейси PXC, які можуть працювати на рівні група довжин хвиль, тобто смуга частот і інтерфейси G.709 забезпечення оптичних можливостей.

Fibre-Switch Capable (FSC) інтерфейси: Інтерфейси, які перемикають дані в залежності від положення даних в (реальний світ) фізичні простору. Прикладом такого інтерфейсу є що PXC або OXC, які можуть працювати на рівні одного або кілька волокон.

Розширення площині управління показано на рис. 28. Створення LSP, які охоплюють тільки можливість комутації пакетів (PSC) або інтерфейси Layer-2 Switch Capable (L2SC) визначені для оригінальні площині управління MPLS і / або MPLS-TE. GMPLS розширює ці площини управління для підтримки кожного з п'яти класів інтерфейсів (тобто шари), визначені вище.

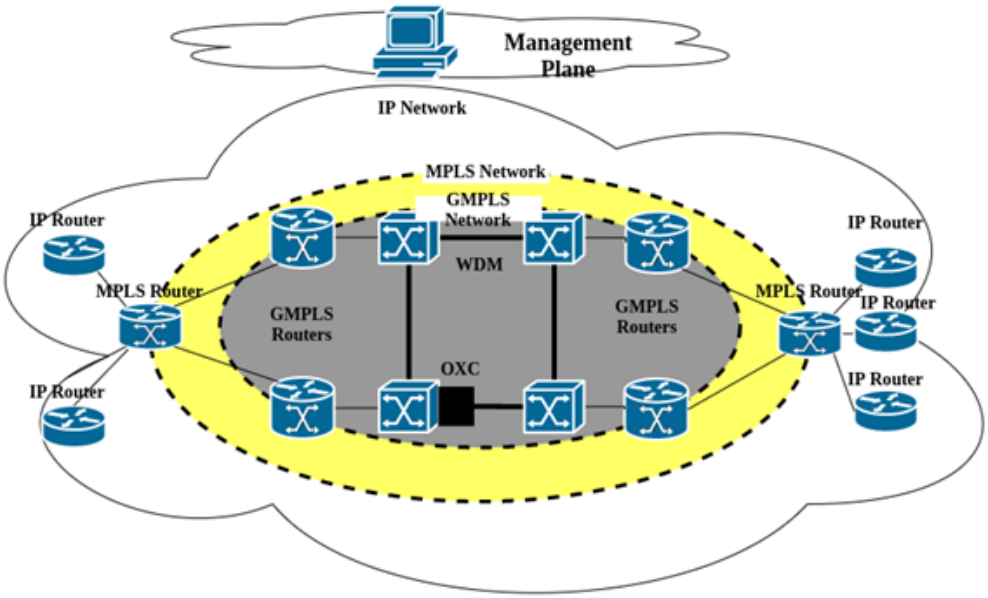

Рис. 28. Площина управління

Зверніть увагу, що площина управління GMPLS підтримує модель накладення, розширену модель і однорангову (інтегровану) модель. У найближчому майбутньому GMPLS, здається, дуже підходить для управління кожним шаром незалежно. Цей елегантний підхід сприятиме подальшому розгортанню інших моделей.

GMPLS зберігає IP-адресацію. Це означає, що IPv4 та / або IPv6-адреси використовуються для ідентифікації інтерфейсів. Така адресація використовується не тільки для інтерфейсів IP-вузлів, але і для ідентифікації будь-яких PSC-і не PSC-інтерфейсів. Для підтримки різних типів інтерфейсів GMPLS надає розширену універсальну мітку. Його новий формат містить інформацію, яка дозволяє приймальному пристрою створювати LSP і відправляти дані незалежно від його конструкції (пакетні мережі, TDM і т.д.). Такий міткою може бути одиночна хвиля, оптичне волокно або тимчасовий слот TDM. Також підтримуються традиційні мітки ATM MPLS, віртуальне з'єднання каналів (VCC), IP-shim. Універсальна мітка містить, принаймні, тип LSP, який визначає, який тип мітки буде передаватися (пакет, SDH/SONET і т.д.), тип пересилання, який вказує, чи має намір вузол використовувати

комутацію пакетів, тимчасові інтервали, світлову хвилю або FSC, і узагальнений ідентифікатор навантаження, що відображає тип навантаження, що передається через LSP (віртуальні потоки припливу, DS-3, ATM, Ethernet і т. д.). Щоб сформувати пакет LSP, необхідно послідовно запитувати ресурси на нижчих рівнях. Таким чином, в рамках GMPLS вводиться поняття ієрархії LSP (Рис. 29).

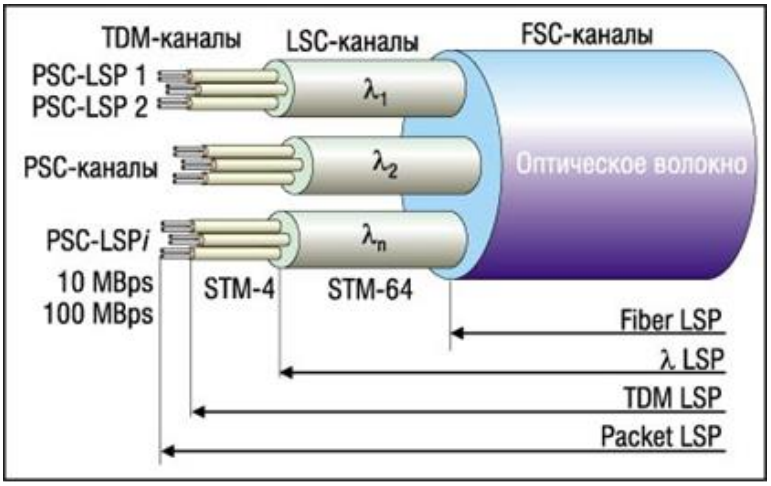

Рис. 29. LSP в GMPLS

Розглянемо процедури реалізації пакетного LSP (рис. 30) в мережі GMPLS. Таким чином, мережі з комутацією пакетів підключаються через STM-4 до кільця SDH. Кільця SDH суміщені з оптичними поперечними з'єднувачами (OXC1, OXC2). Між поперечними з'єднувачами проходить оптична лінія з смугою пропускання STM-64. Ви повинні створити LSP і передати дані з LSR1 в LSR4. Для формування пакету LSP (рис . 30, LSP pc), необхідно сформувати пакетний тунель через LSP нижчого рівня ієрархії. Для цього надішліть запит шляху (RSVP-TE) або запит мітки (CR-LDP) на нижчий рівень ієрархії. Повідомлення містить узагальнений запит із зазначенням типів LSP і навантаження (пакет, слот TDM і т.д.), а також ряд параметрів корисності. Після обробки запиту низхідний вузол пересилає повідомлення зіставлення RESV / Label, що містить універсальну мітку, яка повинна використовуватися для цього LSP. Оскільки приймач ініціює з'єднання в RSVP-TE, у випадку пакета LSP буде створено наступне:

1. LSP між OXC1 і OXC2.

2. LSP між DSC1 і DSC2 (прикордонними вузлами), потім після поширення інформації про отримані мітки в межі домену - LSP між DSC1 і DSC4 (LSP TDM).

LSP між прикордонними маршрутизаторами пакетної мережі LSR2-LSR3 і шлях LSR1-LSR4 згідно переданої в межах домену інформації про отримані мітки.

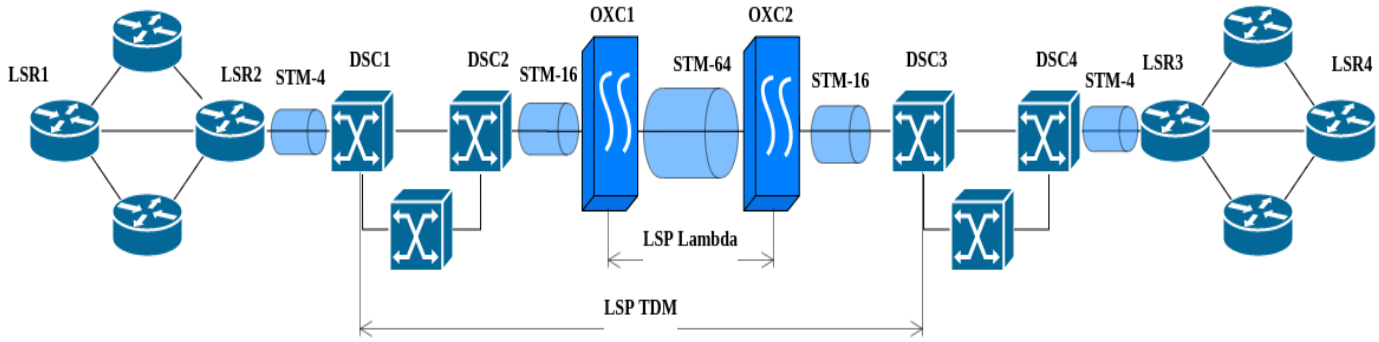

Рис. 30. Реалізація пакетного LSP в мережі GMPLS

Рішення для підвищення масштабованості. Для роботи GMPLS необхідно відправити значну кількість трафіку протоколу сигналізації та маршрутизації. Крім того, очікується, що зі збільшенням пропускної здатності оптичних каналів необхідно буде створювати і підтримувати інформацію про велику кількість з'єднань. Для підтримки високої масштабованості в рамках архітектури GMPLS було додано кілька механізмів:

1. Безадресні (ненумеровані) з'єднання (або інтерфейси). З'єднання (або інтерфейси), які не мають IP-адрес. Оскільки ці інтерфейси не визначаються IP-адресою, необхідно ввести ідентифікатор, локальний для LSR, до якого він належить. Щоб створити LSP, сусідні маршрутизатори обмінюються локальними ідентифікаторами. Пересилання ідентифікаційних даних може бути виконана з використанням протоколу LMP.

2. Угруповання (зв'язування) каналів. Коли сусідні маршрутизатори мають багато з'єднань (записи в таблиці стану OSPF / IS-IS), можна об'єднати кілька (або всі) з цих з'єднань в один запис OSPF / IS-IS. Результуючий логічний

канал однозначно визначається трьома параметрами: ідентифікатором групового каналу, ідентифікатором складеного каналу і міткою.

3. Агрегування декількох LSP в один для підвищення масштабованості, що може бути зроблено декількома способами. Специфічний для GMPLS метод агрегації-пересилання суміжності (FA) - виглядає наступним чином. Вузол оголошує LSP як канал TE в існуючій таблиці OSPF / IS-IS, якщо він має запис, який визначає необхідний маршрут для цього LSP. Після додавання FA, OSPF / IS-IS оновлює і передає інформацію про стан каналу. ФАС являють собою як адресні, так і неадресні канали. ОС може являти собою пов'язане ланка між двома вузлами. Такий підхід дозволяє поліпшити використання смуги пропускання в тому випадку, якщо вона розподіляється динамічно. З іншого боку, при об'єднанні декількох LSP в один немає необхідності підтримувати великий обсяг інформації про стан зв'язку.

Використання таких технологій, як DWDM (щільне розділення довжин хвиль), означає, що тепер ми можемо мати дуже велику кількість паралельних з'єднань між двома безпосередньо сусідніми вузлами (сотні довжин хвиль або навіть тисячі довжин хвиль, якщо використовується кілька волокон). Така велика кількість посилань спочатку не розглядалася для площини управління IP або MPLS, хоча це можна зробити.

Ще однією особливістю технології GMPLS є двонаправлений LSP. GMPLS дозволяє встановлювати двонаправлені симетричні LSP (несиметричні LSP). Симетричний двонаправлений LSP має ті ж вимоги до трафіку, включаючи розподіл трафіку, захист і відновлення, LSR і вимоги до ресурсів (наприклад, затримка і тремтіння) в кожному напрямку. При розмові про двонаправленому LSP доцільно оперувати такими поняттями, як ініціатор і Термінатор. Перше поняття означає вузол, який почав створювати LSP, а друге-кінцевий вузол. Тільки один Термінатор і один ініціатор можуть існувати для одного двонаправленого LSP. Переваги двонаправленого LSP в порівнянні з односпрямованим LSP полягають в наступному:

• знижується час встановлення двостороннього зв'язку між вузлами, а також час її відновлення,

• використовується менше службових повідомлень,

• спрощується вибір маршруту і підвищується ймовірність успішного встановлення двостороннього зв'язку,

• надається інтерфейс для обладнання SDH, що вимагає двонапрямлених зв'язків hop-by-hop,

• задовольняється побажання багатьох провайдерів послуг оптичних мереж щодо можливості мати двонаправлені оптичні LSP.

Але, незважаючи на очевидні переваги, є і недоліки, такі як необхідність присвоєння відразу двох міток одному сеансу передачі і випливають з цього наслідки - вирішення конфліктів. Наприклад, конфлікт виникає, коли вузли з обох сторін призначили однакові мітки одночасно. Вирішення цієї проблеми полягає в тому, щоб ввести такий ідентифікатор, як ідентифікатор вузла (node ID), і вузол, що має більше значення цього ідентифікатора, має пріоритет і передає повідомлення PathErr / NOTIFICATION notification.

GMPLS UNI дозволяє прозоро передавати IP-сервіси по транспортній мережі після того, як вихідний EN і кінцевий EN налаштовані на основі NMS. Таким чином, нові IP-сервіси не потребують розгортання протягом декількох місяців, і немає необхідності в обтяжливих переговорах між відділами управління IP-мережею і транспортною мережею.

Як тільки тунель GMPLS UNI був встановлений, тунель можна використовувати тільки в тому випадку, якщо він оголошений в IP-мережі для IP-служб. Існує кілька способів рекламувати тунель GMPLS UNI в IP-мережі. Наприклад, тунель GMPLS UNI може бути безпосередньо оголошений в IP-мережі в якості тунельного інтерфейсу; альтернативно, тунель GMPLS UNI може бути підключений до логічних інтерфейсів GMPLS UNI, і логічні інтерфейси оголошені в IP-мережі. В даний час NE20E використовує метод

прив'язки логічного інтерфейсу для оголошення тунелю GMPLS UNI в IP-мережі. На рисунку 31 показані деталі цього методу.

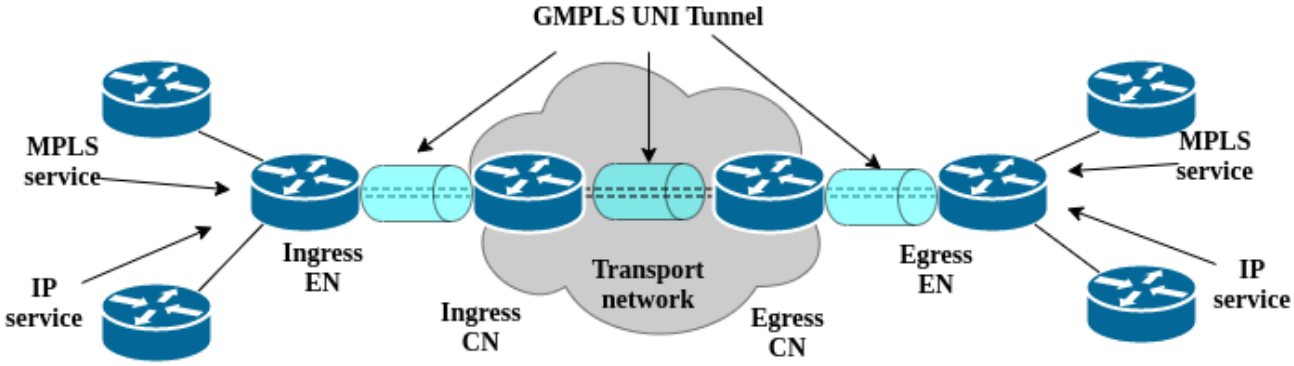

Рис. 31. GMPLS UNI Tunnel

Захист інформації переноситься в новий додатковий інформаційний об'єкт / TLV protection. Може вказувати бажану посилання безпеки для кожного посилання LSP. Інформація про захист також вказує, чи є LSP первинним або вторинним. Вторинний-це резервна копія основного шляху LSP.

Інформація про захист передається в GMPLS новим об'єктом захисту (рис.32). Використання інформації про безпеку є необов'язковим для кожного LSP. Інформація про захист відображає тип захисту, необхідний для створення LSP.

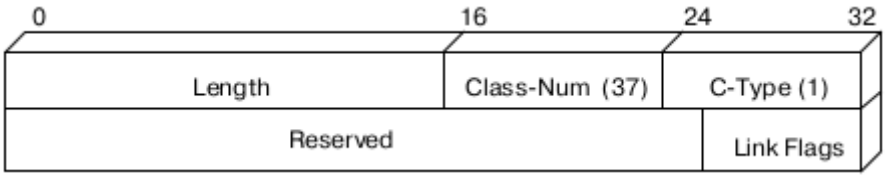

Рис. 32. Формат об’єкту Protection

Secondary (S) - значення цього біта, що дорівнює одиниці, вказує, що запитуваний LSP є вторинним.

Reserved - 25-бітове поле, що має значення нуль на передачу іігноровані на прийомі.

Link Flags - 6 бітів, що визначають бажаний тип захисту ланки; можливі значення типів захисту наведені в табл. 2.

Поле Link Flags	Тип захисту
000000	Може використовуватися захист будь-якого типу, або вона може бути відсутнім
000001	Extra Traffic - LSP повинен використовувати ланки, які використовуються для захисту інших ланок (по яких проходить первинний трафік). Ці ланки повинні бути звільнені в разі виходу з ладу захищається ланки. Таким чином це - найнижчий рівень захисту ланки
000010	Unprotected - не повинно бути захисту ланки
000100	Shared - потрібен захист шляхом резервування
001000	Dedicated 1: 1 - потрібен захист типу 1: 1
001010	Dedicated N + 1 - потрібен захист типу N + 1
010100	Enchased - потрібен захист, більш надійна, ніж дає схема N + 1

Таблиця 2. Типи захисту

У майбутньому GMPLS буде розглядатися як технологія для побудови мереж передачі даних наступного покоління, які будуть надавати принципово нові послуги, такі як пропускна здатність на вимогу і оптичні VPN (OVPN).

Висновок по розділу 4:

В даному розділі було проаналізовано мережу GMPLS, її основні частини та властивості. Було запропонована модель мережі, яка побудована на основі GMPLS, описані частини такої мережі. GMPLS дозволяє значно збільшити кількість паралельних зв’язків між вузлами в мережі. Це важливо у фотонній мережі, де між парами вузлів можуть існувати сотні паралельних з’єднань. GMPLS також полегшує швидке виявлення несправностей, усунення несправностей та перехід на альтернативні канали, мінімізуючи час простою мережі.

ЗАГАЛЬНИЙ ВИСНОВОК

В ході написання дипломної роботи було виконано поставлені задачі.

У першому розділі були розкриті умови, які спричинили виникнення такої технології як MPLS. Повною мірою описані її основні складові такі як мітки, їх структура і місце в ієрархії протоколів другого та третього рівнів, LSP тракти, їх утворення та робота та FEC.

У другому розділі було проаналізовані базові протоколи, які використовуються у тісній взаємодії з технологією MPLS. Такі базові технології як OSPF та BGP для попереднього встановлення та маршрутизації. Протокол LDP для організації шляху комутації по міткам, аналіз встановлення процедур передачі за допомогою процедур LDP. Розглянутий протокол резервування та сигналізації, в технології MPLS, RSVP.

У третьому розділі було побудовано базову телекомунікаційну мережу на основі технології MPLS. Розглянуто призначення та роботу основних частин телекомунікаційної мережі, їх взаємодія між собою. Написан алгоритм роботи протоколів OSPF, BGP-4, LDP та RSVP в мережі побудованої на основі MPSL. Також було досліджено роботу сервісів, які працюють на основі MPLS.

В четвертому розділі було запропоновано структуру GMPLS мережі. Розглянуто роботу основних частин такої мережі, інтерфейсів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ:

1. Гольдштейн А.Б. Технологія та протоколи MPLS – Санкт-Петербург, 2014 – 304 с.
2. Опис протоколу Label Distribution Protocol (LDP) [Електронний ресурс] – Режим доступу до ресурсу: https://www.opennet.ru/docs/RUS/mpls/ldpdescription.html#mozTocId461962
3. Мережі для наймолодших. Частина дев'ята. Базовий MPLS. [Електронний ресурс]– Режим доступу до ресурсу: https://habr.com/ru/post/246425/#ABOUT_MPLS
4. How MPLS Traffic Engineering works [Електронний ресурс] – Режим доступу до ресурсу: https://community.cisco.com/t5/networking-documents/how-mpls-traffic-engineering-works/ta-p/3128593
5. Структура мережі MPLS [Електронний ресурс] – Режим доступу до ресурсу: https://studopedia.su/6_47976_struktura-setey-MPLS.html
6. АНАЛІЗ ПРИНЦИПІВ ПОБУДОВИ MPLS L3 VPN
7. GMPLS — універсальний механізм комутації [Електронний ресурс] – Режим доступу до ресурсу: https://itc.ua/articles/gmpls_-_universalnyj_mehanizm_kommutacii_17845/
8. Протокол маршрутизації OSPF [Електронний ресурс] – Режим доступу до ресурсу: http://ciscotips.ru/ospf
9. Організація VPN на базі MPLS [Електронний ресурс] – Режим доступу до ресурсу: https://www.opennet.ru/docs/RUS/mpls/testbed1.html
10. Застосування MPLS [Електронний ресурс] – Режим доступу до ресурсу: https://docstore.mik.ua/manuals/ru/mpls/mplsapplication.html
11. Вступ в архітектуру MPLS [Електронний ресурс] – Режим доступу до ресурсу: https://www.osp.ru/nets/1999/12/144399/
12. MPLS - ЯК ПРАЦЮЄ І НАВІЩО ПОТРІБЕН? [Електронний ресурс] – Режим доступу до ресурсу: https://wiki.merionet.ru/seti/25/mpls-kak-rabotaet-i-zachem-nuzhen/
13. RFC 3945 Generalized Multi-Protocol Label Switching (GMPLS) Architecture [Електронний ресурс] – Режим доступу до ресурсу: https://www.protocols.ru/WP/rfc3945/