Хмельницький національний університет
Факультет програмування
та комп'ютерних і телекомунікаційних систем
Кафедра комп'ютерної інженерії та системного програмування

КВАЛІФІКАЦІЙНА РОБОТА

бакалавр
Освітній рівень

Побудова базової телекомунікаційної мережі на основі технології MPLS
Назва теми

КвРКІ.170135.17.01.07 ПЗ
Шифр

Галузь знань *12 «Інформаційні технології»*
Шифр, назва

Спеціальність *123 «Комп'ютерна інженерія»*
Шифр, назва

Освітня програма *«Комп'ютерна інженерія»*
Назва

Виконав: студент IV курсу, група КІ–17–1 _____ Дмітрієв Б.В.
Підпис Ініціали, прізвище

Керівник _____ Іванов О.В.
Підпис, дата Ініціали, прізвище

Нормоконтролер _____ С.М. Лисенко
Підпис, дата Ініціали, прізвище

До захисту допускаю:
Зав. кафедри комп'ютерної
Інженерії та системного
Програмування _____ Т.О. Говорущенко
Підпис Ініціали, прізвище

«18» червня 2021 р.

Хмельницький 2021

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Програмування та комп'ютерних і телекомунікаційних систем

Кафедра Комп'ютерної інженерії та системного програмування

Освітній рівень бакалавр

Галузь знань 12 Інформаційні технології

Спеціальність 123 Комп'ютерна інженерія

Освітня програма освітня програма «Комп'ютерна інженерія»

ЗАТВЕРДЖУЮ

Зав. кафедри Т.О.Говорущенко

" 11 " 01 2021 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ БАКАЛАВРА

Дмітрієв Богдан Васильович

Прізвище, ім'я, по батькові студента

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

Керівник проекту (роботи) Іванов О.В., доцент кафедри КІСП.

Прізвище, ім'я, по батькові, науковий ступінь, вчене звання

Затверджена наказом ректора університету від 05.02.2021 р. № 11

2. Строк подання студентом проекту (роботи) на кафедру 07.06.2021 р.

3. Вихідні дані до проекту (роботи) Завдання на дипломне проектування

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити)

Аналіз відомих рішень та засобів

Мінімізація вартості побудови телекомунікаційної мережі

Комутація пакетів з використанням міток

Побудова VPN мережі через MPLS

5. Перелік графічного матеріалу (із зазначенням обов'язкових креслень)

Схема логічної топології мережі

Схема фізичної топології мережі з віртуальним рівнем

Схема маршруту пакета в мережі з інтерпретацією на кожному з рівнів моделі OSI

6. Консультанти розділів дипломного проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдан…
Нормоконтроль	Лисенко С.М., професор кафедри КІСП		
Антиплагіат	Нічепорук А.О., доцент кафедри КІСП		

7. Дата видачі завдання «_11_» _______01_________ 2021 р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів (розділів) дипломного проекту (роботи)	Термін виконання етапів проекту (роботи)
1	Вибір напряму дослідження та узгодження тематики кваліфікаційної роботи з керівником	11.01.2021
2	Ознайомлення з предметною областю; формулювання мети та задач дослідження; визначення об'єкта та предмета дослідження	01.02.2021
3	Робота над розділом 1 – аналіз відомих засобів та рішень	01.03.2021
4	Робота над розділом 2 – Компоненти системи автополиву	01.04.2021
5	Робота над розділом 3 – Організація системи з веб-інтерфейсом	30.04.2021
6	Оформлення пояснювальної записки згідно вимог	31.05.2021
7	Попередній захист ВКР	02.06.2021
8	Захист ВКР на засіданні ЕК	Червень 2021 року

Студент ____________ Дмітрієв Б.В.

Підпис Ініціали, прізвище

Керівник проекту (роботи) ____________ Іванов О.В.

Підпис Ініціали, прізвище

№ рядка	формат	Позначення	Найменування	Кіл. листів	№ екз	Примітка
			Текстові документи			
1		КвРКІ 170139.17.01.07 ПЗ	Пояснювальна записка	62		
			Графічні матеріали			
2		КвРКІ 170139.17.01.07 Е8	Схема логічної	1		
			топології мережі			
3		КвРКІ 170139.17.01.07 Е8	Схема фізичної топології	1		
			мережі з віртуальним рівнем			
4		КвРКІ 170139.17.01.07 Е8	Схема маршруту пакета в	1		
			мережі з інтерпретацією на			
			кожному з рівнів моделі OSI			

Арк	№ докум	Підпис	Дата	КвРКІ.170139.17.01.07 ВП		
Розробив	Дмітрієв			Відомість проекту	Літера	Аркуш / Аркушів
Перевір.	Іванов				У	1 / 1
Н. контр.	Лисенко				ХНУ, КІ-17-1	
Затв.	Говорушенко		18.06			

АНОТАЦІЯ

Тема кваліфікаційної роботи: «*Побудова базової телекомунікаційної мережі на основі технології MPLS*».

Автор роботи: *Дмітрієв Богдан Васильович.*

Керівник роботи: *Іванов Олексій Валентинович.*

Пояснювальна записка: *62 с.*, 26 *рис.*, 5 *табл.*, 4 *дод.*, 40 *джерел.*

Графічна частина: 7 презентаційних слайдів

ТЕЛЕКОМУНІКАЦІЙНА МЕРЕЖА НА ОСНОВІ MPLS, КОМУТАЦІЯ ПО МІТКАМ, GNS3, LSR ТА LSP, L3VPN.

Метою даної роботи є побудова телекомунікаційної мережі з використанням технології MPLS, де основою взята проста IP мережа у яку встановлено даний протокол маршрутизації.

Методи досліджень. До уваги взяти існуючі на цей день технології та протоколи, другого та третього рівня моделі взаємодії відкритих систем, виконати їх порівняння та аналіз. Здійснюється реалізація мережі з наглядним показом руху пакетів, та управління цією конфігурацією. В результаті було наведено порівняльну характеристику та опис протоколів технології, здійснено реалізацію базової мережі використовуючи програмне забезпечення емуляції мережевих приладів, що наглядно покаже нам як виглядає зв'язок компонентів і полегшить його розробку. Результати досліджень можуть бути використані як схема побудови власної мережі для потреб компанії чи особисто

Підпис студента  Дата 17.06.2021

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

BGP– протокол граничного шлюза.

CE– кордонний маршрутизатор користувача.

FEC— це класи трафіка.

IP– інтернет протокол.

LER MPLS— це крайовий вузол MPLS мережі, який з'єднує домен MPLS з вузлом поза цим доменом.

LSP— шлях проходить через один або більше LSR тракт, по якому йдуть пакти одного і того ж FEC.

LSR - маршрутизатор, здатний пересилати пакети за технологією MPLS.

LDP– протокол розподілу міток.

MPLS– багатопротокольна комутація міток.

OSPF– протокол динамічної маршрутизації.

OSI – взаємозв’язок відкритих систем.

PE– кордонний маршрутизатор провайдера.

PVC – постійна віртуальна мережа.

RSVP– протокол резервування мережевих ресурсів.

TE– інжиніринг трафіку.

VPN– віртуальні приватні мережі.

VRF – віртуальна маршрутизація та переадресація.

ВСТУП

З давніх часів , люди завжди чимось обмінювалися, починаючи з простих речей ,наприклад:

1) шкірою диких тварин;
2) м’ясом;
3) фруктами;
4) рукописними роботами;
5) тощо.

Згодом люди зрозуміли, що обмінюватися можна швидше, використовуючи різний транспорт. Обмін речей також еволюціонував в обмін інформацією. Її передавали з таким ж принципом, записуючи її та відправляли отримувачу наприклад через пошту.

За для покращення швидкості, ми пройшли великий розвиток та дійшли до передач інформації у вигляді бітів (мінімальна кількість інформації, що дорівнює двом станам 0 або 1), електромагнітних сигналів, оптичних. Шифруючи так інформацію, ми її транспортуємо в мережу, де між собою з’єднані велика кількість користувачів. Як ми вже знаємо, телекомунікаційна мережа передає інформацію по різному. Найновіші з них є мережі, що передають інформацію за рахунок бінарних чисел через:

1) глобальні;
2) локальні;
3) міські;
4) internet;
5) intranet;
6) та віртуальні мережі.

Найкраще ми знаємо саме IP-мережу, це тобто мережа, в якій кожен абонент отримує свою власну адресу. Так ми завжди знаємо звідки та куди відправляти якусь інформац+ію.

Набираючи популярності, у таких типах мереж з’явилися багато проблем, починаючи з швидкості та закінчуючи безпекою маршруту, адже кожен міг би

вільно викрадати трафік. З'явилися інтернет провайдери які дають доступ до глобальної мережі. Вони мають при собі багато мережевих пристроїв для комутації та фільтрації трафіку. Було придумано багато протоколів, щоб покращити швидкість та кількість передач інформації.

Задля безпеки, Інтернет-провайдери нас з'єднують за допомогою такого віртуального каналу як PVC. Знаходився він в хмарі ATM або Frame Relay, але такий тип моделі майже не піддається управлінню та масштабуванню. IP-маршрутизатори не розпізнають зв'язок банкомата, тому така модель досить неефективно використовує ресурси при роботі. Ще з проблем є те, що деякі протоколи мають невисоку якість роботи, типу OSPF. Проблема закладається в тому, що такі протоколи дублюють зв'язки та спонукають до обслуговування великої кількості приладів. Такі проблеми виникають часто, особливо при підключенні 40-60 маршрутизаторів

Важливою була тема передачі інформації по по вузлах широкомасштабної мережі, тому була придумана нова технологія, яка передавала інформацію по роутерах незвичним шляхом, використовуючи не аналіз адресу призначення, зчитуючи заголовок пакету на кожному маршрутизаторі, а перетворювати заголовок в мітку, яку цей маршрутизатор розпізнає та відправляє далі. Це технологія має назву MPLS. Новітня архітектура ефективно вирішує проблему трафіку, який потрібно впорядкувати. Усуваються такі поняття як ATM – "хмари". Обробка зав'язків така ж, як і IP. Будь-який ATM комутатор може працювати нарівні з IP роутерами. При використанні MPLS, ATM комутатори отримали навички передавати IP, що дозволяє вирішити проблему масштабованості. Вирішується це за рахунок усунення накладення зв'язків IP поверх ATM. Так інтеграція різних рівнів створює маршрутизацію розподіленої моделі, в повній мірі використовує перевагу кожного рівня.

Данна інформаційна технологія впроваджується в більшості світових компаніях, які мають філіали в інших країнах, містах, континентах, як протокол корпоративної мережі.

По цій причині саме цю вибрав я тему бакалаврської роботи в якій збудую свою власну мережу з використанням технології MPLS.

Провайдерам ця технологія є максимально ефективною, тому що зменшується кількість приладів та ресурсів під час самої комутації пакетів, та збільшується швидкість. Компаніям вона також приносить багато користі, адже потрібно менше використовувати сторонніх сервісів VPN задля безпеки , адже сам MPLS шифрує інформацію пересилаючи її за допомогою міток не розкриваючи IP адресу.

Метою роботи є проектування маршруту ,використовуючи протокол комутацій за мітками, який дозволилив би передавати інформацію магістральними сітками з трансляцією широкосмугового трафіку за дуже короткий час. Також показати максимальну ефективність всього шляху. Данна технологія є масштабованою, та розв'язує проблеми обслуговування якості QoS.

Проектуючи транспортну мережу потрібно враховувати такі вимоги, як:

1) ефективність – досягається вибором технології;
2) надійність – можна досягнути правильною топологією;
3) економічність – досягається зменшуючи кількість обладнання в мережі.

1 АНАЛІЗ ПРИНЦИПІВ ПОБУДОВИ ТА ФУНКЦІОНУВАННЯ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ

1.1 Аналіз телекомунікаційної мережі та її особливості.

Телекомунікаційна мережа, являє собою систему електронних імпульсів та комутаторів, також елементів управлінь для керування їх роботою. Це дозволяє передавати та обмінюватися інформацією між декількома учасниками з’єднання.

Якщо частина користувачів з телекомунікаційними засобами інформації (наприклад з комп’ютером) бажає спілкуватися між собою за допомогою цих засобів, то їм потрібно організуватися в якусь мережу. Можна використовувати пряме посилання на користувача “з точки до точки” ,але така топологія є непрактична та дорого обходиться. Окрім того більшість посилань буде ніяк не задіяно в роботі. Сучасні телекомунікаційні мережі дозволяють уникати такі недоліки прямої топології. Створюються вузли, або комутатори які пов’язують мережі між собою. Кожен напрямок в такій мережі є каналом зв’язку. Волоконно-оптичний кабель та радіохвилі використовуються для зовсім інших каналів (рисунок 1.1).

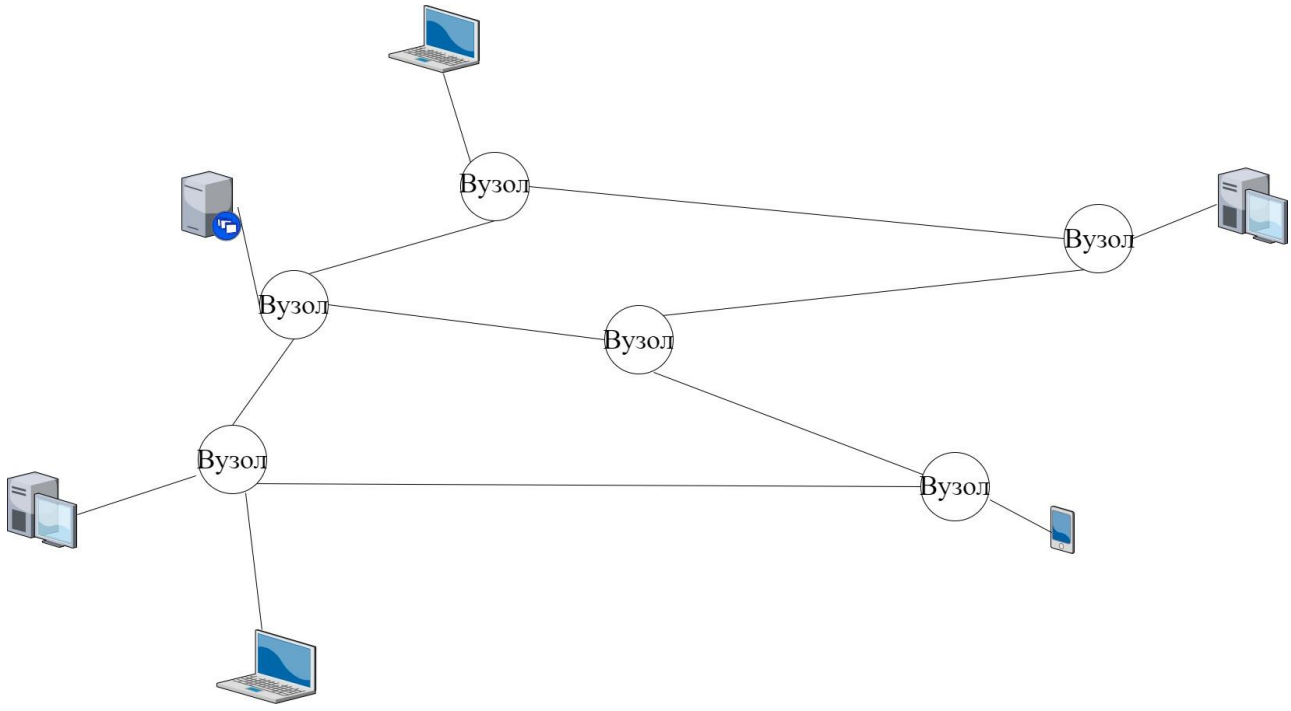


Рисунок 1.1 – Проста телекомунікаційна мережа

Розташування мереж з вузлами , з'єднаними лініями через відправника до отримувача , називають топологією мереж. В сучасному світі існують різні топології мереж.

Топологія в якій кожен пристрій підключений до іншого пристрою через певний канал є топологією «сітка». В цій топології кожен пристрій підключений до всіх інших пристроїв використовуючи канали зв'язку. Припустимо, N кількість пристроїв з'єднали між собою в топології сітки, отже загальна кількість портів яка необхідна кожному пристрою дорівнює N-1. Маючи 5 пристроїв, підключених один до одного, ми отримаємо чотири необхідних порти ,як загальні.

Переваги:

1) міцний зв'язок;
2) несправність легко діагностується;
3) забезпечується безпека та конфіденційність.

До недоліків такої системи можна віднести складність встановлення та налаштування у поєднанні з великою ціною на кабелі, адже їх має бути багато.

В топології «зірка» де всі пристрої під'єднані до одного концентратора за допомогою кабелю. Концентратор є центральним вузлом, а всі інші вузли під'єднанні до нього.

Перевагами є те, що для кожного пристрою потрібно лише один порт, адже все підключається до хаба, отже і кількість кабелів буде меншою. Недоліком є те, якщо концентратор вийде з ладу, то вийде з ладу вся мережа.

Тип мережі, в якому кожен комп'ютер і мережевий пристрій підключені до одного кабелю називають топологія «шини». Він передає дані з початку до кінця в одному напрямку де кабель підключається до пристроїв. Топологія шини немає двонаправленої функції. Це багатоточкове з'єднання та ненадійна топологія, якщо магістраль порушується, топологія виходить з ладу. До переваг можна навести, що вартість кабелю менша порівняно з іншими топологіями мереж. Окрім того що топологія є ненадійною, ще в ній трафік є інтенсивний. Це призводить колізії в мережі, тому на другому рівні , де використовуються MAC – адресація, використовують різні протоколи , такі як:

1) pure aloha;

2) Slotted Aloha;

3) CSMA;

4) CD.

У топології «кільце» утворюється справжнє кільце, що з'єднує пристрої з двома пристроями між ним. Використовується для кільцевої топології ряд ретрансляторів з певною кількістю вузлів, адже якщо хтось хоче послати дані до останнього вузла в цій топології зі ста вузлами, то дані повинні пройти через дев'яносто дев'ять вузлів, щоб досягти сотий вузол. Таким чином, для запобігання втраті даних в мережі використовуються репітери. Передача є односпрямованою, але її допустимо зробити двонаправленою, використовуючи 2 з'єднання між кожним вузлом мережі, така топологія отримала назву подвійного кільця.

До переваг можна віднести мінімальну можливість зіткнення фреймів, та мало фінансовим встановленням. Усунення проблем в цій топології є складною річчю, також додавання нових станцій може порушити все з'єднання.

Однією з варіацій топології «зірка», є топологія з ієрархічним потоком даних – «дерево». В такій топології інформація прямує від пристроїв до вторинних хабів , від яких вона прямує до основного. Він в свою чергу містить у собі ретранслятор. Потік рухається спочатку зверху вниз, а потім знизу до верху. Перевагами є відстань сигналу, яку можна зробити в такій топології, та розробити пріоритети для кожного комп'ютера. Якщо центральний хаб виходить з ладу, виходить з ладу вся система.

В реальності зазвичай використовуються складні топології мереж, які є розширеними та комбінованими базовими фізичними топологіями. Використовуючи складні топології, вдається забезпечити вимоги до масштабованості мереж.

Усі інформаційні потоки інформації, які рухаються в мережі за певним маршрутом та навантажують мережу протягом певного часу називають мережевим трафіком. Топології будуються у першу чергу задля ефективності трафіку у цій мережі. Вузлами звуть прилади, які поєднують між собою елементи мережі на різних рівнях, ними є маршрутизатор, комутатор, концентратор та

мультиплексор. Але що таке модель мережі та для чого потрібно поділяти її на рівні?

1.2 Еталонна модель OSI та протоколи на кожному з рівнів

Мережа та в особливості передача інформація в ній, є складними процесами які досить важко пояснити, щоб наприклад можна було щось полагодити. На допомогу прийшла ISO – «Міжнародна організація стандартизації» яка у 1984 році розробила модель взаємозв'язку відкритих систем (OSI). Це є еталонною моделлю, що описує, як інформація з програмного додатку на одному комп'ютері переміщується через фізичний носій до програмного забезпечення другого комп'ютера. Сім шарів лежить в основі моделі OSI, та кожен шар виконує певну функцію мережі. Зараз вона розглядається як архітектурна модель для між комп'ютерних комунікацій.

Можна сказати, що модель ділить завдання на сім менших і керованих завдань, де кожному шару призначене певне завдання. Шари в моделі є повністю автономними, тому завдання виконується незалежно один від одного. OSI поділяється окрім шарів, ще на два шари: верхній та нижній.

Верхній шар в моделі OSI займається проблемами, пов'язаними з програмами, які реалізовані лише в програмному забезпеченні. Рівень програми є ближчим до кінченого користувача. Як і користувач, так і прикладний рівень взаємодіють з програмами . Верхній шар відноситься до шару особисто над іншим шаром. Нижні рівні моделі OSI мають справу з проблемами передачі даних. Рівень каналу даних та фізичний рівень реалізовані в апаратному та програмному забезпеченні. Фізичний рівень - це нижній шар моделі OSI який більше керується фізичними явищами. Зображення моделі дивитися на (рисунок 1.2).

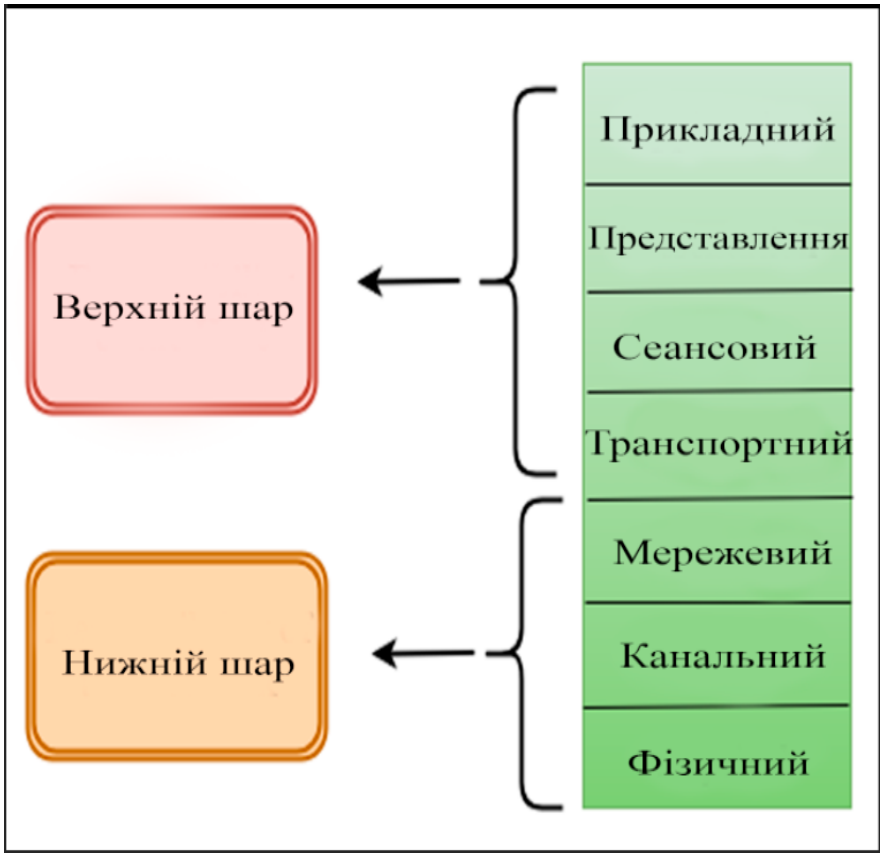


Рисунок 1.2 – Модель OSI з 7 рівнями

В семи рівнях еталонної моделі кожен шар виконує певні функції, які є унікальними та незмінними.

Фізичний рівень є найнижчим шаром еталонної моделі OSI. Його відповідальність лежить на передачі бітів з одного комп'ютера до іншого. Цей рівень ніяк не стосується значень бітів, а стосується налаштування фізичного підключення до мережі, а також передач та прийому сигналу. Забезпечуються засоби для транспортування у мережевому носію бітів, що складає кадр канального шару. Цей рівень приймає повний кадр з канального рівня і кодує його як впорядковану кількість сигналів, що транспортуються на локальний носій. Кодовані біти, які містять кадр, отримують або кінцеві пристрої, або проміжний пристрій для подальшої її передачі по мережі.

Функціонал який виконує фізичний рівень:

1) синхронізація: Передавач інформації та її отримувач можуть синхронізуватися на рівні бітів;

2) інтерфейс: фізичний рівень визначає який саме буде інтерфейс передачі між пристроями та середовищем;

3) топології: Пристрої слід підключати використовуючи топологій які вже було наведено;

4) конфігурація лінії: Цей елемент з'єднує пристрої із середовищем: Конфігурація від «точки до точки» та конфігурація з кількома точками;

5) режими передачі: Фізичний рівень визначає напрямок передачі між двома пристроями: Simplex, Half Duplex, Full Duplex;

6) швидкість передачі даних: Цей шар визначає швидкість передачі даних, тобто яка саме є кількість бітів в секунду;

7) представлення бітів: Дані цього рівня складаються з течії бітів. Біти кодуються в сигнали для передачі. Визначається тип кодування, тобто як 0 і 1 змінюються на сигнал.

Через те, що фізичний рівень знаходиться в самому низу, він перший контактує з широкосмуговою передачею.

Технології цього рівня побудовані саме в транспортних засобах цих сигналів так, щоб вони показали як саме будуть цю інформацію передавати, наприклад:

1) Rs-232 – інтерфейс обміну інформації між двома пристроями шляхом послідовного передавання;

2) 100BaseTX(Fast Ethernet) – використовуються для передачі в комп’ютерних мережах в першому і в другому рівні еталонної моделі, забезпечує передачу даних зі швидкістю 100 Мбит/с по кабелю, який складається з двох скручених пар п’ятої категорії;

3) ISDN – є першою технологією, що забезпечує одночасну передаю даних цифрових та аналогових. Використовується при цьому всього лиш одна лінія зв’язку. Тобто можна одночасно використовувати телефон та інтернет підключившись до одного кабеля;

4) також використовуються такі технології як bluetooth, wi-fi та інші.

Мережевими приладами першого рівня є концентратори(Hub) та ретранслятори(Repeater). Ці мало функціональні пристрої, що працюють з фізичним сигналом не концентруючись на його логіці, а тільки передають надісланий сигнал далі

Канальний рівень є наступним рівнем після фізичного тому вони інкапсулюються та декапсулюються між собою. На цьому рівні забезпечується функціональні та процедурні можливості для передачі даних між мережевими об'єктами та виявлення , редагування помилок, які можуть з’явитися на фізичному рівні. Спочатку цей шар призначався для мережевих технологій "точка-точка" і "точка-багато точок", характерних для широкоформатних засобів масової інформації в телефонній системі. Шар каналу даних приховує деталі базового обладнання та представляє себе верхньому шару як засіб спілкування.

Рівень каналу даних має відповідальність за перетворення потоку даних у сигнали по бітах і передачу інформації через базове обладнання. На кінці прийому рівень передачі даних забирає дані з апаратних засобів, які мають форму електричних сигналів, трансформує їх у згаданому форматі кадру і передає на верхній шар. Канальний рівень поділяється на два підрівня:

1) логічне керування посиланням має справу з протоколами, управлінням правилом та контролем помилок;

2) контроль доступу до засобів масової інформації стосується фактичного управління над засобами масової інформації.

Функціонал який виконує канальний рівень:

1) кадрування. Рівень каналу передачі даних отримує пакети з мережевого рівня і інкапсулює їх у кадри, а потім передає кожен кадр в бітовому форматі на апаратне забезпечення. В кінці приймача інформації канальний рівень передачі даних приймає сигнали від апаратного забезпечення та збирає їх у кадри;

2) звернення. Рівень каналу передачі даних дає апаратний механізм адресації другого рівня. Адреса апаратного забезпечення вважається унікальною за посиланням. Вона кодується в апаратне забезпечення під час виготовлення, наприклад MAC-адреса чи LLC;

3) синхронізація. Коли кадри даних надсилаються за посиланням, обидві машини повинні бути синхронізовані, щоб здійснити передачу;

4) контроль помилок. Іноді сигнали можуть зіткнутися з проблемою при переході, і біти повертаються назад до передавача. Ці помилки виявляються і намагаються відновити посилання біт даних. Він також надає відправнику механізм повідомлення про помилки;

5) управління потоком. Станції телекомунікацій на одній лінії зв'язку можуть мати різну швидкість або пропускну здатність. Канальний шар забезпечує контроль потоку, що дозволяє обом машинам обмінюватися даними з однаковою швидкістю;

6) мультидоступ. Коли хост спільного посилання намагається передати дані, існує велика ймовірність зіткнення. Рівень каналу передачі даних забезпечує такий механізм, як CSMA/CD, щоб забезпечити можливість доступу до спільного носія інформації між різними системами.

Можна сказати, що на цьому рівні використовується адресація кожного приладу у системі, адрес цього приладу є MAC-адресом. Він є унікальним ідентифікатором, який присвоюється кожній одиниці активних пристроїв, та в деяких інтерфейсах мереж Ethernat. При проектуванні стандартам Ethernet було вказано, що кожна мережева карта має мати при собі унікальний шести байт номер MAC (рисунок 1.3) , що вшитий в мережеву плату, який надає ідентифікацію відправника та отримувача фрейма.

Також використовується на цьому рівні протокол LLC, що є підрівнем управління логічним посиланням (LLC) рівня каналу даних , управляє зв'язками між пристроями, керуючи синхронізацією кадру, контролем потоку та перевіркою помилок. Цей протокол запитує у канального рівня, яку саме потрібно здійснити транспортну операцію, та з якою швидкістю. Рівень LLC забезпечує передачу даних без підключення та орієнтовану на зв'язок .

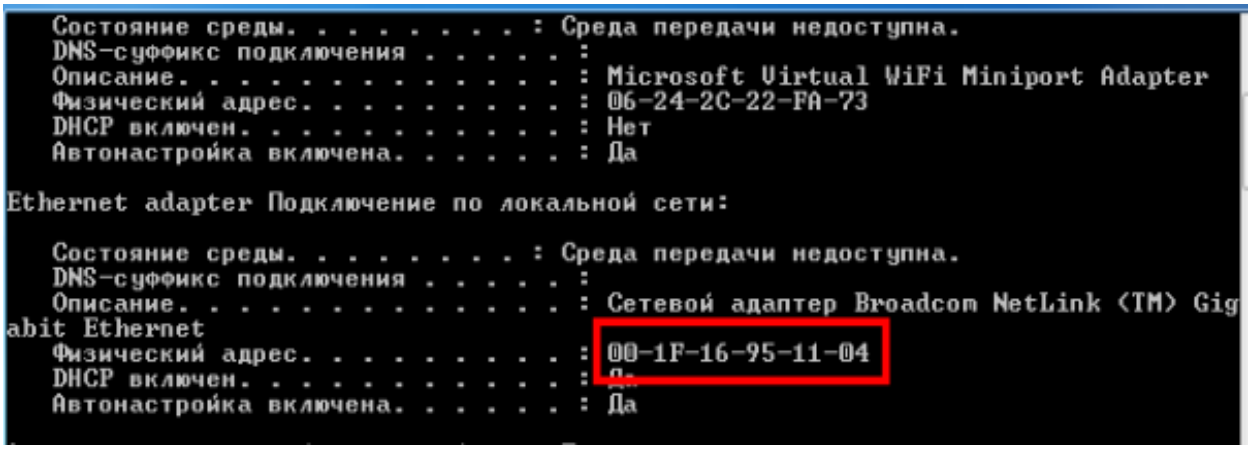


Рисунок 1.3 – Вигляд MAC-адресу в командному рядку

На канальному рівні вже використовуються більш розумні прилади порівняно з фізичним. Такі прилади як Комутатор(Switch) та Міст(Bridge). Вони виконують передачу нашого фрейму, потрібному отримувачу, з використанням певних протоколів передачі.

Залежно від вимог вибираються протоколи передачі, які підбирають виключно для певної мережі. Приклад: комутатори Cisco надають перевагу власному протоколу зв'язку.

Ось список часто використовуваних протоколів рівня 2 (таблиця 1.1).

Таблиця 1.1 – Основні протоколи другого рівня моделі OSI

IP-маршрут	Ця команда містить інформацію з таблиці маршрутизації IP, яка може бути використана для переадресації пакету через кращий маршрут до точки призначення.
ARP (протокол дозволу адреси)	ARP транслює динамічний IP (третій рівень) з MAC-адресами (другий рівень). ARP перекладає 32-розрядні адреси в 48-розрядні

Кінець таблиці 1.1 – Основні протоколи другого рівня моделі OSI

Протокол багатоканальної транкінгу (MLT)	Забезпечує високошвидкісне, стійке до відмов з'єднання між серверами, комутаторами та маршрутизаторами, групуючи всі канали Ethernet в єдине логічне з'єднання Ethernet.
CAN (мережа контролера)	Полегшує зв'язок між додатками мікроконтролерів та їх засобами, не покладаючись на головний комп'ютер.
PPP (протокол точка-точка)	Дозволяє встановити зв'язок між двома маршрутизаторами без допомоги хоста.
CDP (протокол виявлення Cisco)	Власний протокол компанії Cisco, який підтримує версію LLDP IEEE 802.1ab, і в основному використовується для обміну інформацією між безпосередньо підключеними пристроями Cisco для більш коректного з’єднання.

Також в канальному рівні еталонної моделі є такі протоколи як : ATM (Асинхронний режим передачі), Ethernet(відноситься і до 1 і до 2 рівня моделі), Frame relay, NDP (Протокол виявлення Nortel) , IEEE 802.2 (надає функції LLC рівням MAC IEEE 802) , HDLC(Високорівневий контроль передачі даних). Також частино входить до протоколів рівня передачі даних протокол та технологія MPLS, про неї поговоримо пізніше.

Мережевий рівень є одним з двох з двох можливих шарів, в яких ми використовуємо адресацію. Найчастіше саме тут ми застосовуємо IP-адреси. Тож

не дивно, що це також рівень, де відбувається маршрутизація. На цьому рівні всі дані, що надсилаються через Інтернет, розбиваються на менші фрагменти, які отримала назву «пакет». Наприклад, коли Василь надсилає Галині повідомлення, його повідомлення розбивається на більш дрібні шматки, а потім знову збирається на комп'ютері Галини. Пакет складається з двох частин: заголовка, який містить інформацію про сам пакет, і тіла, яке є фактичними даними, що надсилаються. Для того щоб переслати пакет з однієї мережі в іншу потрібно здійснити таку дію як маршрутизація. Фактична маршрутизація (або переадресація трафіку) між мережами, здійснюється апаратним пристроєм - маршрутизатором.

Для досягнення мети, що робить мережевий рівень, є додаванням іншого заголовка. Цей заголовок включає початкову та кінцеву IP-адреси, а також іншу інформацію про пакет. Заголовки, додані шарами 3 і 4, зазвичай не змінюються, коли пакет рухається по мережі. Є такі технології, як NAT, який змінює IP-адресу в глобальній мережі інтернету. Як ми знаємо, канальний рівень може обробляти тільки блок даних максимального розміру. Отже, частина роботи мережевого рівня лежить в тому, щоб досвідчитися, що пакет не є великого розміру. Якщо пакет занадто великий, він буде розбитий на менші частини, які називаються фрагментами. Вони зберуться знову, коли досягнуть хоста отримувача. Кожен фрагмент має власний набір заголовків.

Мережевий рівень не вимагає надійності. Йому не потрібно здійснювати перевірку на помилки, адже вже інші шари це роблять за нього.

Функціонал який виконує канальний рівень:

1) маршрутизація. Протоколи мережевого рівня визначають, яким саме маршрутом буде прямувати пакет від одного джерела до іншого;

2) логічна адресація. Для того, щоб розпізнати кожен пристрій в мережі, а саме інтернет, мережевий рівень визначається схема адресації;

IP-адреса відправника та одержувача розміщується у заголовку над мережевим рівнем. Така адреса відрізняє кожен пристрій унікально та універсально на логічному рівні.

В загальному на мережевому рівні відбувається встановлення маршрутів для проходження пакетів даних, та перевірку того, чи працює сервер в іншій

мережі, а також адресацію та отримання IP-пакетів з інших мереж. Цей останній процес є, мабуть, найважливішим, оскільки переважна більшість Інтернет-трафіку передається через IP.

Ряд протоколів мережевого шару робить можливим підключення, тестування, маршрутизацію та шифрування. Основними протоколами цього рівня є (таблиця 1.2).

Таблиця 1.2 – Основні протоколи третього рівня моделі OSI

IP	Використовується для передачі датаграм з іншими учасниками мереж, найвідомішими форматами є (IPv4, IPv6)
IPsec	Протокол шифрування IP - пакетів
ICMP	Використовується, щоб отримати інформацію про помилку яка виникла під час передачі.
IGMP	Використовують для групових транспортувань пакетів та управління групою передач даних

Останні рівні відносяться до верхнього шару еталонної моделі, тому в виконанні моєї мережі вони не використовуються

Транспортний рівень дає вільну передачу даних між кінцевими користувачами, забезпечуючи надійні послуги передачі даних до верхніх шарів. Транспортний шар бере керування надійністю даного каналу використовуючи контролю потоку, десегментації та сегментації також в своєму арсеналі він має контроль помилок. Котрі протоколи застосовуються на стан та зв’язок. Отже це говорить, що транспортний рівень має змогу відстежувати сегменти та ще раз

передавати ті, які не пройшли перевірку. Четвертий рівень також надає підтвердження вдалої передачі даних та надсилає іншу інформацію, якщо немає помилок. Типовими прикладами четвертого рівня є:

1) протокол управління передачею (TCP);
2) протокол датаграм користувача(UDP).

Сеансовий рівень дозволяє користувачам на різних машинах ставити активні сеанси зв'язку з ними. Основною метою є встановлення , підтримки та синхронізації між системами зв'язку. П’ятий рівень керує та синхронізує розмову між двома різними програмами. На рівні сеансу потоки інформації позначаються та ре-синхронізуються так як потрібно, так що в кінці повідомлення не обрізаються і втрачається увага на втрату даних. Прикладом протоколів такого рівня є:

1) netBIOS;
2) winsock.

Представницький рівень є рівнем який використовується для подання даних на прикладний рівень (рівень 7) у максимально точному, чіткому та стандартизованому форматі. Тобто на цьому рівні всі інформація подається у вигляді, який максимально чіткий простому користувачу. Тут використовуються такі протоколи:

1) AFT;
2) ICA;
3) LPP;
4) та інші.

Прикладний рівень **і**нтерфейс прикладного рівня повністю взаємодіє з додатком і забезпечує загальні послуги веб-додатків. Рівень програми також робить запит до рівня презентації. Рівень додатків - це найвищий рівень відкритих систем, що надає допомогу безпосереднього для процесу прохання допомоги. Тобто це рівень надає доступи наприклад до якогось ресурсів в інтернеті. Прикладом протоколів є:

1) DNS;
2) FTTP;

3) FTP;

4) та інші.

1.3 Умови появи нової технології мереж

Мережа інтернет створена для того, щоб з’єднати всіх користувачів по різних містах та країнах. Для цього будуються магістральні лінії по всіх районах, велика клієнтська база. Виникає питання: «Як створити мережу для корпоративних клієнтів?

Для цього використовуються в першу чергу широкосмуговий доступ до інтернету, до якого входять різні технології мереж. Він дає змогу передавати велику кількість інформації та досягає високої швидкості передачі інформації з багатоканальністтю, що є дуже важливим для багатьом компаній. Але є велика кількість мега-корпорацій яким потрібен сервіс VPN, що створює віртуальні канали передачі інформації в першу чергу задля її безпеки . Коротко , цей сервіс створює тунелі в яких адрес призначення шифрується адресом від сервісу VPN. Недоліками такого сервісу є те, що він вимагає більше обчислювальної потужності приладів для шифрування інформації. Також збільшується час передачі інформації до кінченої точки. Також не всі пристрої VPN взаємодіють між собою добре, тому мережевий інженер повинен над цим попрацювати. На даний час найпопулярнішою технологією мережевого рівня є пакетна комутація на основі IP, в свою чергу, канальний використовує Ethernet.

Існує велика кількість місць, де використовується вже застарілі технології телекомунікаційних мереж. Наприклад технологія канального рівня ATM, або така технологія як PDH яку потрібно передати з одного кінця в інший. Клієнт наприклад хоче аби його Ethernet-мережа виявилась доступною з іншого кінця міста так, ніби він з’єднаний через сервіс VPN. Як це було колись: брали ATM між двома точками на карті - канал в середині на базі ATM, PDH - лад PDH. Хотілось б щоб все робило через одну мережу, а не конструювати окрему для кожного типу трафіку. Для цього придумали такі технології як:

1) GRE;

2) PPpoE;

3) ATM over Ethernet;

4) TDM over IP;

5) численні інші over іншої технології.

Можна створити ще багато інших, щоб покрити вже всі існуючі комбінації, і настане неймовірне щастя в хаосі стандартів. Так дрібні виробники таким методом і пішли. Коли клієнти замовляли власну приватну мережу маршрутизатори постачальника надавали послугу другого рівня по відношенню до клієнтських маршрутизаторів третього рівня, розділення та ізоляція між різними клієнтами у мережі були гарантовані. Такі види мереж називають мережами, що накладаються .

На допомогу прийшла технологія, що буквально лежить між канальним та мережевим рівнем. Вона була створена у другій половині 1990-х років, щоб маршрутизатори могли обходити пошук маршрутів у таблицях маршрутизації, тим самим покращуючи швидкість потоку мережевого трафіку. У 1994 році компанія Toshiba започаткувала ідею робочій групі Інженерного проектування (IETF), Вони почали передувати сучасні стандарти MPLS . Потім у 1996 році Cisco, Ipsilon та IBM розповіли всім про плани використовувати комутацію за мітками , що призведе до сучасної реалізації протоколу. Нарешті, на початку 2000-х рр. Методи були додатково розроблені та впроваджені, що призвело до широкомасштабного впровадження, яке відбулося між компаніями протягом останніх кількох років. Так і з’явилася нова технологія, яка має назву MPLS – багатопротокольна комутація з використанням міток. Найголовнішими перевагами технології є:

1) використання однієї уніфікованої мережевої інфраструктури;

2) краща інтеграція технологій IP з ATM;

3) безкоштовне ядро BGP;

4) рівна модель для MPLS VPN;

5) оптимальний транспортний потік.

1.4 Висновки

В цьому розділі було розглянуто структуру телекомунікаційної мережі, її основні типи топології та вузлів. Також розібрано еталонну моделі OSI та технології на кожному з рівнів, та причини появи нової технології комутації з використанням у своєму заголовку мітки.

2 СПОСОБИ ІНТЕГРАЦІЙ ТЕХНОЛОГІЇ MPLS У ТЕЛЕКОМУНІКАЦІЙНУ МЕРЕЖУ

2.1 Аналіз технології, її адресація у пакеті

Головною ідеєю MPLS є створення позначок, або міток, вхідних пакетів на основі їх призначення або попередньо налаштовані критерії транспортування з переключенням всього трафіку через спільну інфраструктуру. Як ми знаємо, головною перевагою IP, э те що ми можемо через нього передавати будь-які технології, адже не тільки дані передаються через IP, а також телефонія. Прийнято рішення використовувати MPLS разом з IP, так розширюються можливості того, що можна передавати. Додавання міток до пакету дозволяє нести інші протоколи, крім простого IP, через MPLS підтримку третього рівня IP магістралі. Технологія міток може транспортувати:

1) IPv4;
2) IPv6;
3) Ethernet;
4) високорівневий контроль передачі даних (HDLC);
5) PPP;
6) та інші технології другого рівня.

Функція, з використанням якої, будь-який кадр другого рівня переноситься через магістраль MPLS, отримала назву «Транспортування через MPLS (AToM)». Маршрутизатори, які перемикають трафік AToM, не повинні знати про позитивне навантаження MPLS; їм просто потрібно мати можливість переключити трафік в якого є мітка, дивлячись на заголовок в ньому. По суті, комутація міток MPLS є простим методом комутацій певної кількості протоколів в одній мережі. Для реалізації вам потрібно мати таблицю посилань, яка складається з вхідних ярликів з обміном вихідними мітками та наступним стрибком. Перемикання міток вказує на те, що комутовані пакети більше не є пакетами IPv4, пакетами IPv6 або навіть кадрами другого рівня при перемиканні, але вони позначені. Найважливішим

елементом для MPLS є мітка. Одна мітка MPLS є полем з 32 бітами інформації та з певною структурою (рисунок 2.1).

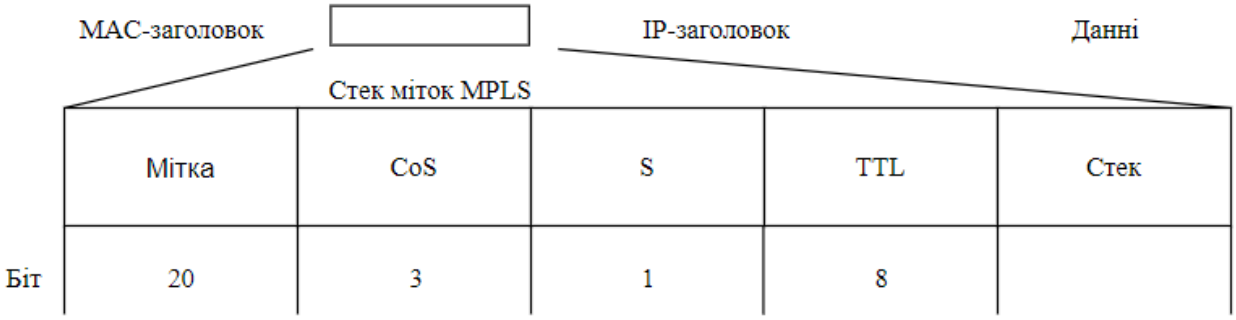


Рисунок 2.1 – Заголовок MPLS

Перші 20 бітів є значення мітки. Це значення може становити від 0 до 2^{20} – 1, або 1,048,575. Однак перші 16 значень звільняються від простого використання, тобто вони мають особливе значення. Біти від 20 до 22 є трьома експериментальними (EXP) бітами. Ці біти використовуються виключно для якості послуги (QoS). Біт 23 - біт нижнього стека (BoSom Stack(S), BoS). Він дорівнює 0, якщо це не нижня мітка в простому стані. Якщо так, біт BoS дорівнює 1. Стек - це колекція міток, які знаходяться поверх пакета та може складатися лише з однієї мітки, а може й більше. Кількість міток, яке ви можете знайти тут є безмежним, хоча рідко вам доводиться бачити такий. Стек складається з чотирьох або більше міток.

Біти від 24 до 31 - це вісім бітів, що використовуються для часу життя (TTL). Цей TTL має ту саму функцію, що і TTL, знайдений у заголовку IP. Він просто зменшуються на 1 при кожному стрибку, і його основною функцією є уникнення зупинки пакета в циклі маршрутизації. Якщо виникає цикл маршрутизації, а TTL відсутній, цикли в файлах пакетів будуть назавжди. Якщо TTL мітки досягає 0, пакет відкидається.

Постає питання: «Де саме розміщується ця мітка?». Відповідь одна, вона розміщується до третього рівня тобто, перед заголовком транспортованого протоколу, але після заголовка другого рівня. Часто ярлик стеку MPLS називається заголовком прокладення через його розміщення(таблиця 2.1).

Таблиця 2.1 – Стек міток для міченого пакета

Заголовок канального рівня	Стек міток MPLS	Транспортний протокол
Кадр другого рівня		

Оскільки стек міток у кадрі канального рівня раніше розміщується заголовок транспортного рівня або інший переданий протокол, потрібно мати нові значення для каналу передачі даних. Де вміщується MPLS? MPLS не є протоколом другого рівня , оскільки інкапсуляція рівня 2 все ще присутні з міченими пакетами. MPLS також насправді не є протоколом транспортного рівня , оскільки рівень 3 протокол все ще присутній. Тому MPLS не надто добре вписується в шари еталонної моделі OSI. Можливо найпростіше, що потрібно зробити, це розглянути MPLS як 2.5-шар і закінчити з ним.

2.2 Перемикання міток в MPLS, та маршрутизація

Всі мітки в заголовку MPLS повинні розміщуватися на якомусь апаратному пристрої та якось взаємодіяти між собою, для цього кожен маршрутизатор для перемикання міток повинен відповідати мітці на вхідному пакеті, змінити його місцем призначення із вхідною міткою та переслати пакет.

Маршрутизатором для перемикання міток є пристрій із назвою LSR - це маршрутизатор, який підтримує MPLS. Він здатний розуміти MPLS мітки та приймати і передавати пакети з мітками по лінії передачі даних. LSR можуть швидко маршрутизувати пакети даних без необхідності перевіряти таблиці адресації або робити розрахунки маршрутизації, які додають час надсилання та отримання даних. Оскільки на мітках вже є вказівки щодо шляху, по якому йдуть дані, маршрутизатор просто повинен направляти дані на основі інструкцій на мітках. Існує чотири види LSR у мережі MPLS:

1) вхідний маршрутизатор , який базується на початку або в точці входу LSP. Це одиничний маршрутизатор, де звичайний IP-трафік може перетворитися в шлях MPLS. Вхідні маршрути використовують вхідні маршрутизатори, які отримують інформацію від IP-трафіку, що потім проходить через LSP, аби дістатися до місця призначення. Вхідний маршрутизатор використовує інкапсуляцію трафіку за допомогою заголовка MPLS;

2) транзитний маршрутизатор, що знаходиться в середині шляху LSP. На відміну від вхідного маршрутизатора, який використовує вхідні маршрути, транзитні маршрутизатори перемикають пакети MPLS на наступний шлях у LSP. Він використовує інтерфейс, з якого прийшов пакет, а також заголовок MPLS для інформації про його призначення;

3) передостанній маршрутизатор розташований на останній до останньої зупинки в LSP. Передостанній маршрутизатор використовується для видалення заголовка MPLS перед тим, як подати його до останнього направлення в LSP. Заголовки MPLS більше не потрібні, оскільки останній маршрут у LSP не повинен переключати пакети вперед на інший транзитний маршрутизатор;

4) вихідний маршрутизатор відомий як вихід з маршрутизації по міткам. Він приймає IP-трафік, який вийшов з передостаннього маршрутизатора, і виконує стандартний пошук IP-адреси, який потім відправляє , використовуючи вже звичайну IP-маршрутизацію.

Цей маршрутизатор виконує 3 основних операції: Pop, Push , Swap. Мітка MPLS має важливе застосування лише між будь-якими двома LSR, тому одна і та ж мітка може використовуватися одночасно в мережі, що підтримує MPLS. Для того, щоб MPLS LSR міг переключити пакет MPLS, мітка, яка використовується в заголовку цього пакета, повинна представляти запис у MPLS LFIB цього LSR.

LFIB в свїй суті є базою даних перемикання між мітками. Також мітки які використовується для програмування площини пересилання LSR. Як тільки пакет буде отримано, його мітка буде використовуватися площиною пересилання для прийняття рішення про те, куди переслати пакет. По краях мережі, що підтримує MPLS, маршрутизатори комутації міток будуть відображати IP-пакети у FEC на основі інформації, що надається площиною управління MPLS. FEC - це набір

префіксів ,або потік пакетів які обробляються однаково, шляхом потрапляння LSR, переглядаючи його заголовок мережевого рівня і пересилаючи його до наступного LSR, який замість того, щоб шукати заголовок мережевого рівня, щоб прийняти рішення про пересилання, буде дивитись лише на мітку і відповідно міняти мітку і переслати його до наступного LSR, і цей процес триває, поки пакет не досягне місця призначення. Усі пакети, що належать до того ж FEC , мають однакову позначку. Однак не всі пакети, що мають однакову мітку, належать до того самого FEC, оскільки їх значення EXP можуть відрізнятися, переадресація може бути різною і вони могли належати до іншого FEC. Маршрутизатор, який вирішує які пакети до яких належать FEC - це вхідний LSR. Це логічно, оскільки вхідний LSR класифікує та вміщує пакети. Можна навести такі приклади FEC:

1) пакети з IP-адресами призначення транспортного рівня, що відповідають певному префіксу;

2) багатоадресні пакети, що належать до певної групи;

3) пакети які мають однакову обробку переадресації на основі коду IP DiffServПоле точки (DSCP);

4) кадри на другому рівні, що передаються шляхом MPLS, отримані на одному VC або на виході LSR;

5) пакети з призначенням третього рівня, які належать до набору протоколу BGP, про який поговоримо пізніше.

Цей останній приклад FEC є особливо цікавим. Всі пакети на вході LSR для якої IP-адреса призначення вказує на набір маршрутів BGP у таблиці маршрутизації - вся однакова адреса наступного переходу BGP - належить одному FEC. Це означає, що всі пакети, які надходять у MPLS отримають мітку залежно від того, яким буде наступний стрибок BGP

Шлях з комутацією міток (LSP) є послідовністю LSR маршрутизаторів, які перемикають пакет з міткою через MPLS мережі або частину мережі (рисунок 2.2).

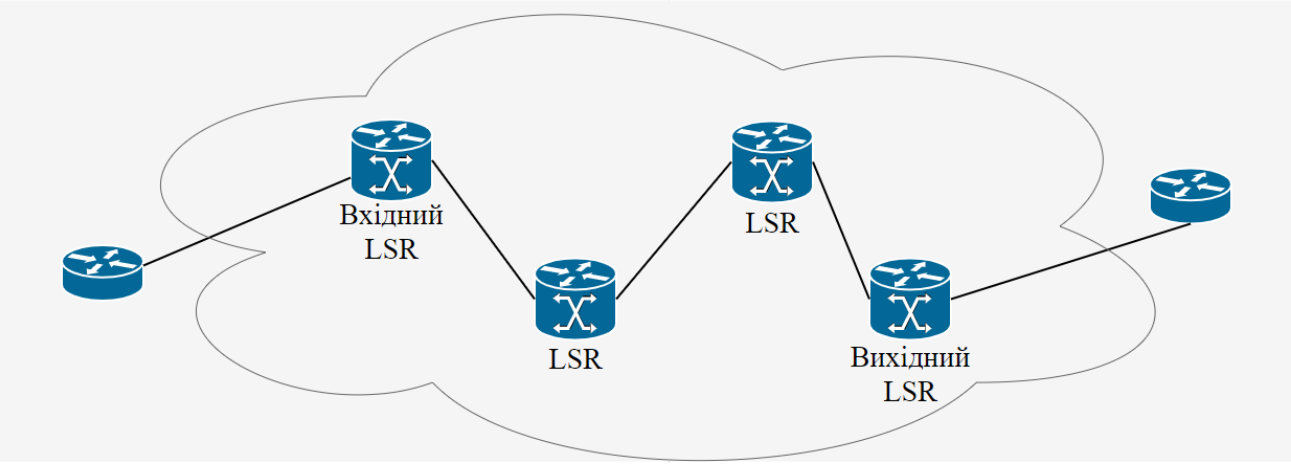


Рисунок 2.2 – Простий LSP через MPLS мережі

В основному беруть пакети з одного кінця до іншого з використанням маршрутизаторів з мітками. Перший LSR в LSP є вхідний роутер для цього LSP, тоді як останнім LSR LSP є вихідний роутер. Всі LSR між вхідними та вихідними LSR є проміжними.

Отже, можна зобразити як відбувається передача пакету в такій простій схемі. Нюансом є те ,що передача відбувається тільки в одну сторону, тобто до вхідного LSR, де відбувається звичайний перехід IP пакета, чи фрейм в звичайну IP адресацію. Так , порядок передачі інформації такий:

1) пакет потрапляє у вхідний LSR, де взнає місце призначення інформації, тобто отримує FEC. Для цього FEC є вже мітка, тому маршрутизатор добавив її в стек, тобто відбувся Push label в даний пакет;

2) проміжний LSR побачив пакет який надійшов, та глянув що у ньому вже є мітка, яку потрібно замінити іншою, тобто Swap lable, та послати в інший LSR, де відбувається ідентична дія заміни мітки;

3) як тільки пакет дійшов до вихідного LSR, там відбувається вже не заміна мітки іншою, а повне її знищення зі стеку заголовка, тобто Pop lable, далі трансляція відбувається за звичайною IP чи ATM адресацією.

Недоліком такої LSP системи є її маленький функціонал транспортної мережі, адже все транспортування відбувається тільки в одну з сторін, тому потрібно вирішувати цю проблему.

У випадку MPLS VPN, технологія віртуальних каналів з використанням міток , вхідні та вихідні LSR називаються постачальниками крайніх (PE) маршрутизаторів. Проміжні LSR називаються маршрутизаторами провайдера, тобто (P). Терміни PE та P маршрутизатори стали настільки популярними, що їх також використовують, коли мережа MPLS не працює в мережі MPLS VPN.

Вхідний LSR в LSP не завжди є першим маршрутзатором який надасть мітку пакету. Пакет може вже бути позначений попереднім LSR. Такий випадок будує «вкладений LSP» – тобто LSP всередині іншої мережі LSP. Інший LSP починаючи з третього LSR , закінчується з наступного до останнього LSR. Тому коли пакет потрапляє до другого LSP на своєму вхідному LSR (це означає третій LSR), він вже при собі має мітку. На вхід LSR вкладеного LSP штовхається друга мітка у пакет (таблиця 2.2). Заголовок пакета на другому LSP тепер має дві мітки. Верхня мітка належить вкладеному LSP,а нижня мітка належить LSP, що охоплює всю мережу MPLS.

Таблиця 2.2 – Приклад дворівневого стека міток MPLS

Заголовок 2 рівня	MPLS мітка №2	MPLS мітка №3	Заголовок 3 рівня	Дані

Така система вже наблизилася до вирішення проблеми, але якщо LDP буде складатися не в одну ліні «Точка-точка». Можливо з якоїсь топології «Кільце», чи з якоїсь складної топології будуть виникати трудності. Щоб такого не виникало, потрібно використовувати протоколи маршрутизації які використовується для забезпечення маршрутизації у внутрішній мережі провайдера, щоб можна було генерувати мітки, такі як OSPF та IS-IS.

2.3 Протоколи маршрутизації в технології комутацій по міткам

Розглянемо приклад простого IPv4-over-MPLS, який є найпростішим прикладом MPLS мережі. Звичайний IPv4-over-MPLS - це мережа, що складається з LSR, які запускають протокол 3 рівня IPv4 та протокол шлюзу IGP ,наприклад,

спочатку відкрити найкоротший шлях [OSPF], проміжна система [IS-IS] та вдосконалений протокол маршрутизації внутрішніх шлюзів [EIGRP].

Вхідний маршрутизатор шукає IPv4 адресу пакетного призначення, накладає мітку та пересилає пакет. Наступний роутер (і будь-який інший проміжний роутер) отримує мічений пакет, обмінюється вхідною міткою з вихідною міткою та пересилає пакет. Вихід LSR згортає мітку та пересилає пакет IPv4 без міток на вихідному посиланні. Щоб це працювало, сусідні LSR повинні узгодити, який заголовок використовувати для кожного префікса IGP. Отже, кожен проміжний LSR повинен зрозуміти, на яку саме змінювати мітку, що надходить. Отже вам потрібен механізм, який повідомляє маршрутизаторам, які мітки використовувати під час переадресації пакету. Всі мітки використовуються локально для кожної пари сусідніх маршрутизаторів. Етикетки не мають глобального значення в мережі. Для сусідніх маршрутизаторів, щоб узгодити яку мітку використовувати для префіксу потребуються певної форми спілкування між ними. В іншому випадку, маршрутизатори не знають, якому вихідному ярлику потрібно відповісти якій вхідній мітці. Потрібен протокол розповсюдження етикеток. Ви можете розповсюджувати мітки двома способами:

1) посилання на мітки в існуючому протоколі IP-маршрутизації;
2) мати окремий протокол розподілу міток.

В першому способі лежить те, що новий протокол потрібен не для запуску на LSR, а в кожному існуючому протоколу IP-маршрутизації потрібно розширяти, щоб містити мітки. Це не завжди є легкою роботою. Великою перевагою того, що протокол маршрутизації несе мітки, що маршрутизація та розподіл міток завжди синхронізовані, це означає, що ви не можете мати мітку, якщо заголовок є відсутній або навпаки. Це також усуває необхідність використання іншого протоколу, запущеного на LSR, для розподілу міток. Для роботи MPLS у маршрутизаторі має проходити розподілення міток для кожного заголовка, тобто IGP ,що є протоколом для обміну інформацією про маршрутизацію між шлюзами (хостами і маршрутизаторами) та в автономній мережі (наприклад, система корпоративних локальних мереж). Інформація про маршрутизацію може потім використовуватися Інтернет-протоколом (IP) або іншими мережевими

протоколами для вказівки маршрутизації передач. Існують два загальновживаних IGP:

1) протокол маршрутизації інформації (RIP);

2) протокол відкритого найкоротшого шляху (OSPF).

Знаючи що технологія комутацій за мітками використовується у провайдерських компаній, ми можемо сказати, що вони не використовують протокол IGP, адже є набагато кращий, такий як BGP. Цей протокол маршрутизації який може одночасно мати заголовки та розповсюджувати мітки за потрібним шляхом. Він використовується для перенесення зовнішніх заголовків між іншими системами мереж, які прямо не з’єднані між собою. BGP використовується в основному для розповсюдження міток у MPLS VPN мережі. Саме з цим протоколом, показуються всі переваги MPLS, адже він динамічно маршрутизує між автономними системами з можливістю передавати мітки(рисунок 2.3). Під час роботи BGP повідомлення обмінюються через TCP-з'єднання між одного рангу протоколами BGP. Четверта версія протоколу BGP максимально відрізняється від попередньої розробки BGP і фактично включає окремі протоколи з різним функціоналом:

1) протокол EBGP - External Border Gateway Protocol, - використовуваний для маршрутизації між автономними системами;

2) протокол IBGP - Internal Border Gateway Protocol, - використовуваний для маршрутизації всередині автономних систем.

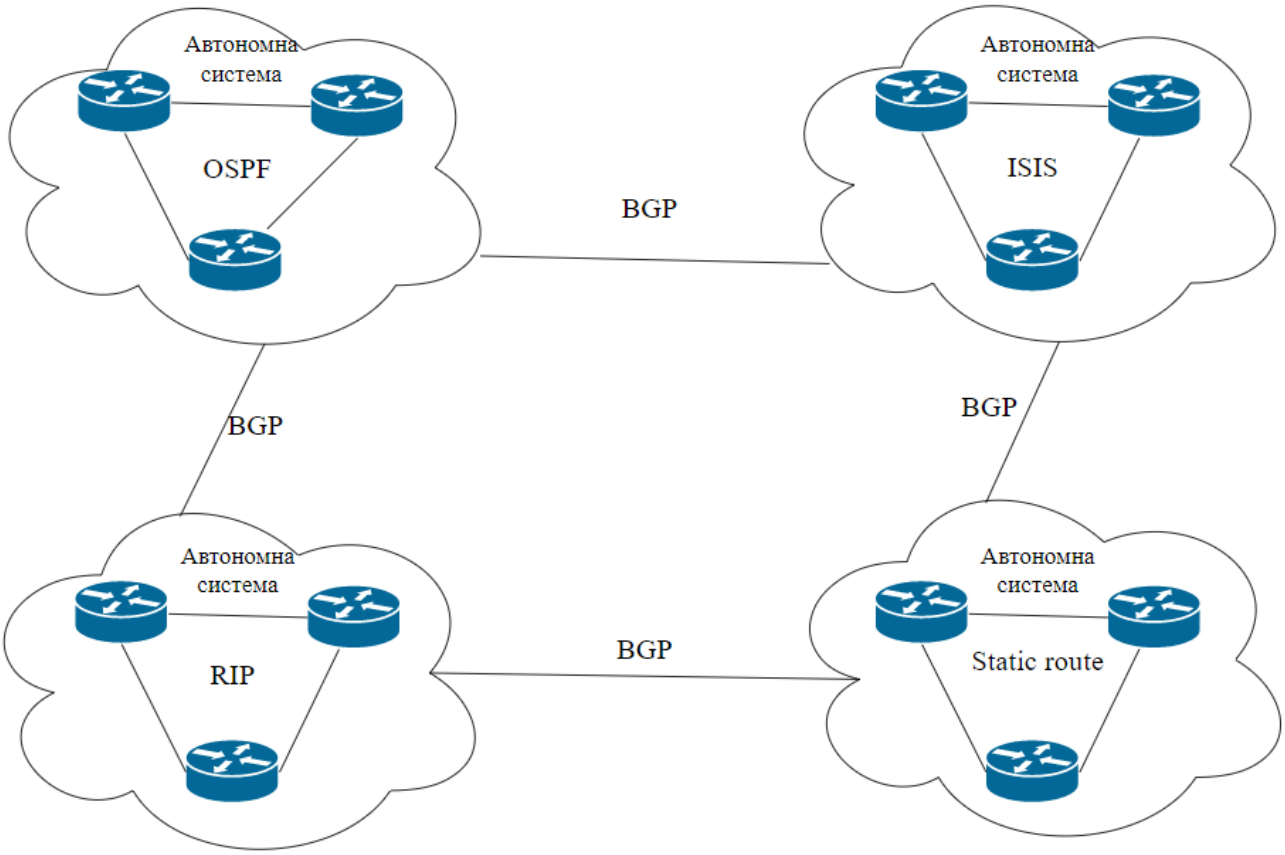


Рисунок 2.3 – Робота BGP протоколу

Коли хмара MPLS використовується в ядрі, BGP може розгортатися на краях мережі за допомогою основних маршрутизаторів, що несуть лише інформацію про наступний крок BGP. Протокол встановлює маршрути без циклу та обмінюється інформацією про маршрутизацію між групою маршрутизаторів (автономних систем). Хмара MPLS не розсіює BGP по мережі, адже забезпечує наскрізний транспорт для маршрутів BGP. Це можна зробити, запустивши BGP скрізь, перерозподіливши BGP в протокол Interior Gateway Protocol і проклавши тунель GRE з PE на PE.

У випадку великомасштабної мережі ,ми маємо запустити ядро BGP без MPLS. Зв'язок між кінцями хмари MPLS буде видимий кожному клієнту тієї ж мережі. Отже, інтернет провайдер несе відповідальність за підтримку необхідних прав безпеки та доступу до мережевого з'єднання.

Мітки MPLS додаються до оновлених повідомлень, які відправляє маршрутизатор. Маршрутизатори обмінюються такими типами повідомлень BGP:

1) повідомлення для прояву уваги- маршрутизатор надсилає повідомлення, якщо виявлено помилку;

2) повідомлення про підтримку - маршрутизатор надсилає сигнал, щоб перевірити наявність сусіднього маршрутизатора;

3) повідомлення про оновлення - якщо маршрут новий, модифікований чи зламаний, надсилається повідомлення про оновлення стану сусіднього маршрутизатора. В таке повідомлення включено шляхи, які функціонують та не функціонують;

4) відкриті повідомлення - після встановлення з'єднання TCP між маршрутизаторами вони передають відкриті повідомлення, що містить IP-адресу відправника повідомлення та номер автономної системи, до якого підключений маршрутизатор.

Як саме працює протокол BGP зі сторони міток? BGP проходить маршрут разом із міткою MPLS, яка відображається на цьому маршруті. Повідомлення про оновлення BGP містить інформацію про відображення міток MPLS та який складається маршрут. Маршрутизатори переконуються, що вони можуть надсилати транспортування з мітками MPLS. Якщо перевірка між маршрутизаторами виконана, тоді мітки MPLS додаються до вихідних оновлень BGP.

Переадресацію пакетів, здійсненої протоколом BGP, з використанням технології міток в мережі MPLS VPN можна оглянути на (рисунок 2.4).

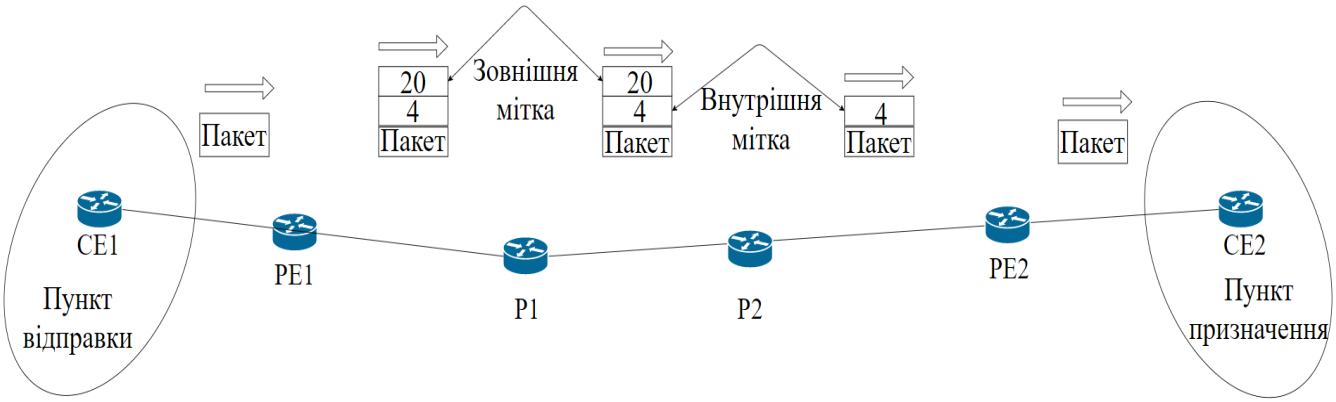


Рисунок 2.4 – Переадресація пакетів BGP в MPLS

Маршрути між мітками MPLS закодовуються багатопротокольними розширеннями які містять мітку. Мітки MPLS, які рухаються між маршрутизаторами, керуються картою маршруту. Якщо маршрутизатор отримує мітки, потрібно вказати маршрути, які приймаються та встановлюються в таблиці BGP. Карта маршруту дозволяє нам обрати маршрути, які з максимальною ймовірністю будуть розподілятися між спікерами. Спікери являють собою маршрутизатори автономних систем BGP, за допомогою яких обмінюються копії таблиць маршрутизацій в період початкового двостороннього сеансу . Карти маршрутів обробляються лише на рівні повідомлень про коригування , але не фільтрують маршрути, що надходять на роутер. Карти маршруту вміщають у собі метрики, за допомогою яких працює алгоритм маршрутизації.

2.4 Протоколи для побудови LSP тракту та розподілення міток

Можна сказати, що на деяких пристроях, розподілення міток можна зробити вручну. В епоху автоматизації існує три основних протоколи для розподілу міток:

1) LDP;
2) RSVP-TE;
3) MBGP.

Перед тим як ми про них поговоримо, потрібно розібратися як саме в цих протоколах передається інформація міток . По-перше, трафік прямує ,або з Вхідного LSR до вихідного, або навпаки. Така методика називається Downstream та Upstream. Також ми знаємо, що мітки розподіляються тільки вверх по течії, наприклад в нас є проста LSP, де вже є налаштований FEC. В цій ілюстрованій мережі LSR прямує від R1 до R5, та в нас є FEC з адресом 1.1.1.1/32 (рисунок 2.5).

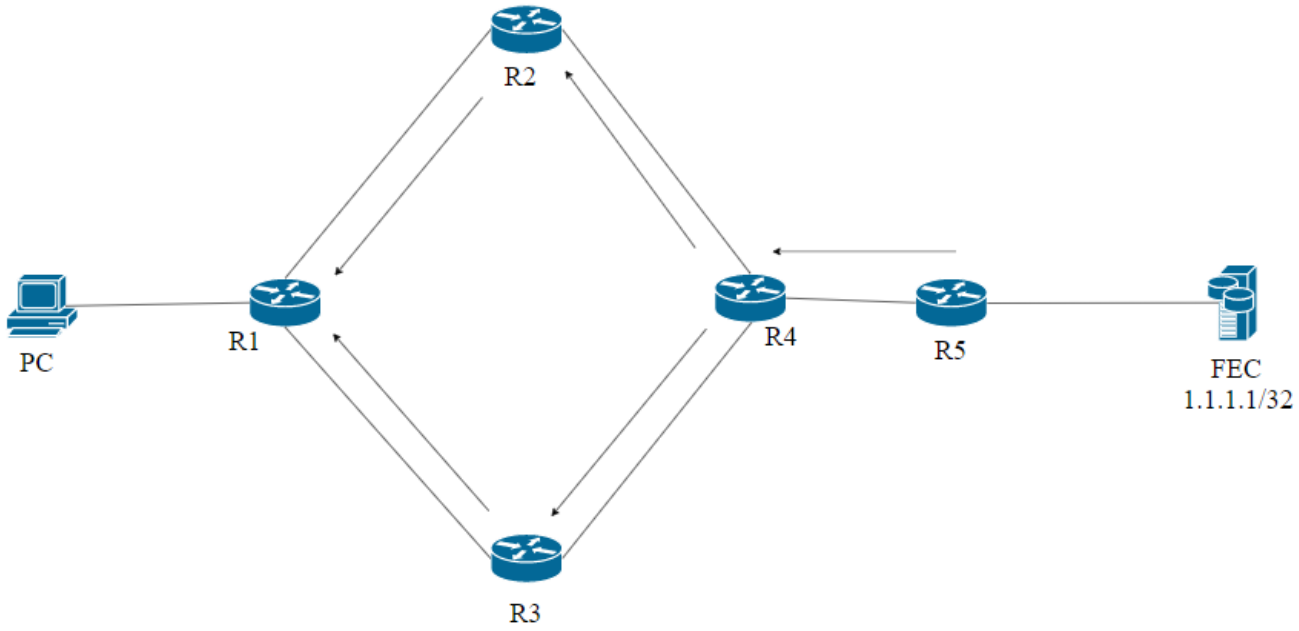


Рисунок 2.5 – LSP мережа з налаштованим FEC, та рух міток в ній

Як тільки в мережі встановлюється таблиця адресацій FEC, починається переадресація міток в усіх LSR маршрутизаторах. Коли на цей FEC поступає певний пакет інформації, відбувається почергова зміна міток:

1) маршрутизатор R5 дає запит для R4 про отримання пакета з міткою «0» для FEC 1.1.1.1/32. Ця мітка яка є статичною, та вказує на видалення всіх MPLS міток з пакету, адже R5 є вихідним LSR в LSP тракту;

2) в свою чергу R4 дає запит R3 та R2 на отримання свого пакета з міткою, вона може бути різноманітною, та взята з стека міток;

3) маршрутизатор R3 та R2 дають запит на отримання мітки з R1, після чого запитів немає, адже LSP закінчується.

По-друге, пакети можуть переадресовуватися по запиту, та безумовно. Тобто DoD - Downstream-on-Demand / Do - Downstream Unsolicited .

В випадку DoD , R1 просить мітку в R2 , той в свою чергу виділяє та сповіщає її. У випадку Do, R2 нічого не очікує, а просто відправляє мітку на R1.

По-третє, є два режима отримання міток для всіх LSR:

1) функція Independent Control – дозволяє нам відразу будувати шлях LSP, як тільки крайній LSR дізнається свій FEC, тобто свої мітки отримають відразу всі;

2) функція Ordered Control – відправка міток йде послідовно, тобто якщо наступний LSR , від крайнього не отримає мітку, він буде неефективний цей час.

По-четверте, LSR має можливість зберігати лишні мітки, також може їх відразу видаляти. Тобто, якщо R1 отримує мітки від R2 та R3, в залежності який шлях було вибрано транспортування пакету, ті мітки які не використовувалися в шляху видаляються або ні. Якщо мітки видаляються, то буде більше економніше використовуватися простір міток, а якщо не видаляються, то при поломці на шляху завжди буде резервний шлях. Ці режими називаються LRM – коли мітки зберігаються, CRM – коли мітки видаляються.

Всі ці режими застосовуються в таких протоколах як LDP та RSVP TE, вони є два максимально різними методами рішень цих проблем, адже є дві основні цілі , це розподіл сервісних та транспортних міток. Саме транспортні мітки застосовуються для передачі трафіка по мережі MPLS, та для них використовуються вищевказані протоколи. Сервісні мітки розподіляються для різних сервісів, та для них вже використовується протокол MBGP. Для роботи всіх динамічних протоколів, потрібно щоб була базова конфігурація IP зв’язків. Для цього в мережі потрібно підключити IGP. Найпростіше розподіляти мітки, це використовувати протокол LDP.

Цей протокол автоматично генерує та обмінюється мітками між маршрутизаторами LSR. Кожен маршрутизатор буде локально генерувати мітки для своїх префіксів, а потім буде передавати значення міток між своїми сусідами. Цей стандарт заснований на власному протоколі TDP (протокол розподілу міток) від Cisco. Компанія створила протокол, а стандарт - пізніше. У наш час майже всі використовують LDP замість TDP. Як і багато інших протоколів, LDP спочатку встановлює сусідство між іншими LSR , перш ніж він обміняється інформацією про мітки. Це працює дещо інакше, ніж більшість протоколів динамічної маршрутизації.

Реалізація протоколу відбувається саме так, що спочатку ми надсилаємо багатоадресні пакети UDP для виявлення інших сусідів. Як тільки два LSR вирішили стати сусідами, тобто надіслали одне одному UDP повідомлення «Hello», вони готові встановити сесію за допомогою TCP-з'єднання . Потім це

з'єднання використовується для обміну інформацією про мітки та помилки. Зазвичай для примикання сусідів використовується інтерфейс зворотного зв'язку. Далі наведено приклад реалізації LDP при комутації двох маршрутизаторів LSR (рисунок 2.6).

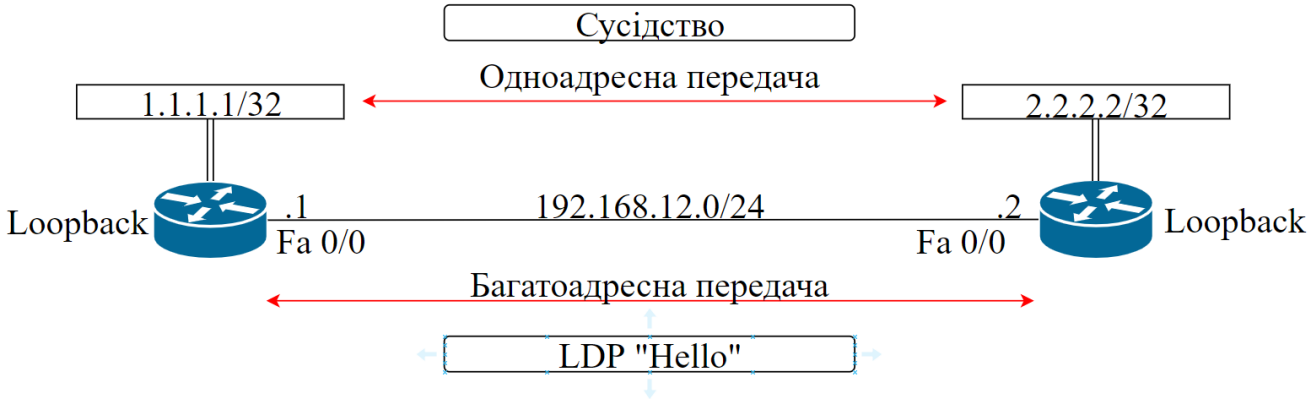


Рисунок 2.6 – Приклад комунікації маршрутизаторів в LDP

Два маршрутизатори, що наведені вище, послали багатоадресні пакети привітання на свої інтерфейси FastEthernet. У цьому пакеті з привітанням вони будуть розповідати про свою транспортну IP-адресу . Потім ця IP-адреса використовується для встановлення TCP-з'єднання між двома маршрутизаторами.

Коли ми використовуємо LDP на Cisco IOS, ми локально генеруємо мітку для кожного заголовка, який ми можемо знайти в RIB, за винятком заголовків BGP . Потім ця інформація додається до LIB (Label Information Base). Інформація в LIB використовується для побудови LFIB (інформаційної бази пересилання етикеток) . Коли маршрутизатору потрібно переслати пакет із позначкою MPLS, він буде використовувати LFIB для пересилання.

При маршрутизації в LDP, не використовуються протоколи динамічної маршрутизації. Вся інформація береться з таблиці маршрутизації LSR при наповнені міток. Отже, на R1 прийшло дві мітки тільки для одного FEC, але сусідні маршрутизатори різні, тому шлях LSP буде обраний тільки через найкращий інтерфейс. Для того, щоб запрацював LDP, потрібно запустити основний протокол динамічної маршрутизації, навіть RIP підійде. Якщо основний

шлях виходить з ладу, спочатку має запрацювати маршрутизація і тільки тоді починає працювати LDP.

Проблемами протоколу є те, що в домені MPLS будується велика кількість LSP до різних адресів FEC. Це впливає на завантаженість мережі та зменшується стек міток.

Одним із рішенням була поява нового протоколу з назвою RSVP – TE. Протокол використовується маршрутизаторами для доставки запитів про якість обслуговування (QoS) до всіх вузлів вздовж шляху передачі даних та встановлює підтримку стану запитуваної послуги. Запити RSVP зазвичай призводять до резервування ресурсів у кожному вузлу вздовж шляху до даних. Тобто протокол будує LSP при умовах певних обмежень з резервом ресурсів на кожному вузлу від вхідного LSR до вихідного. Головними атрибутами RSVP є:

1) підтримує як пакети IPv4, так і IPv6, що мають змогу надсилатися через LSP, та сигналізуються RSVP;

2) залежить від теперішніх і майбутніх протоколів маршрутизації, але сам по собі не є протоколом маршрутизації;

3) дозволяє одержувачу потоку даних ініціювати та підтримувати резервування ресурсів, що використовується для цього потоку;

4) здійснює резервування ресурсів для односпрямованих потоків даних.

Основною властивістю RSVP є те, що він працює разом з Traffic Engineering. Завдяки Traffic Engineering (TE), замість того, щоб надсилати трафік через найкоротший шлях, але перевантажений. TE спрямовує призначений трафік через недостатньо використані або простої в вузлах, тим самим розподіляючи навантаження пропускної здатності в мережі. TE тунелі також забезпечують механізм створення шляхів з певними характеристиками якості обслуговування (QoS). Основними перевагами MPLS Traffic Engineering є уникнення навантажень мережі та ефективне використання існуючих ресурсів, які можуть не працювати чи недостатньо використовуватися. Переміщаючи трафік від надмірно використовуваних міток до недостатньо використовуваних, TE уникає перевантаження мережі, спричинене занадто великим трафіком на найменш

витратному каналі. Це допомагає запобігти падінню пакетів і гарантує доставка даних.

Запит RSVP складається з FlowSpec що визначає вимогу до якості обслуговування (QoS) для потоку транспорту і FilterSpec, який визначає, який потік повинен отримувати пріоритет QoS. Як тільки необхідна смуга пропуску буде зарезервована по шляху з RSVP, пристрій зробивши запит, починає передавати трафік. Протокол в основному використовується для налаштування в реальному часі, або мультимедійних додатках бронювання пропускної здатності. Отже, RSVP повідомляє вимоги конкретних потоків трафіку до мережі. Протокол сигналізації RSVP був розширений за допомогою функцій MPLS для підтримки MPLS TE.

Під час резервування шляху для трафіку RSVP TE використовує чотири повідомлення:

1) пов. RSVP PATH - повідомлення, що використовується для перевірки доступних ресурсів на шляху TE і діє як запит на резервування;

2) пов. RSVP RESERVATION - коли маршрутизатор мережі в домені отримує повідомлення PATH, воно генерує повідомлення про підтвердження наявності ресурсів в запиті;

3) пов. RSVP ERROR - якщо ресурс при запиті на повідомлення PATH недоступний, то маршрутизатор який не може зарезервувати ресурс, генерує повідомлення про помилку RSVP і надсилає його маршрутизатору, з якого він отримав запит або відповідь;

4) пов. RSVP TEAR - повідомлення використовується для зриву резервування та вивільнення ресурсів для інших TE-тунелів, які можуть використовуватися.

Приклад резервування маршрутизаторів з передачею повідомлень можна оглянути на (Рис 2.7).

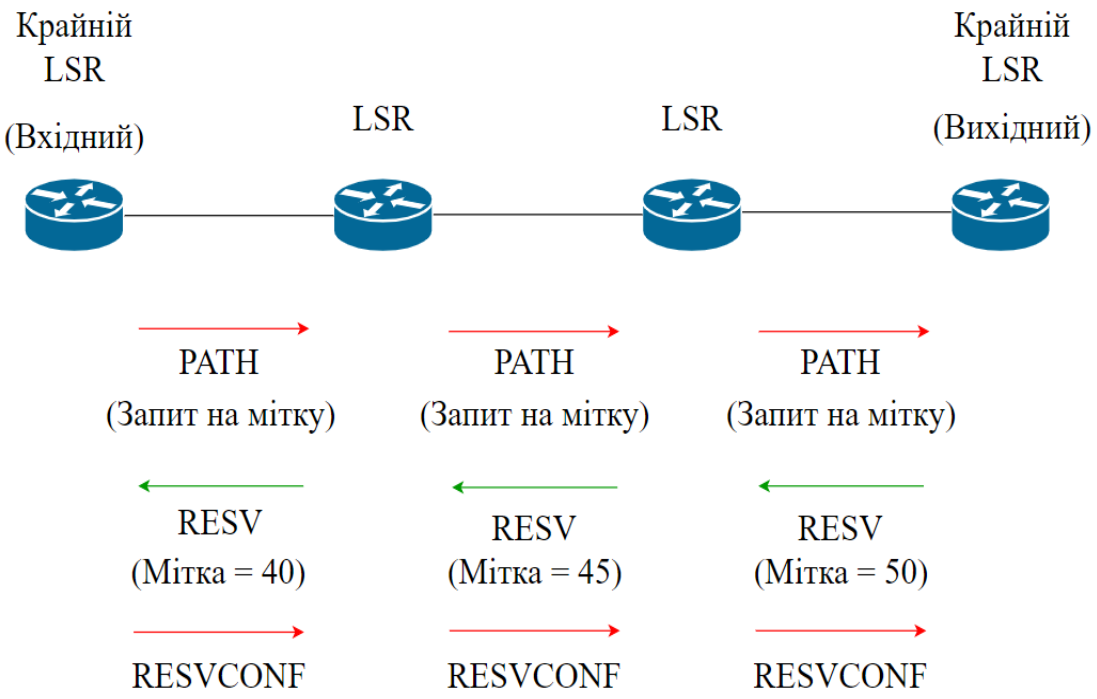


Рисунок 2.7 – Приклад резервування в RSVP TE

Щоб зарезервувати шлях через RSVP-TE, маршрутизатор, який є крайнім до FEC надсилає повідомлення RSVP PATH, яке перевіряє наявність запитуваних ресурсів на всіх LSR на шляху, де має будуватися TE-тунель. Отримавши повідомлення PATH, маршрутний маршрутизатор на шляху підтверджує «бронювання» повідомленням RSVP RESERVATION, що підтверджує призначення LSP тунелю TE. Потім це повідомлення поширюється вгору за течією до головного маршрутизатора через всі LSR на майбутньому шляху тунелю TE. Після того, як усі LSR на шляху приймають і підтверджують LSP, MPLS TE на шляху LSP працює. З цим, головний маршрутизатор потім може спрямовувати рух через нові тунелі на основі потреби ресурсів у трафіку, що передається.

2.5 Висновки

В цьому розділі ознайомилися з реалізацією технології комутацій по міткам. Зрозуміли де саме розміщуються заголовки міток в еталонній моделі OSI, тобто

на 2,5 рівні, між транспортним та канальним рівнем. Також ознайомилися з маршрутизаторами, що мають змогу працювати з технологією MPLS та як саме будується шлях комутації міток, такий як LSP. Розібрали можливі протоколи розподілу міток BGP та IGP, та як саме їх можна вбудувати разом з MPLS. Та розібрали протоколи в середині LSP, задля того, щоб вибрати кращий шлях розподілення міток, такі як LDP та RSVP – TE. Таким чином ми підготовилися до побудови власної MPLS мережі з використанням вищевказаних можливостей та протоколів.

3 РЕАЛІЗАЦІЯ ТА ТЕСТУВАННЯ ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ НА ОСНОВІ ВИБРАНОЇ ТЕХНОЛОГІЇ

3.1 Структурні особливості мережі, її схема та компоненти

Як ми вже знаємо, для побудови телекомунікаційної мережі , простий MPLS не використовується. Тому для цього було реалізовано MPLS L3VPN, що дає змогу увімкнути функціональність MPLS до віртуальної приватної мережі. Особливістю такої системи є те, що маршрутизатори PE –прикордонні маршрутизатори, присвоюють мітку для пакету, які надходять з клієнтських маршрутизаторів CE:

1) обмінюється оновленнями маршрутизації за допомогою маршрутизатора CE;

2) перекладають інформацію про маршрутизацію CE у маршрути VPN версії 4 (VPNv4);

3) обмінюється маршрутами VPNv4 з іншими маршрутизаторами PE через протокол багатопротокольного прикордонного шлюзу (MP-BGP).

4) Для побудови такої мережі, нам потрібно врахувати такі компоненти:

5) налаштування всіх учасників маршрутів VPN та їх список;

6) багатопротокольний BGP (MP-BGP), що проглядає маршрутизатори PE спільноти VPN - MP-BGP поширює інформацію про доступність VRF до всіх членів спільноти VPN. Пірин MP-BGP повинен бути налаштований на всіх маршрутизаторах PE у спільноті VPN;

7) переадресація MPLS - MPLS транспортує весь трафік між усіма учасниками спільноти VPN.

Отже, було розібрано MPLS L3VPN, тому можна розпочинати побудову мережі. Для цього було використано ядро з LSP трактом та з двома зовнішніми клієнтами, які безпосередньо можуть вступати в спілкування одне з одним(рисунок 3.1).

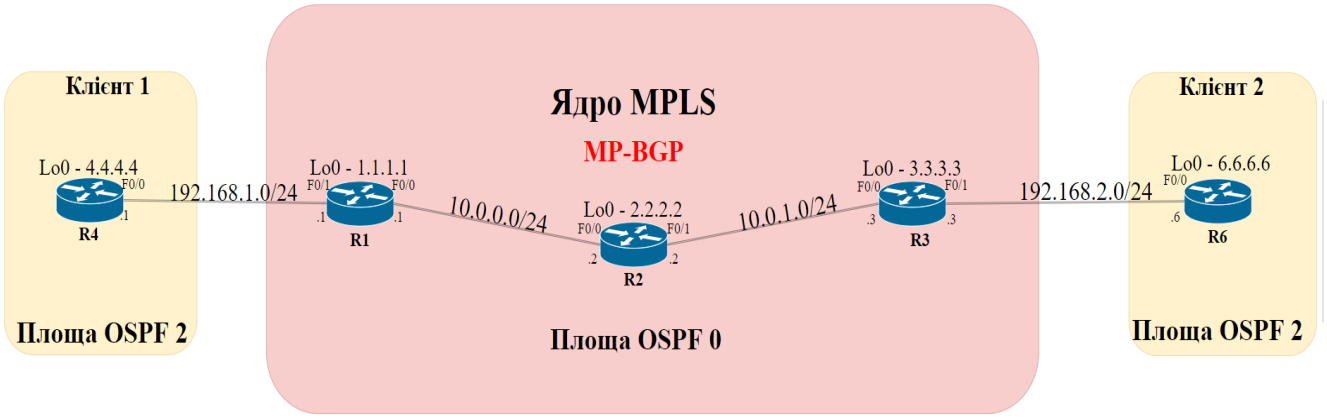


Рисунок 3.1 – Схема базової телекомунікаційної мережі на основі MPLS

Як ми можемо спостерігати, мережа складається з ядра MPLS, де підключено три LSR маршрутизатори. До ядра підключено два клієнта, що знаходяться в одному VRF.

VRF - це технологія, яка включена в Internet Protocol (IP), як мережевий протокол. Вона дозволяє декільком екземплярам таблиці маршрутизації працювати у віртуальному маршрутизаторі одночасно. Ця функціональність збільшує кількість підключень, дозволяючи сегментувати мережеві шляхи без використання декількох пристроїв. Оскільки трафік автоматично відокремлюється, VRF також підвищує безпеку мережі та може усунути необхідність шифрування та автентифікації. Інтернет-провайдери часто використовують переваги VRF для створення окремих віртуальних приватних мереж (VPN) для клієнтів. Коли це зроблено, це називається маршрутизацією та переадресацією VPN. У випадках, коли віртуальна маршрутизація та переадресація не може бути використана, клієнтський трафік маршрутизується за допомогою фізичних інтерфейсів або із фільтрацією на основі контролю доступу, що розділяє трафік. По цій причині, VRF набув популярності у корпоративних

локальних мережах (LAN), центрах обробки даних та постачальниках послуг, що використовують багатопротокольну комутацію етикеток (MPLS) та багатопротокольний протокол прикордонного шлюзу (MP-BGP). В даній мережі ця технологія працює на протоколі динамічної маршрутизаторі як OSPF, як протокол маршрутизації PE – CE.

Для побудови мережі, потрібно розібратися з мережевим обладнанням, які в цю мережу входять. А саме було вибрано маршрутизатори та їх можливе з'єднання між собою. Якщо для під'єднання їх між собою ми використовуємо популярний протокол Fast Ethernet, та всі можливі кабелю з підтримкою цього протоколу. До вибору маршрутизаторів виникають трудності, адже вони мають при собі мати всі підтримку MPLS, та ми маємо бути переконані, що всі пакети, залишатимуться на тому ж шляху, що і магістраль. Тому було вибрано маршрутизатор Cisco 3725 (рисунок 3.2).

Рисунок 3.2 – Маршрутизатор Cisco 3725

Даний маршрутизатор обладнаний багатьма функціями:

1) високопродуктивний 240-МГц процесор з обмеженим набором інструкцій (RISC);

2) до 256 МБ SDRAM;

3) до 128 Мб пам'яті CompactFlash;

4) два слоти для мережевих модулів, один з яких може вмістити подвійний широкий мережевий модуль;

5) три слоти для інтерфейсних карт.

Основною перевагою цього маршрутизатора є те, що з нього можна гарантовано зробити повноцінний LSR маршрутизатор з підтримкою LDP протоколу.

Фізично реалізувати таку мережу з використанням вибраних приладів досить важко, тому для реалізації було вибрано програмне забезпечення, що дає змогу емолювати та конфігурувати мережеву систему використовуючи різноманітні пристрої. Було вибрано GNS3, як один з безкоштовних емуляторів.

Це забезпечення дає змогу протестувати різне фізичне обладнання. Все виконується за допомогою віртуальної машини, до можна додати в систему віртуальної мережі комп’ютери, які імітують різні операційні системи. Якщо порівняти GNS3 з іншим популярним програмним забезпеченням, таким як Cisco Packet Tracer. Це програмне забезпечення ми використовували на курсі навчання. Відмінностями програмного забезпечення GNS3 від програмного забезпечення Cisco Packet Tracer є:

1) GNS3 є емулятором, а Cisco Packet Tracer - симулятором. Робимо висновок, що поки GNS3 запускає операційну систему, що використовується на реальному маршрутизаторі, Packet Tracer використовує програмну віртуальну операційну систему;

2) Проблеми з використанням всіх команд конфігурації в програмному забезпеченні Packet Tracer. Для GNS3 можна використовувати всі команди, діючі для IOS.

Робимо висновок, що в Packet Tracer ми не добилися б побудови MPLS мережі, тому для реалізації використовується GNS3. Перед роботою потрібно розібратися з робочою областю програми(рисунок 3.3).

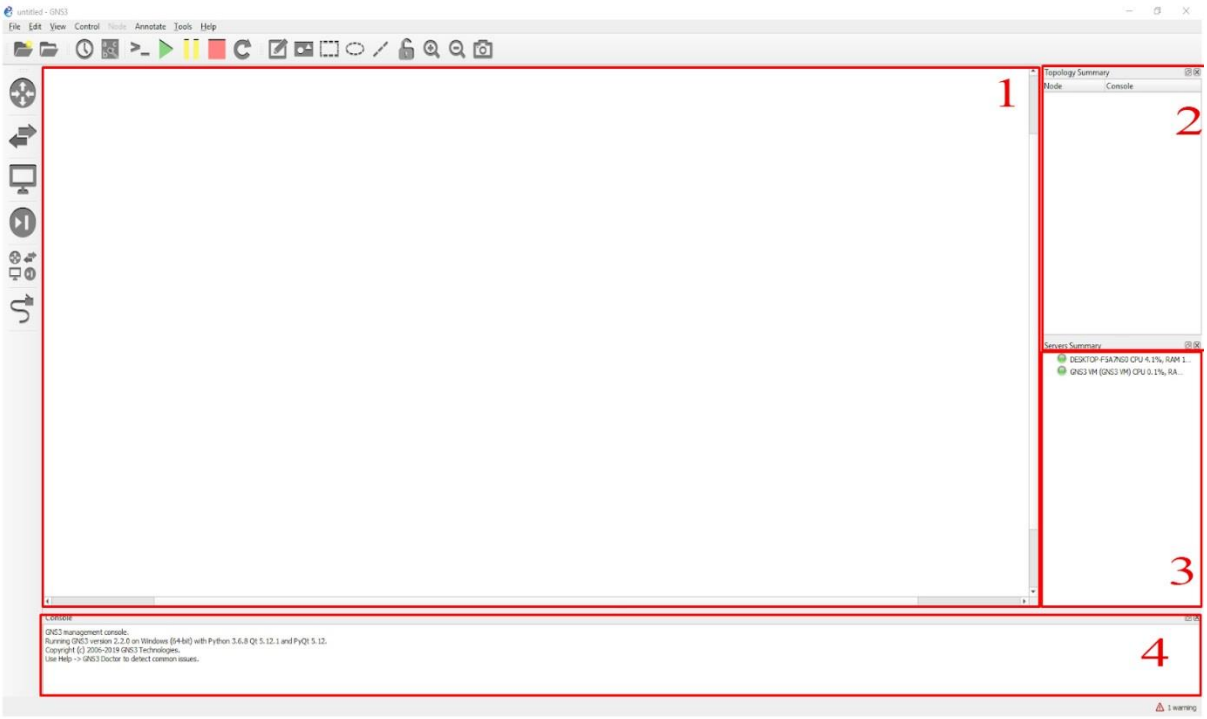


Рисунок 3.3 – Робоча область програми GNS3

На малюнку ми можемо спостерігати такі програмні області:

1) Робоча область, місце куда будуть «перетягуватися» пристрої, щоб побудувати топології;

2) Панель відображення пристроїв, які вже перебувають у робочій області, також їх стан (Вкл/Викл);

3) Область відображення серверів, віртуальні машини, тощо;

4) Область, де відображаються повідомлення про проблеми, з якими стикається сам GNS3.

Інші області є панелями інструментів, де наприклад ми можемо обрати наші девайси та переносити їх на робочу область.

3.2 Реалізація мережі в програмному забезпеченні GNS3

Як тільки було добавлено маршрутизатори Cisco 3725 в середовище програмного забезпечення можна починати добавляти їх на робочу область. Далі будуємо MPLS ядро, для цього розташовуємо маршрутизатори таким чином в області як на (рисунок 3.4). Тобто візьмемо маршрутизатори R1, R2 , R3, та з'єднаємо їх FastEthernet дротом.

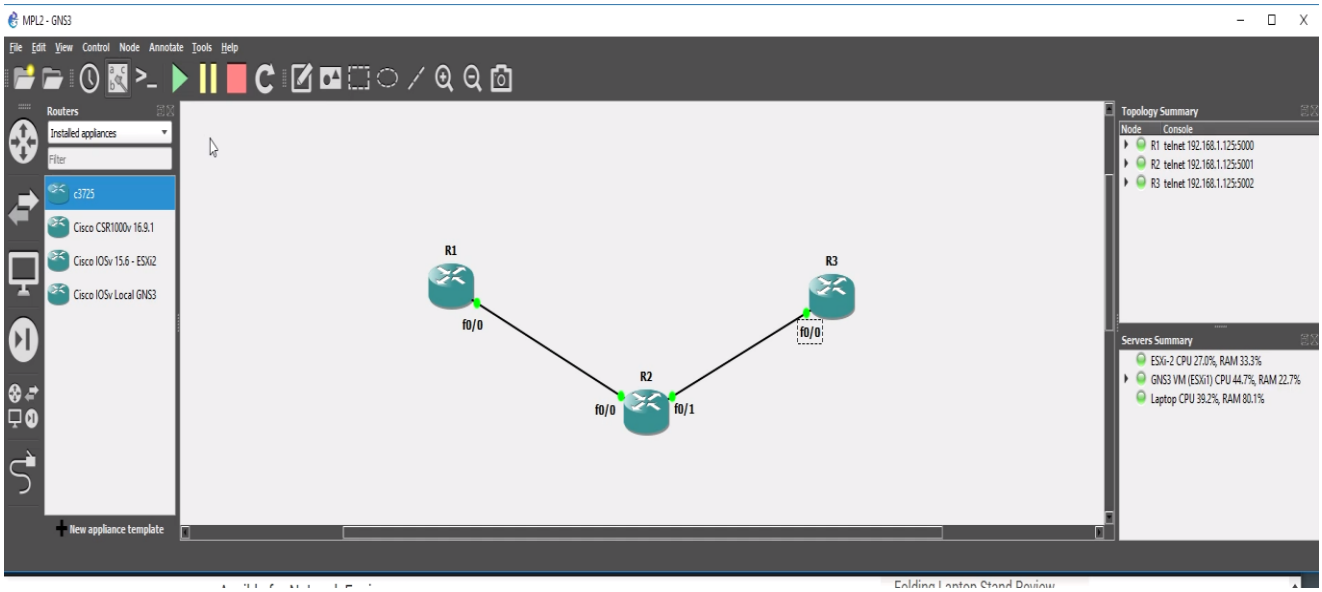


Рисунок 3.4 – Схема Ядра MPLS в GNS3

Далі потрібно конфігурувати маршрутизатори так, щоб кожен з них бачив Loopback, тобто мав адрес зворотного зв'язку на кожному з доданих пристроїв. Для цього ми налаштуємо OSPF маршрутизацію та добавимо петлі між R1 та R3.

Спочатку потрібно надати ім'я хосту на кожному з маршрутизаторів, далі налаштуємо Loopback, та надамо ip адресу на кожному задіяному інтерфейсім Fa0/0, чи Fa0/1. Приклад налаштування R1 маршрутизатора показано нижче:

```
R1
hostname R1
int lo0
ip add 1.1.1.1 255.255.255.255
ip ospf 1 area 0
```

```
int f0/0
ip add 10.0.0.1 255.255.255.0
no shut
ip ospf 1 area 0
```

Інші маршрутизатори конфігурують однаково, але використовують вже іншу IP-адресу для інтерфейсів та Loopback відповідно. Для R2 ми використовуємо Loopback – 2.2.2.2, та для R3 – 3.3.3.3

Наступним кроком буде налаштування вже самої MPLS технології, для цього ми можемо використовувати два варіанта:

1) на кожному інтерфейсі ввести `mpls ip` – команду;
2) під OSPF процесом , ввести команду `mpls ldp autoconfig`.

В вибраній мережі буде використовуватися другий варіант, тому ми вже налаштували OSPF динамічну маршрутизацію. Для кожного такого процесу впишемо цю команду, що дасть нам запустити протокол розповсюдження міток MPLS на кожному інтерфейсі, запущеному OSPF під цим конкретним процесом. Приклад виконання команди можна побачити нижче:

```
router ospf 1
mpls ldp autoconfig
```

Після підключення MPLS LDP на кожному маршрутизаторі, нам має прийти повідомлення, щодо підняття LDP сусідів Можна точно відповісти, що ми вже використовуємо MPLS в нашій мережі з піднятими в ній сусідство LDP.

Наступний кроком є налаштування MP-BGP, щоб конфігурація VPN 3 рівня почала функціонувати. Нам потрібно встановити сеанс багато протокольного BGP між R1 і R3, це робиться шляхом налаштування сімейства адресу vpnv4, як показано нижче на R1

```
R1#
router bgp 1
 neighbor 3.3.3.3 remote-as 1
 neighbor 3.3.3.3 update-source Loopback0
 no auto-summary
 !
```

```
address-family vpnv4
neighbor 3.3.3.3 activate
```

Маршрутизатор R2 налаштовувати не потрібно, як ми вже знаємо він налаштовується автоматично після конфігурації крайніх LSR в BGP протокол. Щоб рухатися далі, потрібно після введення команди отримати повідомлення журналу, щодо найближчих сеансів BGP. Після отримання повідомлення ми можемо говорити, що VPN в нас побудований, але немає клієнтів між якими муде здійснюватися передача.

Наступним кроком буде додавання до нашої топології, ще два маршрутизатори. Це будуть сайти клієнтів, підключені до R1 та R3 відповідно(рисунок 3.5).

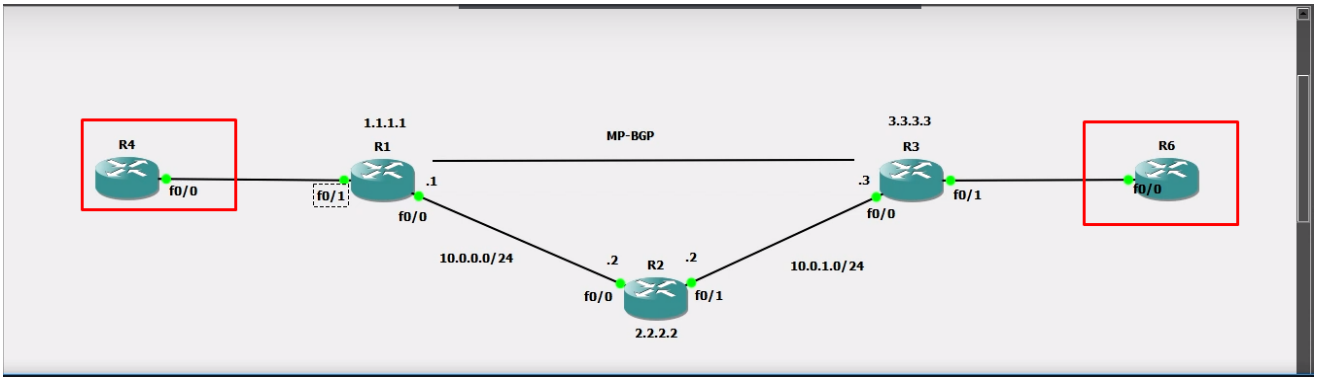


Рисунок 3.5 – Додання двох маршрутизаторів до нашого Ядра MPLS

Ми додали маршрутизатор R4 та R6. Спочатку потрібно налаштувати R4, для цього його конфігуруємо так, щоб він аналізував OSPF використовуючи другий процес ,що прямує до VRF. Його ми налаштовуємо на R1. Так цей маршрутизатор використовує локальну адресу сайту 192.168.1.0/24. Приклад налаштування R4 та інтерфейсу Fa0/1 в R1 нижче.

```
R4
int lo0
ip add 4.4.4.4 255.255.255.255
ip ospf 2 area 2
int f0 / 0
ip add 192.168.1.4 255.255.255.0
```

```
ip ospf 2 area 2
no shut


R1
int f0 / 1
no shut
ip add 192.168.1.1 255.255.255.0
```

На даний момент ми маємо R4, який заглядає до R1, але в глобальній таблиці маршрутизації R1 ще не налаштований повноцінно.

Наступний крок буде налаштуванням VRF. Використання цієї технології допоможе нам розрізняти клієнтів. Як приклад, якщо R1 був маршрутизатором PE провайдера та у нього було два клієнти, до яких обидва отримували адреси локально з адресним простором 192.168.1.0/24, він міг би розмістити обидві їх таблиці маршрутизації в різних VRF - це робить різницю між двома їх за допомогою різниці маршрутів. Отже відкриємо маршрутизатор R1, та налаштуємо в ньому VRF. Наприклад конфігуруємо в ньому VRF зі станом RED.

```
R1
ip vrf RED
rd 4:4
route-target both 4:4
```

Де RD слугує як індикатор та робить унікальну адресу VPNv4 у мережі MPLS, а route-target визначає, які префікси імпортуються та експортуються на PE-маршрутизаторах. Ці два значення не повинні бути однаковими. Далі після налаштування VRF на R1, ми переміщаємо інтерфейс F0/1 в цей VRF.

```
R1
int f0/1
ip vrf forwarding RED
```

Після команди можна спостерігати, що вже налаштована ip адреса на цьому інтерфейсі видаляється, тому потрібно її відновити аналогічно, як ми її підключали з самого початку.

Далі ми налаштуємо OSPF в зовнішньому інтерфейсі F0/1 на маршрутизаторі R1 та переведемо його в другу область.

```
R1
int f0/1
ip ospf 2 area 2
```

Після цього має з'явитися повідомлення, щодо появи нового сусіда по OSPF R4, з loopback 4.4.4.4. та через який інтерфейс. На цьому моменті можна сказати, що налаштування VRF з'єднання між R1 та R4 завершено. На підсумок можна сказати що ми помістили інтерфейс F0/1 в маршрутизаторі R4 у режим VRF. Також ми розмістили OSPF між R4 та R1 на іншому процесі, на відміну від ядра MPLS.

Наступним кроком буде конфігурування маршрутизаторів R6 та R3 за аналогічними командами. Відрізнятися будуть тільки loopback R6, вона буде мати адресу 6.6.6.6, та адреса інтерфейсу R6, буде становити 192.168.2.6. Налаштуємо на зовнішніх інтерфейсах також OSPF з процесом 2 області. VRF не повинен відрізнятися від VRF на маршрутизаторі R1. Налаштовуємо всі інтерфейси за прикладом R1 та R4.

Після налаштування та перевірки , нам потрібно зробити так, щоб маршрутизатор R4 міг пінгувати R6. Саме ця дія буде закінченням роботи, тому потрібно перерозподілити маршрути OSPF на MP-BGP у маршрутизаторах R1,R3. Приклад команди нижче

```
R1
router bgp 1
address-family ipv4 vrf RED
redistribute ospf 2
```

Ми маємо спостерігати, що 4.4.4.4 тепер знаходиться в таблиці BGP у VRF RED на R1 з наступним маршрутом на 192.168.1.4 (R4), а також 6.6.6.6 там також з наступним стрибком 3.3.3.3 (R3 - показуватиме, що він переходить в MPLS, а R1 немає бути). Також це ми маємо спостерігати в маршрутизаторі R3, 6.6.6.6 тепер

знаходиться в таблиці BGP в VRF RED на R3 з наступним стрибком 192.168.2.6 (R6), а також 4.4.4.4 там, а також з наступним стрибком 1.1.1.1(R1 - показує, що він переходить в MPLS, а R2 відсутній)

Останній крок полягає у поверненні маршрутів, які попали на MPLS, назад у OSPF, Це маршрутизатори R1 та R3, тоді ми можемо отримати наскрізне підключення. Приклад команди нижче

```
R1

router ospf 2
redistribute bgp 1 subnets
```

Після введення останньої команди, можна сміло казати, що мережа є готовою. Залишається провести тестування мережі в наступному підрозділі. Для цього будуть здійснені перевірки консольними командами на кожному з маршрутизаторів.

3.3 Тестування мережі в програмному забезпечення GNS3

Для перевірки в ядрі MPLS, чи всі loopback бачать одне одного ми використовуємо команду

```
R3#ping 1.1.1.1
```

Після введення команди, ми відправили ICMP запит на loopback маршрутизатора R1 з маршрутизатора R3. Також ми відправили таку ж команду, але вже на маршрутизатор R2. В результаті ми отримали таку відповідь(рисунок 3.6).

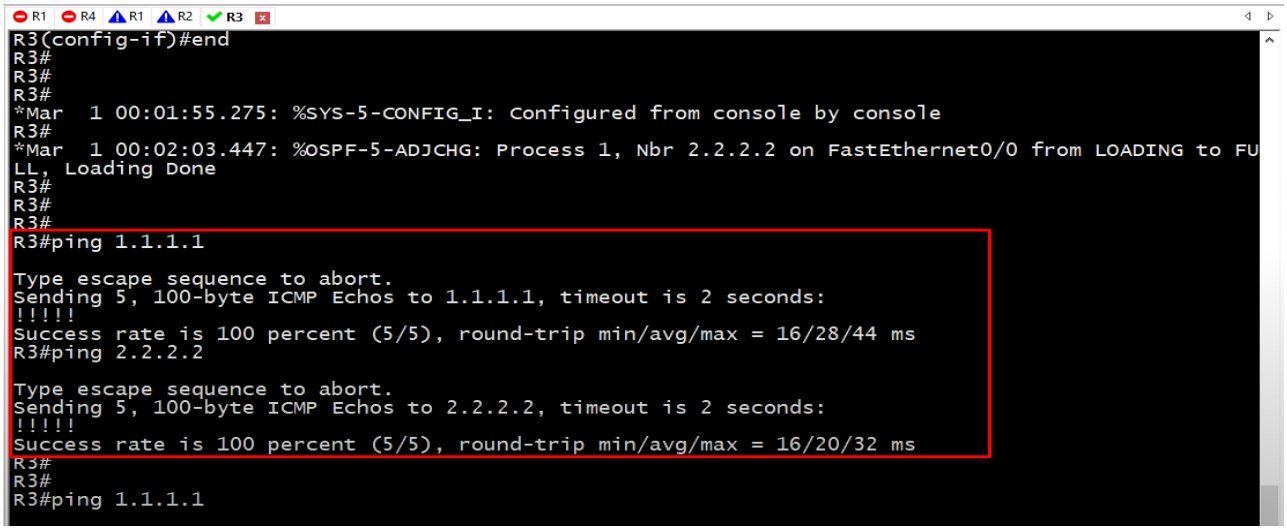


Рисунок 3.6 - Результат виконання команди ping на адресу loopback

Ми можемо спостерігати, що пакет без перешкод відправився до точки призначення, це означає що реалізація виконана виконана правильно.

Наступним буде перевірка підключення MPLS та LDP на нашому ядрі MPLS. Для цього використовуються такі команди як:

```
sh mpls interface
sh mpls ldp neighbors
```

Перша команда дозволяє нам перевірити інтерфейси MPLS, скільки їх працюють і який протокол вони використовують. Наступна команда дозволяє перевірити сусідство LDP. На прикладі маршрутизатора R2, ми використаємо ці команди для перевірки(рисунок 3.7).

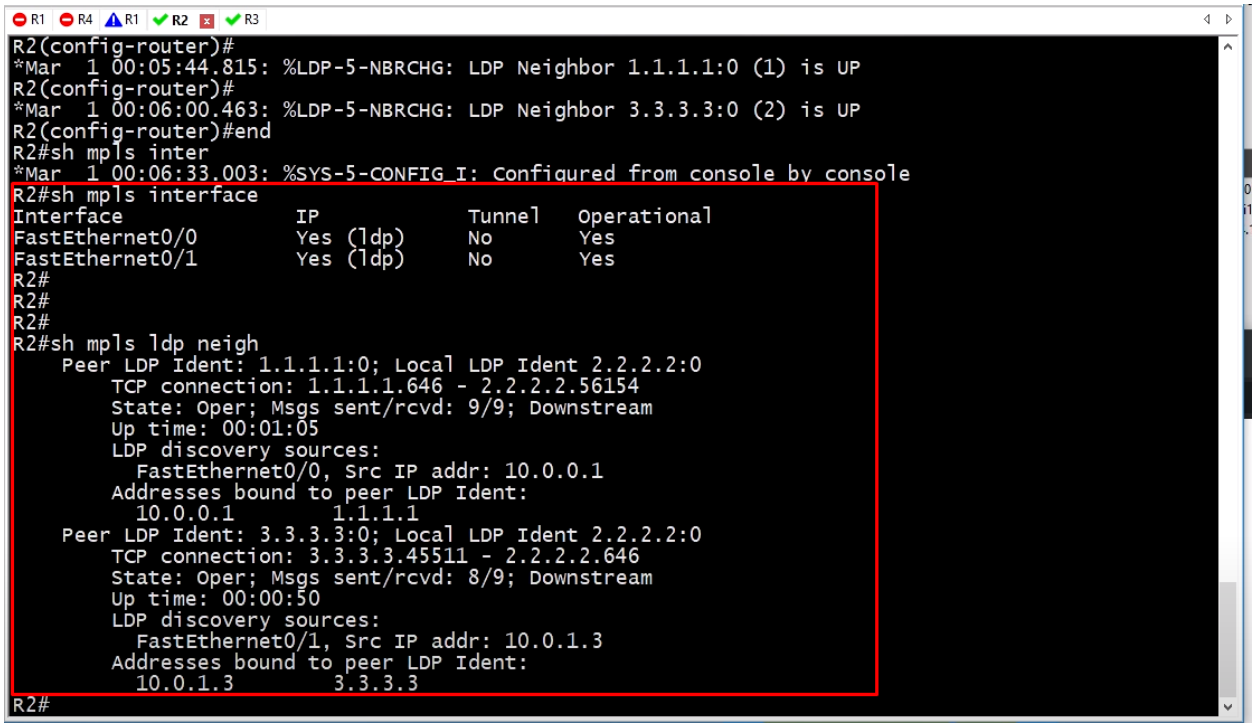


Рисунок 3.7 - Результат виконання команд перевірки MPLS та LDP

Для перевірки того що маршрутизатори дійсно обмінюються між собою пакетами з міткою, здійснимо трасування мережі, введемо команду

```
R1#trace 3.3.3.3
```

Ця команда нам показує як саме пакети рухаються в нашому ядрі MPLS з R1 до R3, результат виконання команди можна спостерігати на (рисунок 3.8).

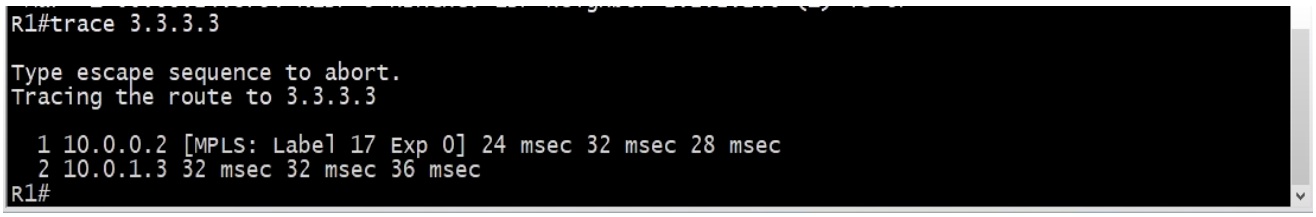


Рисунок 3.8 - Результат виконання трасування з R1 до R3

Можемо спостерігати шлях до R2 використовувало мітку MPLS у шляху «17», оскільки це дуже маленьке ядро MPLS, використовувалася лише одна мітка, оскільки R3 був останнім LSR у мережі, тому мітка з нього видаляється.

Далі потрібно перевірити налаштування BGP, робиться це за допомогою команди

```
R1#sh bgp vpnv4 unicast all summary
```

Після введення команди, ми отримуємо повідомлення, де вказано які сусіди з'єднані в протоколі BGP, та яка версія тунеля підключена(рисунок 3.9)

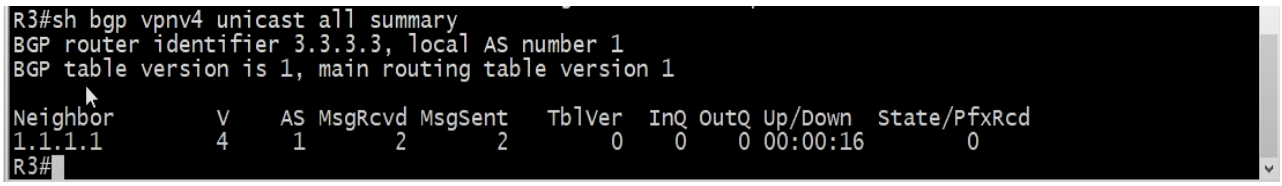


Рисунок 3.9 - Результат виконання команди перевірки BGP

Тут ви можете побачити, що у нас є bgp vpnv4, який заглядає до R1 - дивлячись на PfxRcd, ви бачите, що там написано 0, це тому, що у нас немає маршрутів у BGP.

Далі перевіримо чи після додавання R4 та R6 інтерфейси пінгують на R1 та R3 відповідно, після конфігурування адрес. Пропінгуємо з маршрутизатора R1 на інтерфейс маршрутизатора R4(рисунок 3.10).

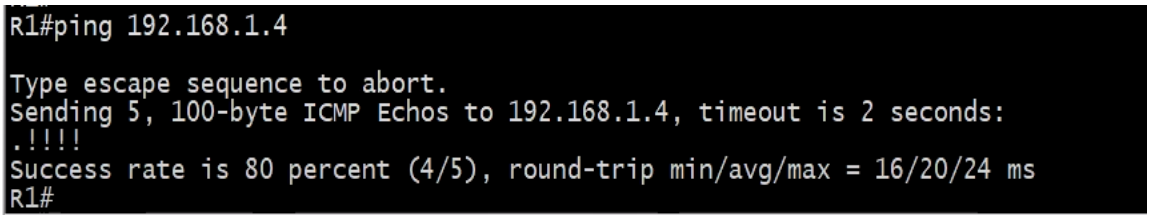


Рисунок 3.10 - Результат виконання команди ping на адресу інтерфейса R4

Після налаштування VRF на потрібних нам інтерфейсах перевіримо маршрути LSR R1 в таблиці маршрутизації VRF RED командою

```
R1 # sh ip route vrf RED
```

Можемо спостерігати loopback 4.4.4.4 маршрутизатора R4, на потрібному нам інтерфейсі та його ip-адреса 192.168.1.0 (рисунок 3.11).

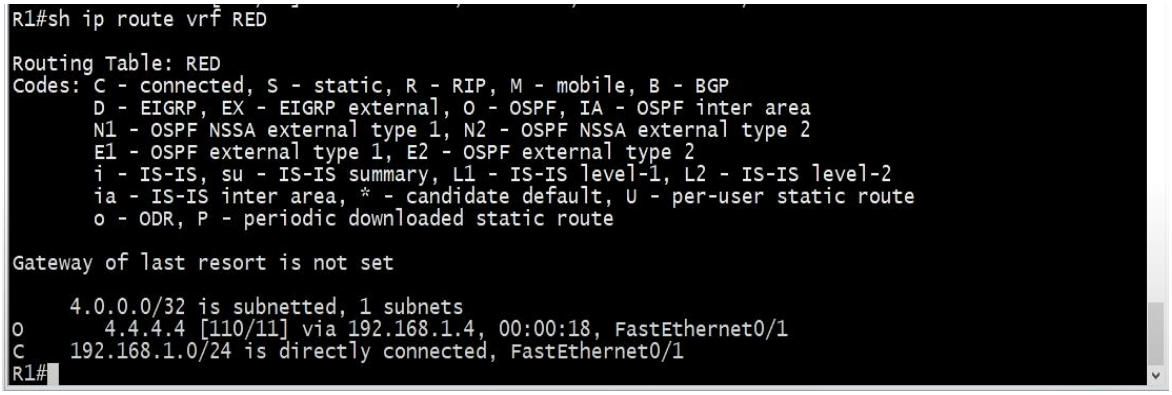


Рисунок 3.11 - Результат перевірки маршрутів в таблиці маршрутизації VRF RED R1.

Аналогічну перевірку треба також здійснити, але вже з маршрутизатором R3 (рисунок 3.12) після того, як ми його конфігуруємо за прикладом R1.

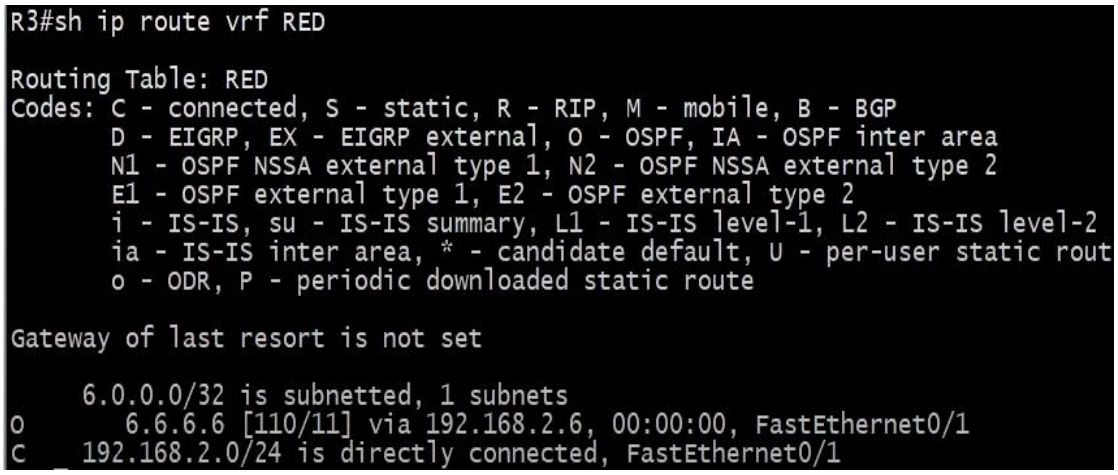


Рисунок 3.12 - Результат перевірки маршрутів в таблиці маршрутизації VRF RED R3.

Далі потрібно перевірити, з ким саме є зв'язок маршрутизатора R4, тому ми введемо команду `sh ip route` , для перевірки. Там ми можемо спостерігати, що є сусідство тільки з Loopback та з локальним інтерфейсом цього ж маршрутизатора.

Коли ми ми цією ж командою перевіряємо маршрутизатор R1, ми можемо спостерігати всі маршрути на кожен маршрутизатор в ядрі MPLS, але побачити маршрут до R4 ми не можемо. Для цього використовується команда `sh ip route vrf RED` , адже ми з'єднали ці маршрутизатори за допомогою VRF.

Тому після перерозподілення OSPF в MP-BGP ми перевіримо розподілення маршрутів в BGP на маршрутизаторі R1(рисунок 3.13).

```
R1#sh ip bgp vpnv4 vrf RED
BGP table version is 9, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - interna
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 4:4 (default for vrf RED)
*> 4.4.4.4/32       192.168.1.4              11         32768 ?
*>i6.6.6.6/32       3.3.3.3                  11    100      0 ?
*> 192.168.1.0      0.0.0.0                   0         32768 ?
*>i192.168.2.0      3.3.3.3                   0    100      0 ?
R1#
```

Рисунок 3.13 - Результат перевірки маршрутів BGP на R1

З перевірки ми спостерігаємо, що loopback R4 та R6 знаходяться в таблиці BGP в маршрутизаторі R1. Аналогічна перевірка відбувається на R3.

Далі, після повернення маршрутів які перебували в MPLS назад в OSPF, ми можемо спостерігати, що маршрутизатор R4 почав бачити ip – адресу loopback та інтерфейса R6(рисунок 3.14)

```
R4#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static rout
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     4.0.0.0/32 is subnetted, 1 subnets
C       4.4.4.4 is directly connected, Loopback0
     6.0.0.0/32 is subnetted, 1 subnets
O IA    6.6.6.6 [110/21] via 192.168.1.1, 00:00:24, FastEthernet0/0
C    192.168.1.0/24 is directly connected, FastEthernet0/0
O IA 192.168.2.0/24 [110/11] via 192.168.1.1, 00:00:24, FastEthernet0/0
R4#
```

Рисунок 3.14 - Результат перевірки маршрутів R4 після запуску OSPF

Залишається зробити дві основні перевірки. Це перевірка на пінг з клієнта R4 до клієнта на R6(рисунок 3.15).

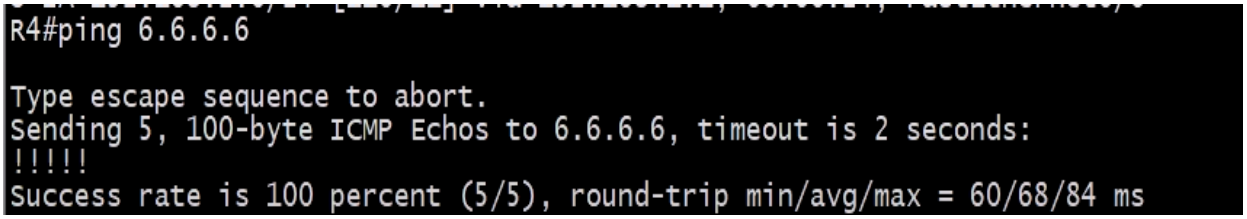


Рисунок 3.15 – Результат виконання команди ping з R4 до R6

За результатом ми розуміємо, що ICMP пакети успішно добралися з маршрутизатора R4 до R6. Також потрібно перевірити трасування мережі з R4 до R6. Так ми зрозуміємо, як саме пакет передавався по вузлам, та що з ним відбувалося на кожному з маршрутизатору(рисунок 3.16).

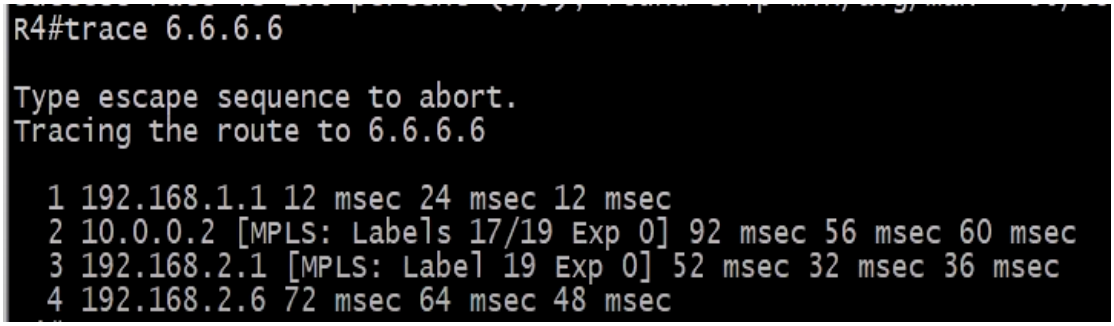


Рисунок 3.16 – Результат виконання команди trace з R4 до R6

Можемо спостерігати такий маршрут розподілу трафіку:

1) пакет прямує з маршрутизатора R4 (4.4.4.4) на інтерфейс F0/1(192.168.1.1) маршрутизатора R1;

2) далі він потрапляє в ядро MPLS на R1, де отримує мітку «17», потім він по інтерфейсу F0/0(10.0.0.2) потрапляє в LSR R2, Там мітка «17» змінюється на мітку «19». Остання мітка має бути «0», що каже, потрібно видалити мітку зі стеку;

3) наступна точка відбувається на інтерфейсі F0/1(192.168.2.1), маршрутизатора R3, тут мітка «19» змінюється на мітку «0» та вивільняється;

4) далі пакет потрапляє вже без мітки на інтерфейс F0/0(192.168.2.6) маршрутизатора R6, тут він потрапляє на 6.6.6.6 та закінчується

3.4 Вартість проекту

Проектуючи телекомунікаційну мережу , було пораховано приблизну вартість апаратних пристроїв які використовувалися. Станом на 2021 рік, ціни на всі ці пристрої та компоненти становлять(таблиця 3.1).

Таблиця 3.1 – Таблиця цін на елементи

Назва	Ціна
Маршрутизатор Cisco 3725/ 5 шт.	2332,04 грн./ 11660.2 грн. за 5 шт
4-парний UTP кабель FastEthernet	11302 грн/км

Отже, приблизна сума проекту буде 22962.2 грн. Сума може змінитися, залежно від довжини кабелю , та якщо купувати маршрутизатори б/у.

3.5 Висновки

Працюючи над третім розділом ми досягнули основної мети роботи, а це побудували власну телекомунікаційну мережу з використанням MPLS. Також було досягнено практичного розуміння тих протоколів маршрутизації, що розібрали у другому розділі. А саме це були:

1) протокол OSPF;
2) протокол BGP;
3) протокол LDP.

Також було спроектовано не просто MPLS, а дійсно телекомунікаційну мережу з використанням MPLS VPN. Для цього використовувалася технологія VRF, щоб тунелювати адресу кожного з клієнтів та щоб кілька екземплярів таблиці маршрутизації співіснували в маршрутизаторі та працювали разом.

ВИСНОВКИ

У ході розробки кваліфікаційної роботи та реалізації виданого завдання, було набуто практичних навичок створення телекомунікаційної мережі разом з технологією MPLS, набуто та освоєно теоретичний матеріал, необхідний для подальшої практичної інженерної діяльності, для реалізації ПЗ було також розглянуто методи побудови телекомунікаційних мереж, принципи функціонування різних топологій мереж, всі сім рівнів еталонної моделі OSI з протоколами на кожному з рівнів, протоколи переадресування міток та їхньої маршрутизації, проаналізовано іноземні джерела, пов’язані з темою бакалаврської роботи, а також підсумовуючи усе вище сказане, було розроблено телекомунікаційну мережу використовуючи програмне забезпечення GNS3.

У ході виконання проекту було написані консольні команди для маршрутизаторів, щоб активувати MPLS технологію , розроблено схематичний малюнок поставленої мережі з описом кожного інтерфейсу, що суттєво полегшило розробку безпосередньо телекомунікаційної мережі яка описується в темі роботи.

Створена мережа реалізує MPLS VPN між двома клієнтами, завданням якої є надіслати трафік з одного сайту на інший використовуючи транспортну мережу з комутацією за мітками. Отже, мета даної роботи досягнена, а поставлені задачі вирішені.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Али С., Симоненко А.В. Потоковая модель динамической балансировки очередей в MPLS-сети с поддержкой traffic engineering queues. *Проблемы телекоммуникаций*. 2010. № 1. с. 59–67.

2. Hemmendinger, David. "Wide area network". *Encyclopedia Britannica* URL:https://www.britannica.com/technology/telecommunications-network/Spread-spectrum-multiple-access (дата звернення 05.03.2021).

3. Корпоративні мережі. URL: www.vaco.net.ua/solutions-corp-networks (дата звернення 08.05.2021).

4. Dr.Anton A. Chuvakin, Branden R. Williams, in PCI Compliance. 2010 chapter 7.

5. J. C. Bedoya, J. Xie, Y. Wang, X. Zhang and C. Liu, "Resiliency of Distribution Systems Incorporating Asynchronous Information for System Restoration," in IEEE Access, vol. 7, pp. 101471-101482, 2019, doi: 10.1109/ACCESS.2019.2930907.

6. Luka Humski , Darko Striga, Vedran Podobnik, Boris Vrdoljak, Marko Banek, Zoran Skocir, Ignac Lovrek . Building implicit corporate social networks: The case of a multinational company. 2013. pp 51-79

7. Lukas Tanutama Characterizing corporate network traffic beyond bandwidth. 2014 . с. 11-23

8. A. R. Eremina, Yu. V. Malinkovskii. Invariance of the stationary distribution of states of networks with multimode service, different types of requests, and discriminatory processor sharing. 2012. pp 170-178.

9. Mark Filer, Jamie Gaudette, Monia Ghobadi, Ratul Mahaja, Tom Issenhuth, Buddy Klinkers, Jeff Cox. Elastic optical networking in the microsoft cloud. 2013. pp A45 - A54

10. I. V. Botsman Universal Corporate Wireless Network Architecture. 2010, pp 14-15

11. А. Г. Микитишин, М. М. Митник, П. Д. Стухляк, В. В. Пасічник. Комп'ютерні мережі. Львів: «Магнолія 2006». 2013. 256 с.

12. Азаров О. Д., Захарченко С. М., Кадук О. В. Комп’ютерні мережі : навчальний посібник та ін. Вінниця:ВНТУ. 2013. 371с.

13. Cisco. URL: www.cisco.com(дата звернення 05.05.2021).

14. Types of Network Topology- EG. URL: https://www.geeksforgeeks.org/types-of-network-topology/(дата звернення 09.04.2021).

15. Physical Layer - OSI Reference Model. Study Tonight URL: https://www.studytonight.com/computer-networks/osi-model-physical-layer (дата звернення 09.04.2021).

16. Data-link Layer Introduction. URL: https://www.tutorialspoint.com/data_communication_computer_network/data_link_layer_introduction.htm (дата звернення 09.04.2021).

17. OSI Model. URL: https://networkdirection.net/articles/network-theory/osimodel (дата звернення 09.04.2021).

18. Luc De Ghein.MPLS Foundament. Cisco press. 2007. с651 с.

19. How MPLS Traffic Engineering works. URL: https://community.cisco.com/t5/networkingdocuments/how-mpls-traffic-engineering-works/ta-p/3128593(дата звернення 09.05.2021).

20. Tomas D. Nado , MPLS Network Management . 2003. p 203с.

21. Label Switching Router. URL: https://www.techopedia.com/definition/20284/label-switching-router-lsr (дата звернення 10.05.2021).

22. MPLS - ЯК ПРАЦЮЄ І НАВІЩО ПОТРІБЕН? URL: https://wiki.merionet.ru/seti/25/mpls-kakrabotaet- i-zachem-nuzhen/(дата звернення 10.05.2021).

23. Мережі для наймолодших. Частина дев’ята. Базовий MPLS. URL: https://habr.com/ru/post/246425/#ABOUT_MPLS(дата звернення 05.05.2021).

24. Alexander Goldstein, Bonch-Bruevich Federal Telecommunications UniversitySessions and Services Management Models in NGN/IMS and Post-NGN Networks Proceeding of the 21st. 2010. Vol. 42. Pp. 265–276.

25. Gateway. URL: https://searchsecurity.techtarget.com/definition/IGP (дата звернення 10.05.2021).

26. MPLS Border Gateway Protocol (BGP). URL: https://www.mplsinfo.org/border-gateway-protocol-bgp.html (дата звернення 10.05.2021).

27. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. Учебник для вузов. 5-е изд. СПб. Питер. 2016. 992с.

28. Бешлей М.І. Підвищення ефективності роботи комунікаційних мереж методом динамічного перерозподілу ресурсів між різними безпроводовими технологіями. Міжнародна науково-технічна конференція «Сучасні інформаціно-телекомунікаційні технології»: матеріали науково-технічної конференції .Т.2 - К: ДУТ. - 2015. - С. 49-50.

29. Кривуца В.Г, В.К.Стеклов, Л.Н.Беркман, Б.Я.Костік, В.Ф.Олійник, С.М.Скляренко. Управління телекомунікаціями із застосуванням новітніх технологій .Підр. для ВНЗ. – К.: Техніка. 2007. 384 с.

30. Klimowicz A.S., Solov’ev V.V. Minimization of incompletely specified Mealy finite-state machines by merging two internal states. 2013. Vol. 52. Pp. 409.

31. Жуков І.А., Дрововозов В.І., Масловський Б.Г. Експлуатація комп’ютерних систем та мереж: Навч. посібник, 2010. 368 с.

32. Chris Carthern, William Wilson, Noel Rivera, Richard Bedwell. Cisco Networks: Engineers' Handbook of Routing, Switching, and Security with IOS, NX-OS, and ASA . 1st ed. Edition by Springer; 1st ed. edition .2015. 870 pages.

33. Олифер В. Г., Олифер Н. А. Питер . Компьютерные сети. Принципы, технологии, протоколыю Юбилейное издание. 2020р. 1000с

34. Букатов А. А., Гуда С. А. Питер . Компьютерные сети: расширенный начальный курс., 2019р. 496с.

35. Эндрю, Уэзеролл Дэвид. Питерю. Компьютерные сети. Т, 2020р. 960с

36. Doug Lowe. For Dummies. Networking All-in-One For Dummies Paperback. 7th edition 2018. 992p.

37. Mike Meyers. McGraw-Hill Education. CompTIA Network Certification All-in-One Exam Guide, Seventh Edition 7th Edition. 2018. 960p.

38. Кошик Авинаш. Веб-аналитика 2.0 на практике. Тонкости и лучшие методики.. Диалектика. 2019г. 528с.

39. Майкл Коллинз. Защита сетей. Подход на основе анализа данных ДМК Пресс. 2019г. 308с.

40. Кріс Сандерс, Вильям. Анализ пакетов. Практическое руководство по использованию Wireshark и tcpdump. 2016г.448с.

ДОДАТОК А

(обов’язковий)

СПИСОК КОМАНД ДЛЯ КОНФІГУРАЦІЇ МАРШРУТИЗАТОРІВ

Команди для маршрутизатора R1:

```
hostname R1
int lo0
ip add 1.1.1.1 255.255.255.255
ip ospf 1 area 0

int f0/0
ip add 10.0.0.1 255.255.255.0
no shut
ip ospf 1 area 0

R1#ping 3.3.3.3 source lo0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 3.3.3.3, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/52/64 ms
R1#
router ospf 1
mpls ldp autoconfig
R1#trace 3.3.3.3

Type escape sequence to abort.
Tracing the route to 3.3.3.3

    1 10.0.0.2 [MPLS: Label 17 Exp 0] 84 msec 72 msec 44 msec
10.0.1.3 68 msec 60 msec *
R1#
router bgp 1
 neighbor 3.3.3.3 remote-as 1
 neighbor 3.3.3.3 update-source Loopback0
```

```
 no auto-summary
 !
 address-family vpnv4
  neighbor 3.3.3.3 activate
R1#sh bgp vpnv4 unicast all summary
BGP router identifier 1.1.1.1, local AS number 1
BGP table version is 1, main routing table version 1

Neighbor           V      AS  MsgRcvd  MsgSent    TblVer   InQ  OutQ  Up/Down
State/PfxRcd
3.3.3.3           4       1       218       218          1     0     0 03:17:48
0
int f0/1
no shut
ip add 192.168.1.1 255.255.255.0
ip vrf RED
rd 4:4
route-target both 4:4
int f0/1
ip vrf forwarding RED
R1(config-if)#ip vrf fo
R1(config-if)#ip vrf forwarding RED
% Interface FastEthernet0/1 IP address 192.168.1.1 removed due to enabling
VRF RED
int f0/1
ip address 192.168.1.1 255.255.255.0
R1#sh run int f0/1
Building configuration...

Current configuration : 119 bytes
!
interface FastEthernet0/1
 ip vrf forwarding RED
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
end

R1#
R1#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
```

```
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2
 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
 ia - IS-IS inter area, * - candidate default, U - per-user static route
 o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

1.0.0.0/32 is subnetted, 1 subnets
C 1.1.1.1 is directly connected, Loopback0
 2.0.0.0/32 is subnetted, 1 subnets
O 2.2.2.2 [110/11] via 10.0.0.2, 01:03:48, FastEthernet0/0
 3.0.0.0/32 is subnetted, 1 subnets
O 3.3.3.3 [110/21] via 10.0.0.2, 01:02:29, FastEthernet0/0
 10.0.0.0/24 is subnetted, 2 subnets
C 10.0.0.0 is directly connected, FastEthernet0/0
O 10.0.1.0 [110/20] via 10.0.0.2, 01:02:39, FastEthernet0/0
R1#sh ip route vrf red
% IP routing table red does not exist
R1#sh ip route vrf RED

Routing Table: RED
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2
 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
 ia - IS-IS inter area, * - candidate default, U - per-user static route
 o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

C 192.168.1.0/24 is directly connected, FastEthernet0/1
 int f0/1
 ip ospf 2 area 2
R1(config-if)#
 *Mar 1 01:12:54.323: %OSPF-5-ADJCHG: Process 2, Nbr 4.4.4.4
on FastEthernet0/1 from LOADING to FULL, Loading Done
R1#sh ip route vrf RED

Routing Table: RED
```

```
4.0.0.0/32 is subnetted, 1 subnets
O 4.4.4.4 [110/11] via 192.168.1.4, 00:02:32, FastEthernet0/1
C 192.168.1.0/24 is directly connected, FastEthernet0/1
R1
router bgp 1
address-family ipv4 vrf RED
redistribute ospf 2
R1#sh ip bgp vpnv4 vrf RED
BGP table version is 9, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best,
 r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? □ incomplete
router ospf 2
redistribute bgp 1 subnets
```

Команди для маршрутизатора R2:

```
hostname R2
int lo0
ip add 2.2.2.2 255.255.255.255
ip ospf 1 are 0

int f0/0
ip add 10.0.0.2 255.255.255.0
no shut
ip ospf 1 area 0

int f0/1
ip add 10.0.1.2 255.255.255.0
no shut
ip ospf 1 area 0
router ospf 1
mpls ldp autoconfig
R2#
*Mar  1 00:31:53.643: %SYS-5-CONFIG_I: Configured from console
*Mar  1 00:31:54.423: %LDP-5-NBRCHG: LDP Neighbor 1.1.1.1:0 (1) is UP
R2#
*Mar  1 00:36:09.951: %LDP-5-NBRCHG: LDP Neighbor 3.3.3.3:0 (2) is UP
R2#sh mpls interface
Interface              IP            Tunnel   Operational
```

```
FastEthernet0/0        Yes (ldp)     No       Yes
FastEthernet0/1        Yes (ldp)     No       Yes
2#sh mpls ldp neigh
    Peer LDP Ident: 1.1.1.1:0; Local LDP Ident 2.2.2.2:0
        TCP connection: 1.1.1.1.646 - 2.2.2.2.37909
        State: Oper; Msgs sent/rcvd: 16/17; Downstream
        Up time: 00:07:46
        LDP discovery sources:
          FastEthernet0/0, Src IP addr: 10.0.0.1
        Addresses bound to peer LDP Ident:
          10.0.0.1        1.1.1.1
    Peer LDP Ident: 3.3.3.3:0; Local LDP Ident 2.2.2.2:0
        TCP connection: 3.3.3.3.22155 - 2.2.2.2.646
        State: Oper; Msgs sent/rcvd: 12/11; Downstream
        Up time: 00:03:30
        LDP discovery sources:
          FastEthernet0/1, Src IP addr: 10.0.1.3
        Addresses bound to peer LDP Ident:
          10.0.1.3        3.3.3.3
```

Команди для маршрутизатора R3:

```
hostname R3
int lo0
ip add 3.3.3.3 255.255.255.255
ip ospf 1 are 0

int f0/0
ip add 10.0.1.3 255.255.255.0
no shut
ip ospf 1 area 0
router ospf 1
mpls ldp autoconfig
router bgp 1
 neighbor 1.1.1.1 remote-as 1
 neighbor 1.1.1.1 update-source Loopback0
 no auto-summary
 !
 address-family vpnv4
  neighbor 1.1.1.1 activate
int f0/1
```

```
no shut
ip add 192.168.2.3 255.255.255.0
ip vrf RED
rd 4:4
route-target both 4:4
int f0/1
ip vrf forwarding RED
R3(config-if)#ip vrf forwarding RED
% Interface FastEthernet0/1 IP address 192.168.2.1 removed due to
enabling VRF RED
int f0/1
ip address 192.168.2.1 255.255.255.0
R3#sh run int f0/1
Building configuration...

Current configuration : 119 bytes
!
interface FastEthernet0/1
ip vrf forwarding RED
ip address 192.168.2.1 255.255.255.0
duplex auto
speed auto
end
int f0/1
ip ospf 2 area 2
sh ip route vrf RED

Routing Table: RED
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP

Gateway of last resort is not set

     6.0.0.0/32 is subnetted, 1 subnets
O       6.6.6.6 [110/11] via 192.168.2.6, 00:02:44, FastEthernet0/1
C    192.168.2.0/24 is directly connected, FastEthernet0/1
router bgp 1
address-family ipv4 vrf RED
redistribute ospf 2
R3#sh ip bgp vpnv4 vrf RED
BGP table version is 9, local router ID is 3.3.3.3
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
```

```
r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

Network Next Hop Metric LocPrf Weight Path
Route Distinguisher: 4:4 (default for vrf RED)
*>i4.4.4.4/32 1.1.1.1 11 100 0 ?
*> 6.6.6.6/32 192.168.2.6 11 32768 ?
*>i192.168.1.0 1.1.1.1 0 100 0 ?
*> 192.168.2.0 0.0.0.0 0 32768 ?
router ospf 2
redistribute bgp 1 subnets
```

Команди для маршрутизатора R4:

```
int lo0
ip add 4.4.4.4 255.255.255.255
ip ospf 2 area 2
int f0/0
ip add 192.168.1.4 255.255.255.0
ip ospf 2 area 2
no shut
R4#sh ip route
4.0.0.0/32 is subnetted, 1 subnets
C 4.4.4.4 is directly connected, Loopback0
C 192.168.1.0/24 is directly connected, FastEthernet0/0
R4#sh ip route


4.0.0.0/32 is subnetted, 1 subnets
C 4.4.4.4 is directly connected, Loopback0
 6.0.0.0/32 is subnetted, 1 subnets
O IA 6.6.6.6 [110/21] via 192.168.1.1, 00:01:31, FastEthernet0/0
C 192.168.1.0/24 is directly connected, FastEthernet0/0
O E2 192.168.2.0/24 [110/1] via 192.168.1.1, 00:01:31, FastEthernet0/0
R4#ping 6.6.6.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 6.6.6.6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max= 40/48/52ms
R4#trace 6.6.6.6
```

```
Type escape sequence to abort.
Tracing the route to 6.6.6.6

1 192.168.1.1 20 msec 8 msec 8 msec
 2 10.0.0.2 [MPLS: Labels 17/20 Exp 0] 36 msec 40 msec 36 msec
 3 192.168.2.1 [MPLS: Label 20 Exp 0] 16 msec 40 msec 16 msec
 4 192.168.2.6 44 msec 40 msec 56 msec
R4#
```

Команди для маршрутизатора R6:

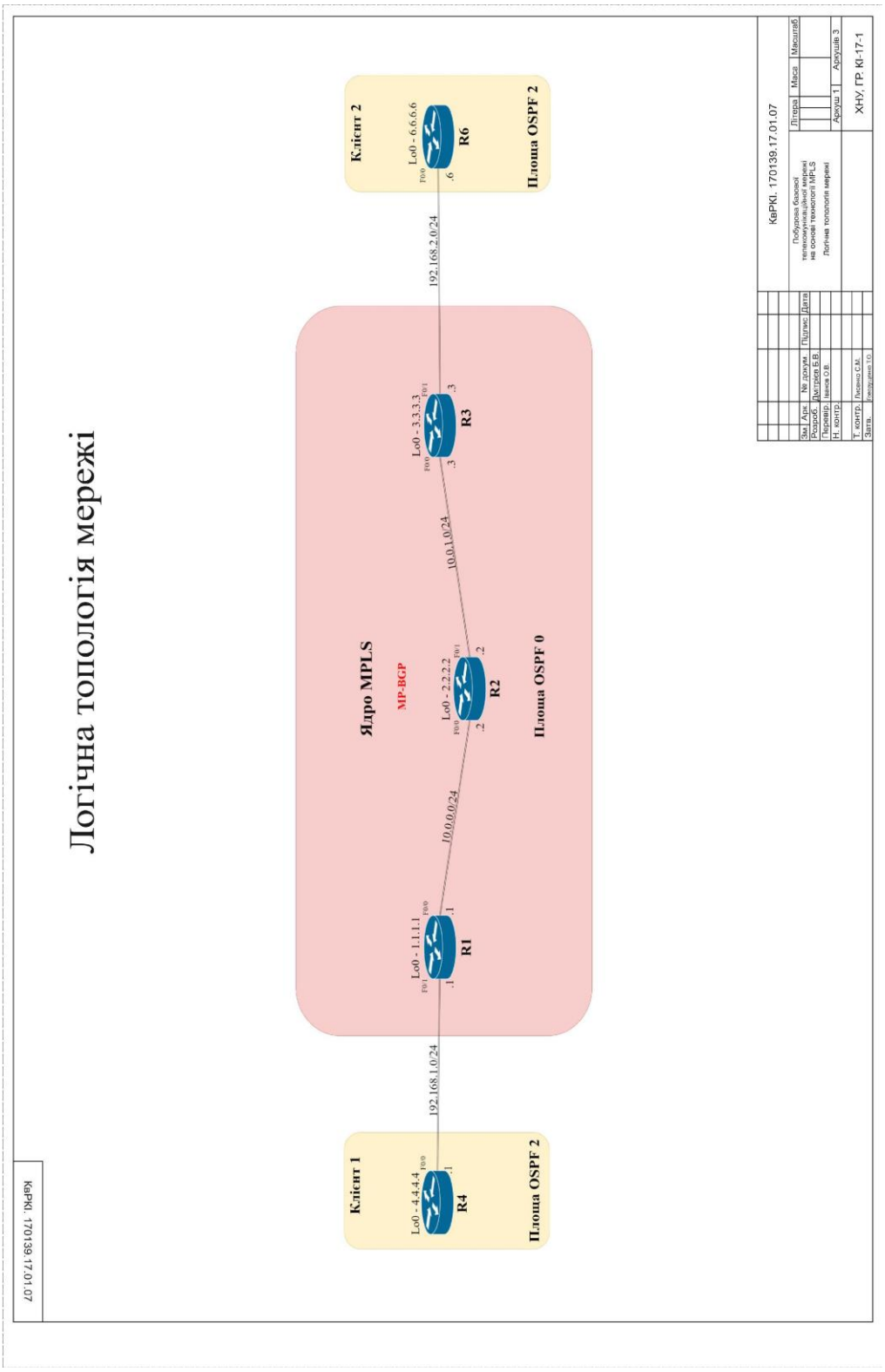
```
int lo0
ip add 6.6.6.6 255.255.255.255
ip ospf 2 area 2
int f0/0
ip add 192.168.2.6 255.255.255.0
ip ospf 2 area 2
no shut
R6#sh ip route

4.0.0.0/32 is subnetted, 1 subnets
O IA 4.4.4.4 [110/21] via 192.168.2.1, 00:01:22, FastEthernet0/0
6.0.0.0/32 is subnetted, 1 subnets
C 6.6.6.6 is directly connected, Loopback0
O IA 192.168.1.0/24 [110/11] via 192.168.2.1,00:01:22,FastEthernet0/0
C 192.168.2.0/24 is directly connected, FastEthernet0/0
```

ДОДАТОК Б

(обов’язковий)

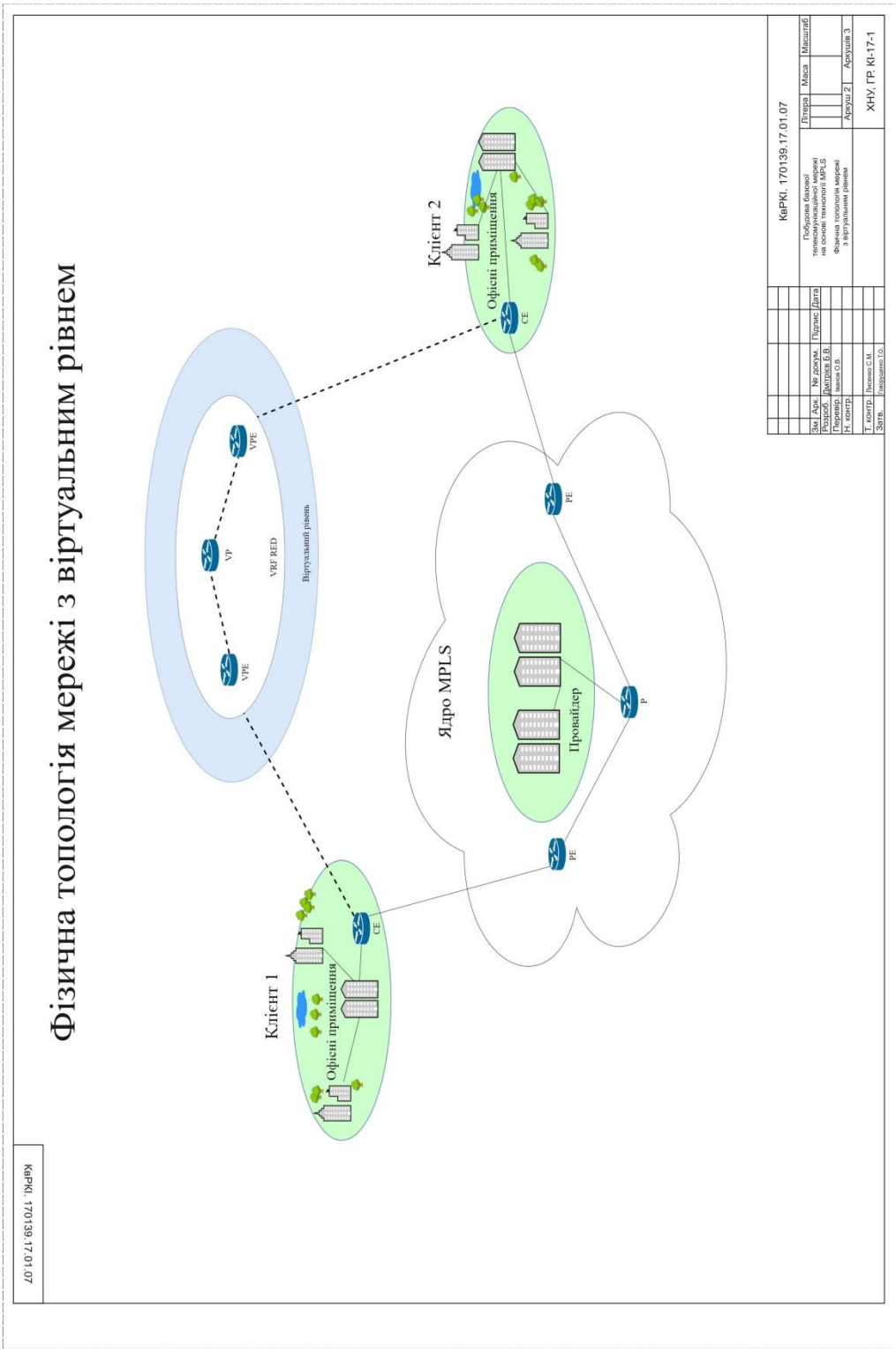
Копія схеми «Логічна топологія мережі»



ДОДАТОК В

(обов’язковий)

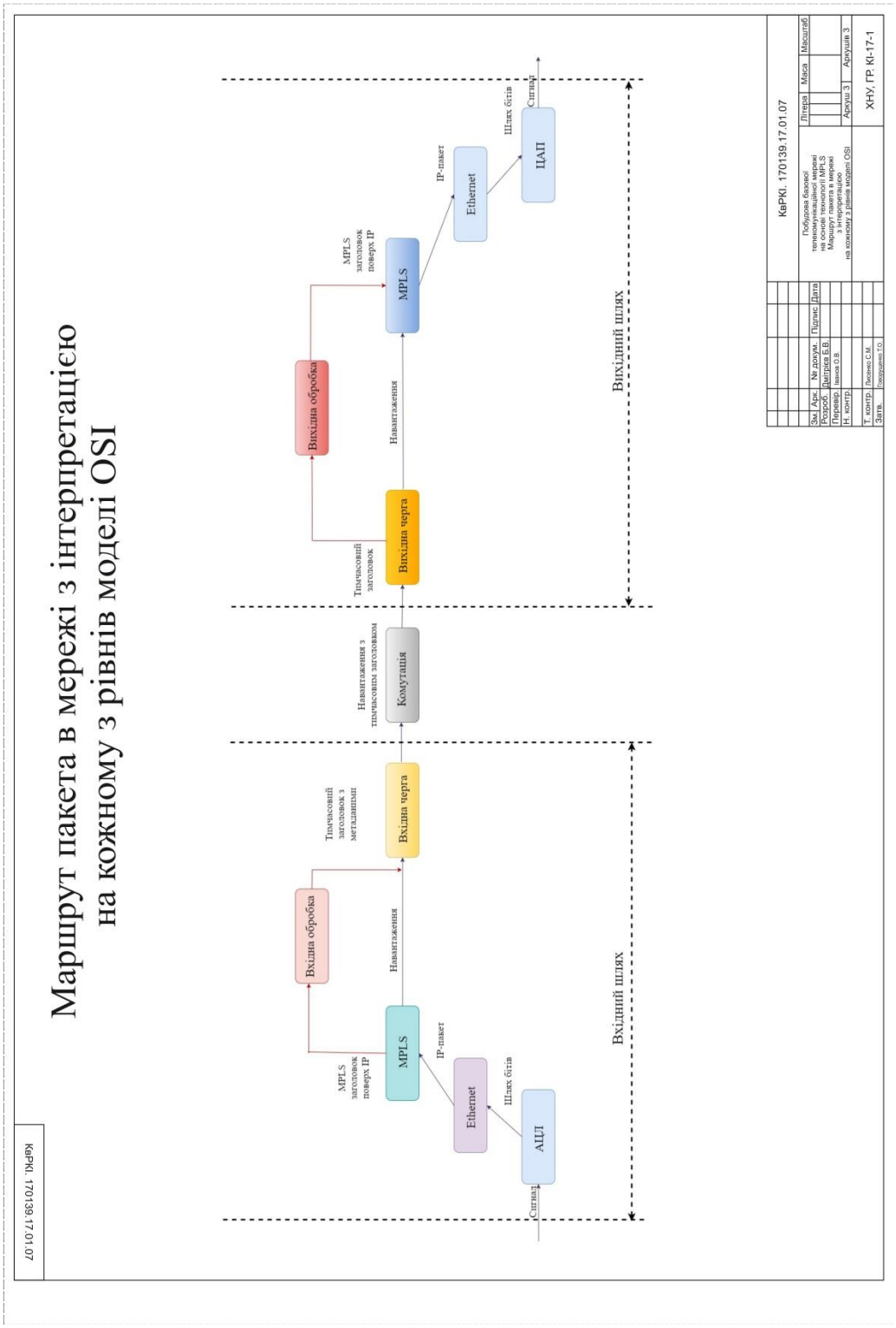
Копія схеми «Фізична топологія мережі з віртуальним рівнем»



ДОДАТОК Г

(обов’язковий)

Копія схеми «Маршрут пакета в мережі з інтерпретацією на кожному з рівнів модель OSI»



UNICHECK

Ім'я користувача:
Кафедра КІ

ID перевірки:
1008308701

Дата перевірки:
16.06.2021 09:14:59 EEST

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
16.06.2021 09:15:34 EEST

ID користувача:
100005591

Назва документа: **Дмітрієв_Побудова базової телекомунікаційної мережі на основі технології MPLS**

Кількість сторінок: **64** Кількість слів: **11529** Кількість символів: **83897** Розмір файлу: **3.50 MB** ID файлу: **1008376605**

1.41% Схожість

Найбільша схожість: **0.93%** з джерелом з Бібліотеки (ID файлу: **1008248421**)

0.93% Джерела з Інтернету	7	Сторінка 66
1.41% Джерела з бібліотеки	47	Сторінка 66

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0% Вилучень

Немає вилучених джерел

Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Замінені символи	6

Anti-Plagiarism v-15.257

Максимальное совпадение с одним документом 0.0%

Словари проверки: en_US, ru_RU, ua_UA. **Ошибок в документах: 11%**

ID: 94120 Название: Побудова базової телекомунікаційної мережі на основі технології MPLS Добавлено в БД: 2021-06-16 Авторы: Дмітрієв Б.В. Руководители: Іванов О.В. Консультанты: Оппоненты:	Документ		Суммарное совпадение по Базе Данных	
	Символы	Лексемы	Символы	Лексемы
	73311	706	307 (0%)	4 (1%)

Источник плагиата

ID	Описание	Наличие плагиата в документе	
		Символы	Лексемы

Завідувачу кафедри КІСП
д-ру техн.наук, проф. Говорущенко Т. О.

Дмітрієв Б.В.

ПІБ здобувача вищої освіти

ФПКТС, 4 курсу, групи КІ-17-1

ЗАЯВА

З правилами чинного Положення «Про дотримання академічної доброчесності в Хмельницькому національному університеті» від 26.09.2020 (зі змінами від 26.11.2020), згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений (а). Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на наявність плагіату ознайомлений(а) та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-технічних засобів (Unicheck та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

17 червня 2021

дата

підпис

РІШЕННЯ ЕКСПЕРТНОЇ КОМІСІЇ

КАФЕДРИ КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА СИСТЕМНОГО ПРОГРАМУВАННЯ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: Побудова базової телекомунікаційної мережі на основі технології MPLS

Автор: Дмітрієв Богдан Васильович

Спеціальність: 123 – Компютерна інженерія

Освітня програма: освітньо-професійна

Науковий керівник: Іванов Олексій Валентинович, к.т.н, доцент

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом. Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	

Підтвердження:

Запозичення, виявлені в роботі, є законними і не є плагіатом, оскільки:

1) запозичення розміщені в розділах аналізу існуючих аналогів та прототипів, які не описують безпосередньо авторське дослідження і не стосуються результатів роботи;
2) усі запозичення фрагментарні, або мають належним чином оформленні посилання;
3) всі зафіксовані системою ознаки модифікації тексту відносяться до комбінування латинських символів зі україномовними скороченнями індексів в певних списках, що не є модифікацією тексту.

Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ ідентичності/схожості, складає 1,41% і адресується до 7 першоджерела, що, з урахуванням наведених обґрунтувань, відповідає характеру наукового дослідження і свідчить на користь кваліфікаційної роботи.

Керівник роботи _____ О. В. Іванов

Гарант ОП _____ С. М. Лисенко

Завідувач кафедри КІСП _____ Т. О. Говорущенко