КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
БУДІВНИЦТВА І АРХІТЕКТУРИ

автоматизації і інформаційних технологій
(факультет)

інформаційних технологій проєктування та прикладної математики
(кафедра)

ПОЯСНЮВАЛЬНА ЗАПИСКА
ДО КВАЛІФІКАЦІЙНОЇ РОБОТИ
НА ЗДОБУТТЯ ОСВІТНЬОГО РІВНЯ «БАКАЛАВР»

на тему: «Побудова віртуальної приватної мережі з використанням технології MPLS»

БАШИНСЬКИЙ ВЛАДИСЛАВ ЄВГЕНОВИЧ
(прізвище, ім’я та по батькові студента повністю)

Київ 2026 р.

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
БУДІВНИЦТВА І АРХІТЕКТУРИ

автоматизації і інформаційних технологій

(факультет)

інформаційних технологій проєктування та прикладної математики

(кафедра)

ЗАТВЕРДЖУЮ
Завідувач кафедри ІТППМ
д.т.н., професор Бородавка Є.В.

_____
«___» _____2026 року

ПОЯСНЮВАЛЬНА ЗАПИСКА
ДО КВАЛІФІКАЦІЙНОЇ РОБОТИ
НА ЗДОБУТТЯ ОСВІТНЬОГО РІВНЯ «БАКАЛАВР»

на тему: «Побудова віртуальної приватної мережі
з використанням технології MPLS»

Виконав: студент 4-го курсу, групи ІСТ-22

Спеціальності: 126 «Інформаційні системи та технології»
(шифр і назва спеціальності)

Башинський В.Є.
(прізвище та ініціали)

Керівник доктор філософії Волох Б.Ю.
(прізвище та ініціали)

Рецензент доктор філософії Рябчун Ю.В.
(прізвище та ініціали)

Київ 2026 р.

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
БУДІВНИЦТВА І АРХІТЕКТУРИ

Факультет: автоматизації і інформаційних технологій

Кафедра: інформаційних технологій проєктування та ПМ

Освітній рівень: «бакалавр» за ОПП

Спеціальність: 126 «Інформаційні системи та технології»

Освітня програма: «Інформаційні системи та технології»

ЗАТВЕРДЖУЮ

Завідувач кафедри ІТППМ

д.т.н., професор Бородавка Є.В.

_____

«___» _____2026 року

З А В Д А Н Н Я
ДО ВИКОНАННЯ КВАЛІФІКАЦІЙНОЇ РОБОТИ
НА ЗДОБУТТЯ ОСВІТНЬОГО РІВНЯ «БАКАЛАВР»
Башинський Владислав Євгенович

1.Тема роботи: «Побудова віртуальної приватної мережі з використанням технології MPLS»,
затверджена наказом ректора КНУБА № 444/52-15/13.6/26 від “08” квітня 2026 року

2. Керівник роботи: Волох Богдан Юрійович, доктор філософії, старший викладач кафедри ІТППМ

3. Строк подання студентом роботи до захисту: червень 2026 року

4. Зміст пояснювальної записки за розділами:

Р.1. Аналіз сучасних методів та принципів побудови мереж VPN

Р.2. Дослідження технології MPLS L3 VPN

Р.3. Побудова віртуальної приватної мережі на базі MPLS

5. Інформаційні слайди:

С.1. Титульний слайд

С.2. Актуальність теми

С.3. Мета роботи, об’єкт та предмет досліджень

С.4. Загальна характеристика мереж VPN

С.5. VPN-мережі зі встановленням з'єднання

С.6. VPN-мережі без встановлення з'єднання

С.7. MPLS L3 VPN

С.8. Порівняння технологій VPN

С.9. Технологія MPLS в моделі OSI

С.10. Комутація пакетів по міткам

С.11. Комплекси VRF

С.12. Пересилання IP-пакетів по мережі провайдера

С.13. Етапи конфігурування

С.14. Модель організації мережі MPLS L3 VPN

С.15. Трасування маршруту для VPN_A

С.16. Дослідження маршруту VPN_A

С.17. Трасування маршруту для VPN_B

С.18. Дослідження мережі провайдера

С.19. Висновки

6. Календарний план виконання кваліфікаційної роботи

Види робіт та їх зміст	Дата виконання
Р.1. Аналіз сучасних методів та принципів побудови мереж VPN.	Лютий 2026 р.
Р.2. Дослідження технології MPLS L3 VPN.	Лютий 2026 р.
Р.3. Побудова віртуальної приватної мережі на базі MPLS.	Березень 2026 р.
Висновок	Квітень 2026 р.
Остаточне оформлення роботи	Травень 2026 р.
Попередній захист роботи на кафедрі	Червень 2026 р.

7. Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали та посада консультанта, представника комісії	Дата	Підпис
Прийом програмного продукту	Доктор філософії, доцент Рябчун Ю.В.		

8. Дата видачі завдання: 12 січня 2026 року

Керівник _____ Волох Б.Ю.
(підпис) (прізвище та ініціали)

Бакалавр _____ Башинський В.Є.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

«Побудова віртуальної приватної мережі з використанням технології MPLS».

Кваліфікаційна робота бакалавра за спеціальністю: 126 «Інформаційні системи та технології», освітня програма: «Інформаційні системи та технології». – Київський національний університет будівництва та архітектури. – Київ, 2026.

Робота присвячена побудові віртуальних приватних мереж на базі технології MPLS. Було проаналізовано сучасні методи організації корпоративних віртуальних приватних мереж, визначено їх переваги та недоліки і обрано найкраще рішення. На основі отриманих даних було спроектовано і налаштовано модель мережі провайдера на базі технології MPLS з підтримкою двох віртуальних приватних мереж..

Ключові слова: віртуальна приватна мережа, багатопротокольна комутація по міткам, мітка, динамічна маршрутизація.

SUMMARY

"Building virtual private networks based on MPLS technology"

Bachelor's qualification work in the specialty: 126 "Information systems and technologies", educational program: "Information systems and technologies". - Kyiv National University of Construction and Architecture. - Kyiv, 2026.

The work is devoted to the construction of virtual private networks based on MPLS technology. Modern methods of organizing corporate virtual private networks were analyzed, their advantages and disadvantages were identified, and the best solution was selected. Based on the obtained data, a provider network model based on MPLS technology with support for two virtual private networks was designed and configured.

Keywords: virtual private network, multi-protocol switching on labels, label, virtual routing and forwarding, dynamic routing.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

VPN – (Virtual Private Network) – віртуальна приватна мережа.

MPLS – (Multiprotocol Label Switching) – багатопротокольна комутація по міткам.

IP – (Internet Protocol) – міжмережевий протокол.

QoS – (Quality of Service) – якість обслуговування.

BGP – (Border Gateway Protocol) – протокол граничного шлюзу.

MP-BGP – (Multiprotocol Border Gateway Protocol) – багатопротокольний протокол граничного шлюзу.

IGP – (Interior Gateway Protocols) – клас протоколів динамічної маршрутизації, що функціонують в межах однієї AS.

AS – (Autonomous System) – автономна система.

FR – (Frame Relay) – технологія передачі даних методом ретрансляція кадрів.

ATM – (Asynchronous Transfer Mode) – мережева технологія комутації і мультиплексування пакетів.

L2 VPN – Layer 2 VPN.

L3 VPN – Layer 3 VPN.

IPSec – (IP Security) – протокол захисту даних , що передається через IP.

GRE – (Generic Routing Encapsulation) – протокол тунелювання мережевих пакетів.

TCP – (Transmission Control Protocol) – протокол керування передачею даних.

CE – (Customer Enge Router) – граничний маршрутизатор клієнта.

PE – (Provider Enge Router) – граничний маршрутизатор мережі провайдера.

OSPF – (Open Shortest Path First) – протокол динамічної маршрутизації.

IS-IS – (Intermediate System-to-Intermediate System protocol) – протокол динамічної маршрутизації.

VRF – (Virtual Routing and Forwarding) – технологія, що дозволяє реалізовувати на базі одного фізичного маршрутизатора мати декілька віртуальних.

CEF – (Cisco Express Forwarding) – технологія високошвидкісної маршрутизації.

LSR – (Label switching router) — комутуюхий мітки маршрутизатор.

LSP – (Label Switch Path) – тунель, шлях в MPLS.

LDP – (Label Distribution Protocol) – протокол розподілу міток.

ЗМІСТ

ВСТУП

При розробці сучасних магістральних мереж найбільших операторів необхідно вирішувати ряд задач, складність і характер яких залежить від вимог до функціонального призначення мережі. Основна маса вимог, що постійно оновлюються і які висуваються до технологій магістральних мереж операторів зв'язку, надходять від постійно зростаючого попиту клієнтів на додаткові послуги. При розробці сучасних магістральних мереж, що відповідають таким вимогам, обираються такі технології і стандарти, які дозволяють в кінцевому результаті отримати мережу, що відповідає вимогам і характеристикам мультисервісної мережі. Мультисервісна мережа – це мережа, яка утворює єдину інформаційно-телекомунікаційну структуру, яка підтримує всі види трафіку (дані, голос, відео) і надає всі види послуг (традиційні і нові, базові і додаткові) в будь-якій точці, в будь-який час, в будь-якому наборі і об'ємі, з диференційованою гарантованою якістю і за вартістю, що буде задовольняти різноманітні категорії користувачів [1].

Однією із найбільш важливих послуг, що надаються інтернет провайдерами, є послуга організації віртуальних приватних мереж (VPN) корпоративних користувачів. Характерною властивістю більшості корпоративних мереж на сьогодні є їх територіально розподілена структура, в результаті чого, виникає задача об'єднання територіально розподілених філіалів і комп'ютерів віддалених користувачів в одну мережу.

Спочатку, ці задачі вирішувалися шляхом організації власної приватної мережі, шляхом прокладання виділених каналів зв'язку, встановлення маршрутизаторів і пристроїв доступу. Переваги приватних мереж беззаперечні, адже вони надають широкі можливості по вибору мережевої технології, і також гарантують високий рівень надійності. Але якщо дивитися на це з економічної точки зору, то стає зрозуміло, що таке задоволення є дуже дорогим. Тому переваги організації VPN через загальнодоступну мережу Internet є беззаперечними.

Стосовно технології магістральної мережі, то для вирішення виникаючих задач розроблялося безліч архітектур, але в наш час найбільш розповсюдженою є архітектура MPLS, яка забезпечує побудову магістральних мереж, що мають майже необмежені можливості масштабування, підвищену швидкість обробки трафіка і безпрецедентну гнучкість з точки зору організації додаткових сервісів.

Провайдери, що пропонують своїм клієнтам IP-послуги по магістралям MPLS можуть підтримувати якість обслуговування (QoS), що дозволяє адміністраторам контролювати такі параметри передачі трафіку, як затримка і втрати пакетів в мережі [4]. Однією із основних переваг є можливість підтримувати різні типи трафіку, такі як дані, голос і відео. Це дозволяє підписувати із замовниками угоди про гарантовану якість послуг.

Враховуючи вищесказане, можна говорити про те, що досить популярна на сьогодні технологія VPN MPLS, без сумніву ще буде затребуваною і в майбутньому. Тому проектування та побудова сучасних мереж MPLS L3 VPN на сьогодні є актуальним завданням.

Об’єкт дослідження - основи побудови віртуальних приватних мереж.

Предмет дослідження – методи та принципи побудови віртуальних приватних мереж 3-го рівня на базі технології MPLS.

Метою даної роботи є побудова віртуальної приватної мережі на базі технології багатопротокольної комутації по міткам в магістральній мережі провайдера. Для досягнення поставленої мети необхідно вирішити наступні завдання:

- аналіз сучасних методів та принципів побудови мереж VPN;
- аналіз принципів функціонування технології MPLS;
- дослідження і оцінка технології VPN L3 MPLS;
- побудова і оцінка моделі мережі MPLS L3 VPN з допомогою мережевого симулятора GNS3;

1. АНАЛІЗ СУЧАСНИХ МЕТОДІВ ТА ПРИНЦИПІВ ПОБУДОВИ МЕРЕЖ VPN

1.1 Загальна характеристика VPN-мереж

VPN (англ. *Virtual Private Network* – віртуальна приватна мережа) – логічна мережа, що будується поверх незахищених мереж, як наприклад Інтернет. Незважаючи на те, що комунікації здійснюються по публічним мережам з використанням протоколів, що не дають гарантій безпеки, за рахунок шифрування в мережах VPN створюються закриті канали обміну інформації, які приховані від небажаних користувачів. VPN дозволяє об'єднати, наприклад, декілька офісів організації в єдину мережу (рисунок 1.1) з використанням для зв'язку між ними непідконтрольних каналів [2].

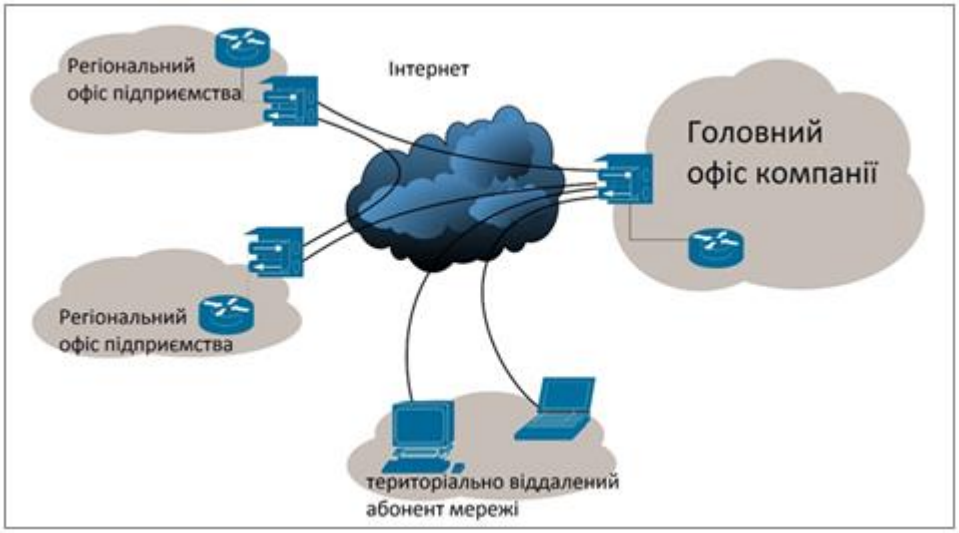

Рисунок 1.1 - Структура мережі VPN

Термін «віртуальна приватна мережа» (VPN) використовується операторами зв'язку і провайдерами служб для позначення сукупності віртуальних каналів закритих груп користувачів з моменту розробки і початку використання служб X.25, Frame Relay і ATM. Пізніше цей термін почав використовуватися при управлінні промисловими мережами (Enterprise Network Management) для позначення закритих груп користувачів в IP-мережах.

VPN-мережі на базі протоколу IP вже давно стали основою доставки голосу, відео і звичайних цифрових даних. Використання функцій VPN в

протоколі IP дозволяє встановити в мережах, на основі програмного забезпечення Cisco IOS, магістральні служби розширюваних VPN-мереж 3-го рівня з використанням протоколу IPv4. VPN-мережі протоколу IP являються базою, що використовується компаніями для розміщення і адміністрування додаткових служб, включаючи розміщення і зберігання даних, електронну торгівлю тощо [5].

Віртуальні приватні мережі можуть гарантувати, що направлений через Інтернет трафік, так само захищений, як і при передачі всередині локальної мережі, при збереженні всіх фінансових переваг, які можна отримати, використовуючи Інтернет.

Високий рівень безпеки в мережах VPN досягається за рахунок того, що для передачі трафіку через публічну мережу застосовуються механізми тунелювання і шифрування. Окрім цього безпека ще й гарантується за рахунок використання спеціальних пристроїв і механізмів захисту. Наприклад, щоб отримати доступ до мережі організації, користувач проходить через брандмауер (залежить від методу реалізації), де йому необхідно виконати автентифікацію і авторизацію. Таким чином VPN гарантує, що віддалений доступ до мережі та її ресурсів зможуть отримати лише довірені особи.

Загалом під терміном VPN розуміють коло технологій, що забезпечують безпечний і якісний зв’язок в межах контрольованої групи користувачів по відкритій глобальній мережі. Мета створення VPN зводиться до максимального ступеня відокремлення потоків даних одного підприємства від потоків даних інших користувачів мережі. Таке розмежування має бути забезпечене по відношенню параметрів пропускної здатності потоків, а також по відношенню конфіденційності даних що передаються.

З огляду на все більш зростаючий інтерес до даної технології, уже сьогодні більшість провайдерів надають послуги з організації віртуальних приватних мереж поверх своїх транспортних мереж. На рисунку 1.2 продемонстрована функціональна модель етапів дослідження і проектування мереж VPN.

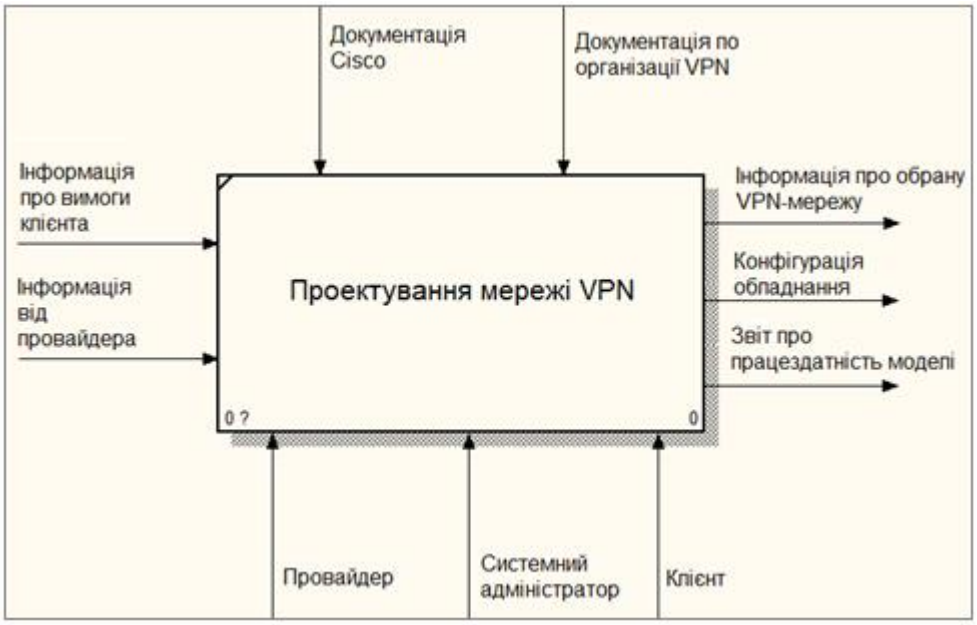

Рисунок 1.2 - IDEF0 модель проектування мережі VPN

На рисунку 1.3 представлена декомпозиція першого рівня, щоб розгорнуто уявити процес дослідження і етапи розробки топології мережі.

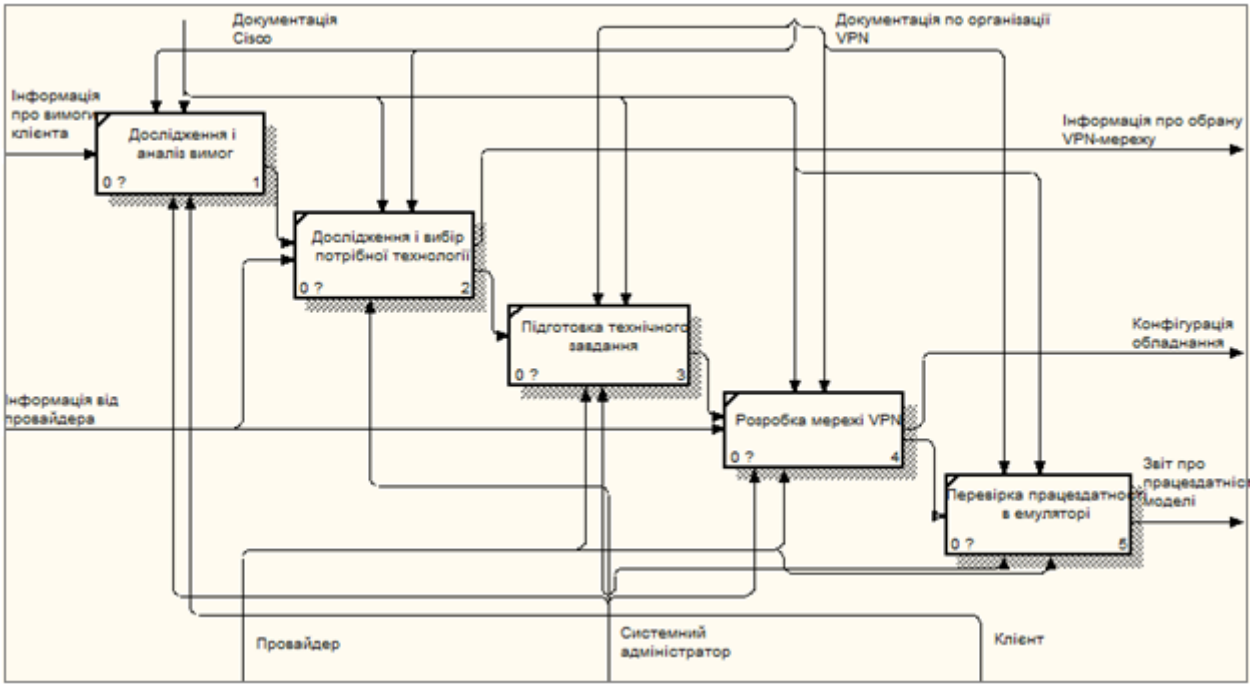

Рисунок 1.3 - DFD модель проектування мережі VPN

Із діаграм видно, як відбувається процес дослідження і проектування мережі VPN під кожен конкретний випадок (в залежності від вимог клієнта).

1.2 Класифікація мереж VPN

Загалом VPN можна класифікувати за різними базовими параметрами. Наприклад, за ступенем захищеності використовуваного середовища розрізняються захищені та довірчі VPN. Захищені віртуальні приватні мережі є найбільш затребуваними, адже вони дозволяють створити надійну і захищену мережу на основі незахищеної. Довірчі рішення VPN навпаки орієнтовані на те, що середовище передачі даних вважається захищеним, тому залишається лише вирішити задачу створення віртуальної підмережі в рамках великої мережі[3].

Також мережі VPN можна класифікувати за такими ознаками як: принцип структурної побудови, основні методи реалізації, за призначенням (Intranet/Extranet VPN). Розглянемо ці ознаки більш детально.

Принцип структурної побудови мереж VPN

Всього існує два типи можливих VPN-з'єднання: Remote access і Site-to-Site. Remote access VPN означає, що з'єднання організовується між додатками на комп'ютері клієнта і будь-яким пристроєм, який виступає в якості сервера і організовує підключення від різних клієнтів (наприклад маршрутизатор, Cisco ASA). Коли створюється VPN-з'єднання, клієнт може отримати доступ до ресурсів організації пройшовши авторизацію. Даний спосіб з'єднання продемонстровано на рисунку 1.4.

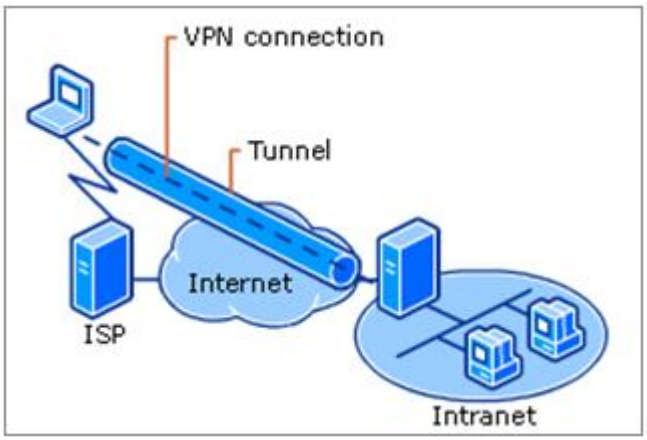

Рисунок 1.4 - Remote access VPN

Інший варіант - Site-to-site VPN, що передбачає наявність двох пристроїв (наприклад маршрутизаторів), між якими створюється постійне з'єднання. В такому випадку, користувачі знаходяться за пристроями в локальних мережах і на їх комп'ютерах не потрібно встановлювати спеціальне програмне забезпечення. Коли мережі підключені через Інтернет, як показано на рисунку 1.5, маршрутизатор перенаправляє пакет іншому маршрутизатору через VPN-з'єднання. Для маршрутизаторів VPN-з'єднання працює як лінк рівня каналу передачі даних.

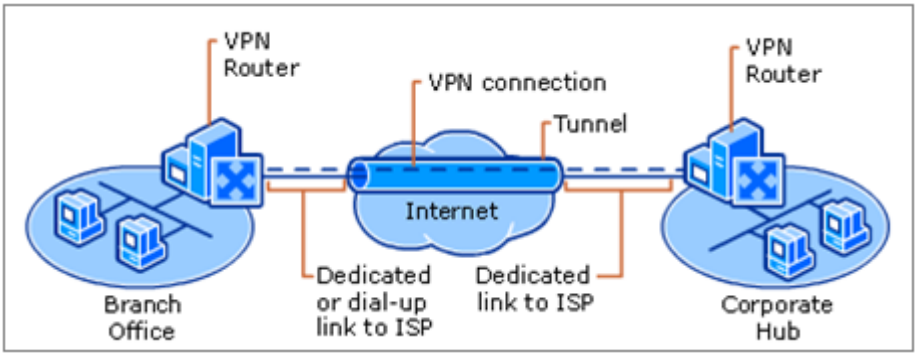

Рисунок 1.5 - Site-to-site VPN

Intranet/Extranet VPN

Всі мережі VPN умовно можна розділити на два основні види:

- внутрішньокорпоративні мережі VPN (Intranet VPN);
- міжкорпоративні мережі VPN (Extranet VPN);

Внутрішньокорпоративні мережі VPN (Intranet VPN) будуються з використанням публічної мережі Internet або роздільних мережевих інфраструктур, що надаються сервіс-провайдерами (рисунок 1.6). Компанії достатньо відмовитися від використання дорогих виділених ліній, щоб замінити їх біль дешевим зв'язком через Інтернет. Це значно зменшує затрати на використання полоси пропускання, оскільки в мережі Інтернет відстань ніяк не впливає на вартість з'єднання.

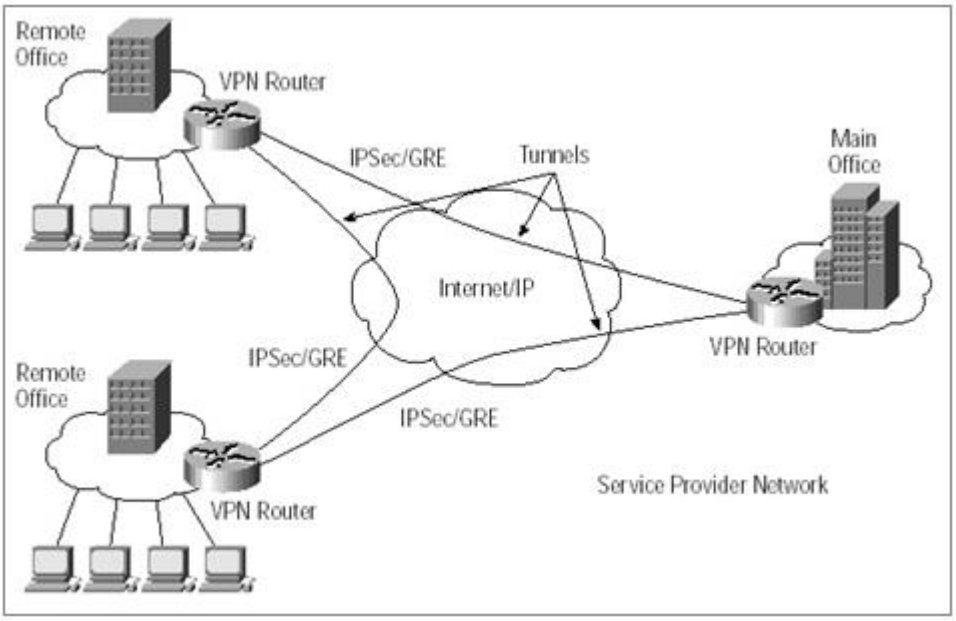

Рисунок 1.6 - Intranet VPN

Серед основних переваг Intranet VPN можна виділити наступні:

- для забезпечення конфіденційності інформації використовуються криптографічні протоколи шифрування;
- надійність функціонування при виконанні критичних додатків (наприклад САП і СКБД);
- хороша гнучкість, що є важливим параметром в умовах стрімко зростаючої кількості нових користувачів, філіалів, програмних додатків;

Побудова Intranet VPN на основі публічної мережі Інтернет є найбільш рентабельним способом реалізації VPN-технології. Але варто зауважити, що в мережі Інтернет не гарантуються рівні сервісу. Тому компанії, яким необхідні гарантовані рівні сервісу, повинні розглянути можливість розгортання своїх VPN з використанням роздільних мережевих інфраструктур, що надаються сервіс-провайдерами.

В мережах Intranet також можливий варіант реалізації мережі Localnet VPN. Така мережа забезпечує захист інформаційних потоків, що циркулюють в локальній мережі підприємства (зазвичай це Центральний офіс), від несанкціонованого доступу з боку співробітників цього підприємства.

Міжкорпоративна мережа VPN (Extranet VPN) являє собою мережеву технологію, яка забезпечує прямий доступ із мережі однієї компанії до мережі іншої (рисунок 1.7) і, таким чином, сприяє підвищенню надійності зв'язку, що підтримується в ході ділової співпраці.

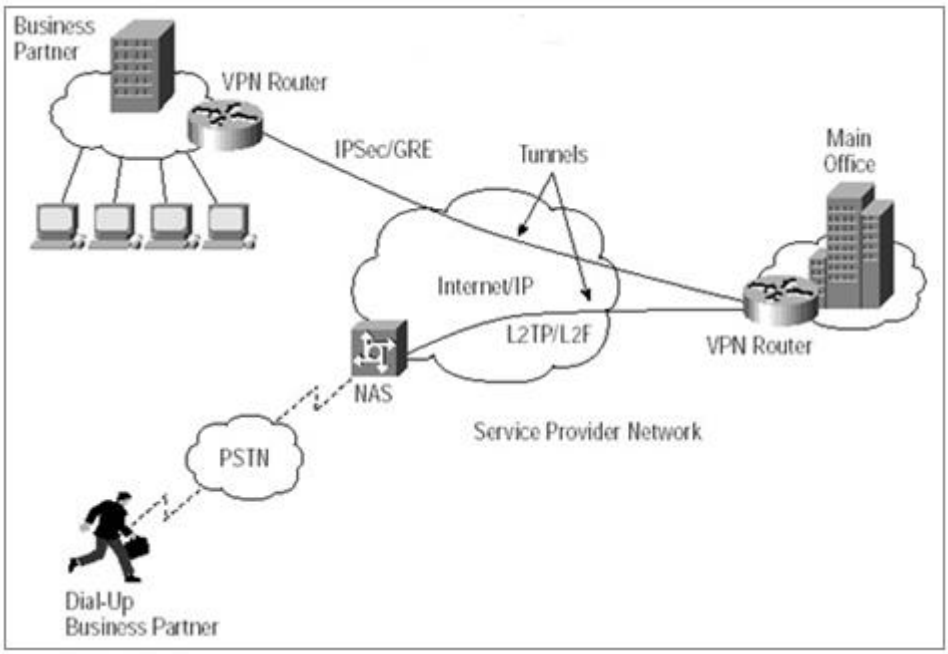

Рисунок 1.7 - Extranet VPN

Мережі Extranet VPN за принципом організації загалом схожі на Intranet VPN. Єдина відмінність полягає у тому, що проблема захисту інформації у міжкорпоративних VPN стоїть більш гостро. Звідси випливає характерна особливість таких мереж – обмеження можливості віддалених клієнтів або бізнес-партнерів по використанню ресурсів корпоративної мережі. Фактично вони будуть обмежені доступом лише до тих ресурсів компанії, які необхідні при роботі зі своїми клієнтами, наприклад, сайт з комерційними пропозиціями [4].

Методи реалізації VPN-мереж

До основних методів реалізації віртуальних приватних мереж можна віднести VPN на основі брандмауерів, VPN на основі маршрутизаторів та VPN на основі програмного забезпечення.

VPN на основі брандмауерів. При побудові VPN на базі брандмауера мережевий екран є VPN-агентом (рисунок 1.8), який забезпечує фільтрацію

вхідного і вихідного мережевого трафіку і виконує функцію тунелювання. Перевагою такого метода є економічність, а захист даних забезпечується шляхом використання надійних алгоритмів шифрування. До недоліків можна віднести залежність продуктивності від апаратного забезпечення.

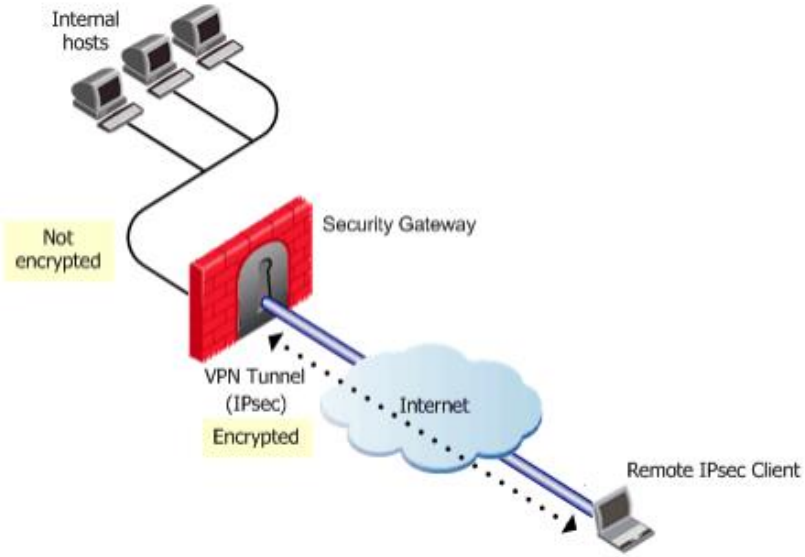

Рисунок 1.8 - VPN на основі брандмауерів

VPN на базі брандмауера будуються на мережевому рівні OSI. Засоби захисту є прозорими для додатків і прикладних протоколів. Фільтрація мережевого трафіка виконується на основі правил, що базуються на аналізі заголовка мережевого пакета. Брандмауер пропускає або відкидає пакети на основі аналізу таких даних із заголовка пакета, як тип протоколу, IP-адреса відправника, номер порту. При цьому доцільно використовувати строгу політику брандмауера: заборонити доступ для пакета, якщо він явно не дозволений. В такому випадку з'єднання з віддаленим користувачем буде встановлено лише в тому випадку, якщо IP-адреса в заголовку отриманого пакета буде співпадати з адресою дозволеного списку. В іншому випадку, пакет буде відкинуто. Недоліком автентифікації на основі адреси відправника є те, що вона не захищає від підміни адреси зловмисником.

Як приклад VPN на базі брандмауерів можна назвати FireWall-1 компанії Check Point Software Technologies. FireWall-1 використовує для побудови VPN стандартний підхід на базі IPSec. Трафік, що приходить в брандмауер,

дешифрується, після чого до нього застосовуються стандартні правила управління доступом.

VPN на основі маршрутизаторів. Маршрутизатор пропускає через себе всі пакети, якими локальна мережа обмінюється із зовнішнім світом (рисунок 1.9). Це робить маршрутизатор платформою для шифрування вихідних пакетів і розшифрування зашифрованих вхідних пакетів. Тобто маршрутизатор може поєднувати в собі основні операції по маршрутизації з підтримкою функцій VPN.

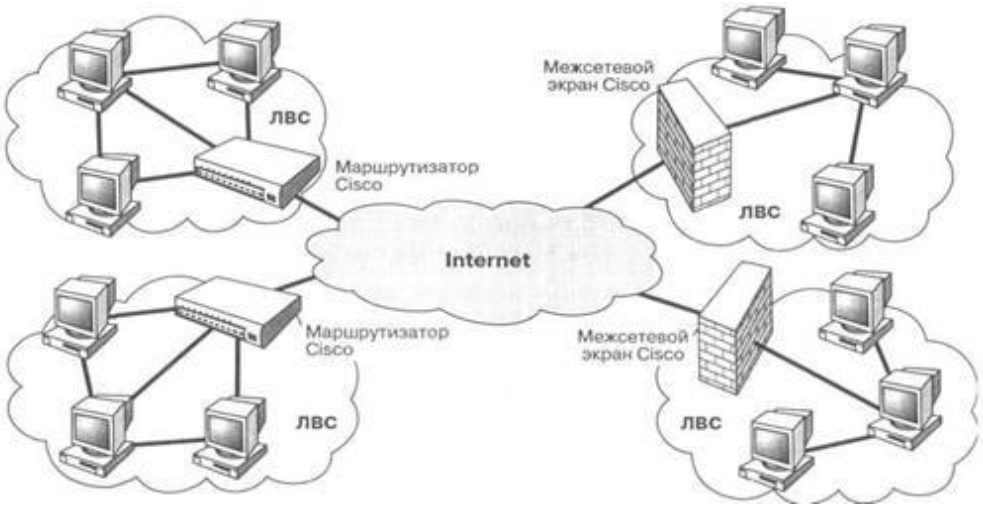

Рисунок 1.9 - VPN на основі маршрутизаторів

Таке рішення має свої переваги та недоліки. Переваги полягають в зручності сумісного адміністрування функцій маршрутизації і VPN. Застосування маршрутизаторів для підтримки VPN особливо корисне в тих випадках, коли підприємство не використовує міжмережевого екрана і організовує захист корпоративної мережі лише з допомогою маршрутизатора, що поєднує функції захисту як по доступу в мережу, так і по шифруванню трафіку, що передається. Недоліки даного рішення пов’язані з підвищеними вимогами до продуктивності маршрутизатора, який повинен поєднувати основні операції по маршрутизації з трудомісткими операціями шифрування і автентифікації трафіка.

Проблема отримання підвищеної продуктивності маршрутизатора зазвичай вирішується з допомогою апаратної підтримки функцій шифрування.

Сьогодні майже всі провідні виробники маршрутизаторів та іншого мережевого обладнання заявляють про підтримку в свої продуктах різних VPN-протоколів.

Характерним прикладом технічних засобів для створення такого VPN є пристрої компанії Cisco Systems. Починаючи з версії програмного забезпечення IOS 11.3(3)T в маршрутизаторах Cisco реалізовано підтримку протоколів IPSec і L2TP, а також гарантуються підтримка таких функцій VPN, як обмін ключами і ідентифікацію при організації тунельного з'єднання. Для збільшення ефективності маршрутизатора можливий також варіант із застосуванням допоміжного модуля криптографічного шифрування ESA (Encryption Service Adapter).

VPN на основі програмного забезпечення. Для побудови VPN широко використовуються спеціалізовані програмні засоби. Програмні засоби побудови VPN дозволяють формувати захищені тунелі суто програмним способом і перетворюють комп'ютер, на якому вони функціонують, в маршрутизатор TCP/IP, який отримує зашифровані пакети, розшифровує їх і пересилає по локальному середовищі далі, до кінцевої точки призначення. У вигляді спеціального програмного забезпечення можуть бути виконані VPN-шлюзи, VPN-сервери і VPN-клієнти.

VPN-продукти, реалізовані програмним способом, з точки зору продуктивності поступаються спеціалізованим апаратним пристроям. У той же час програмні продукти легко забезпечують продуктивність, необхідну для віддаленого доступу. Безсумнівною перевагою програмних продуктів є гнучкість і зручність у застосуванні, а також відносно невелика вартість.

VPN на основі спеціалізованих апаратних засобів. VPN-мережі, побудовані на основі спеціалізованих апаратних засобів характеризуються досить високою продуктивністю. Це пов'язано з тим, що об'єм необхідних обчислень для обробки пакету VPN майже в 50 разів перевищує той об'єм, який потрібно виконати для обробки звичайного пакета. З урахуванням цього, висока продуктивність VPN-систем на базі апаратних засобів досягається за

рахунок використання спеціалізованих мікросхем, розроблених спеціально для процесів шифрування.

Такі VPN-засоби зазвичай сумісні з протоколом IPsec і застосовуються для формування крипто-захищених тунелів між локальними мережами. Яскравим представником таких апаратних засобів є VPN-шлюз (рис. 1.10).

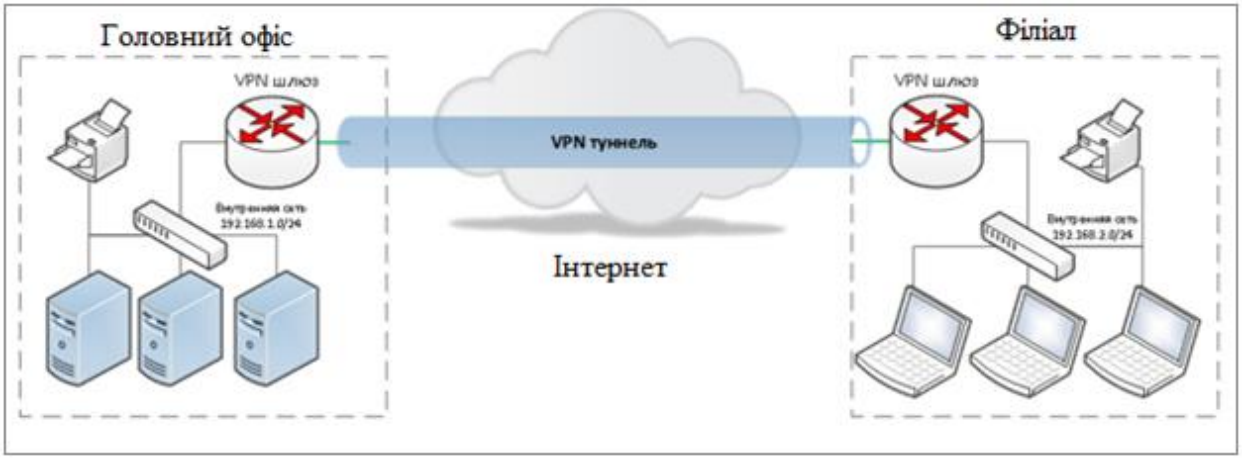

Рисунок 1.10 - VPN на основі VPN-шлюзів

1.3 Основні складові VPN-мереж

Тунелювання являє собою процес передачі конфіденційних даних, призначених лише для використання в приватній мережі, через загальнодоступну мережу. Іншими словами, тунелювання - це процес створення логічного з'єднання між двома кінцевими точками шляхом інкапсуляції різних протоколів. В даному процесі інкапсуляції пакети даних виглядають так, ніби вони є загальнодоступними для публічної мережі, коли насправді вони розглядаються як приватні пакети даних. Це дозволяє їм проходити мережею непомітно.

В процесі тунелювання дані будуть розбиватися на фрагменти, відомі як пакети, які будуть переміщатися по тунелю для транспортування до кінцевого пункту призначення. Коли ці пакети проходять через тунель, вони шифруються і інкапсулюються (рисунок 1.11). На стороні приймача буде відбуватися процес деінкапсуляції і дешифрування.

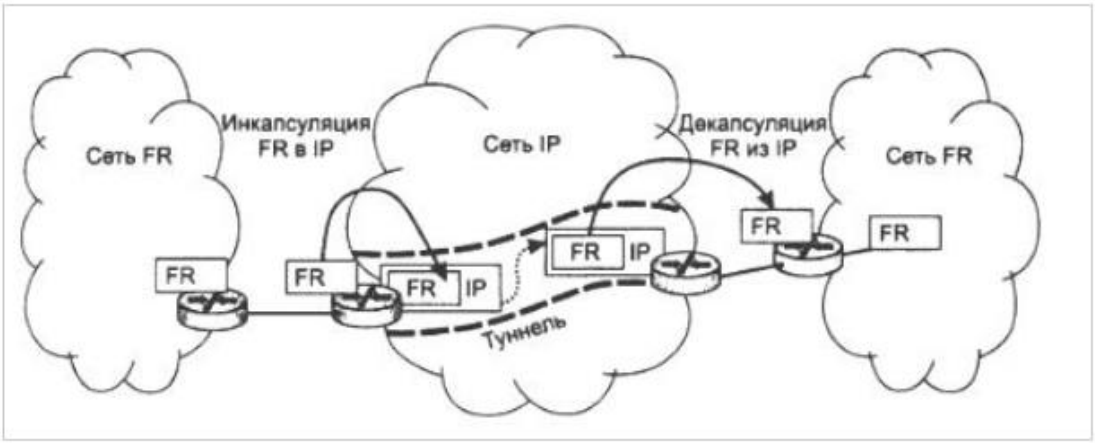

Рисунок 1.11 - Тунелювання трафіка Frame Relay через IP-мережу

В процесі інкапсуляції приймають участь три типи протоколів: той що транспортується, той що транспортує і протокол інкапсуляції. Пакети протоколу, що транспортується, поміщаються в поле даних пакетів несучого протоколу з допомогою протоколу інкапсуляції (рисунок 1.12). Така процедура передачі призводить до того, що пакети "пасажири" не обробляються маршрутизаторами при транспортуванні по транзитній мережі. Інкапсуляція виконується маршрутизатором або шлюзом, які знаходяться між вихідною і транзитною мережами. Деінкапсуляція виконується іншим граничним пристроєм, який розташовується між транзитною мережею і мережею призначення.

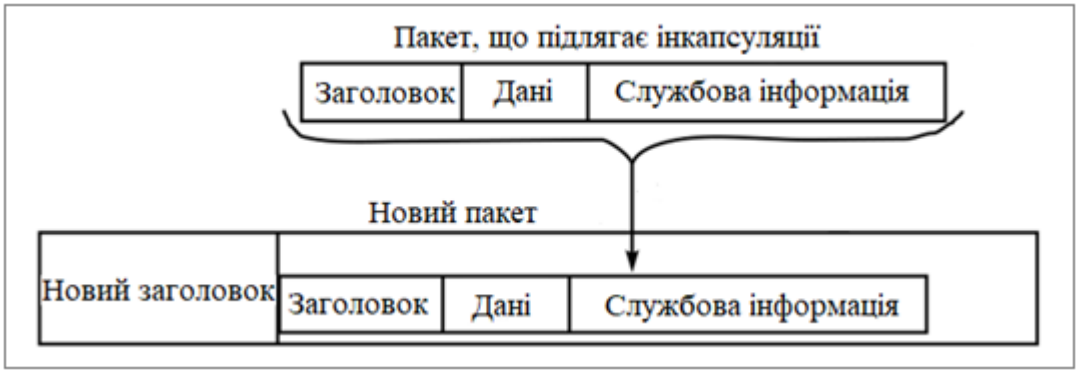

Рисунок 1.12 - Процес інкапсуляції

Особливістю процесу тунелювання є те, що граничні пристрої в заголовках несучих пакетів вказують лише адреси своїх інтерфейсів в полях

«source» і «destination», а адреси вузлів мережі призначення в заголовках "пасажира" є зашифрованими аж до процесу деінкапсуляції.

Використання тунелів для передачі інформації між віддаленими офісами є досить корисною річчю, але проблема полягає в тому, що сам по собі тунель не гарантує захисту передаваємої інформації, а виступає лише методом транспортування. Це досить серйозна проблема з урахуванням того, що така інформація може становити корпоративну таємницю (як приклад, фінансові звіти або ж особисті дані клієнтів чи співробітників). Не менш тривожним є і той факт, що зловмисник легко може модифікувати дані, що передаються через тунель і тоді отримувач вже ніяк не зможе перевірити їх достовірність. З огляду на це, виникає необхідність у виконанні процесів автентифікації і шифрування.

На сьогоднішній день, така необхідність легко вирішуються сучасними засобами криптографічного захисту інформації. Проблема модифікації легко вирішується шляхом використання методу електронного цифрового підпису (ЕЦП). Даний метод базується на асиметричному шифруванні з відкритим ключем. До пакетів даних, що необхідно передати, додається додатковий блок інформації, який і є ЕЦП пакета. Він дозволяє виконати автентифікацію даних одержувачем, якому відомий ЕЦП відправника. Сама інформація захищається шляхом використання надійних методів шифрування. Найпопулярнішими на даний момент є протоколи шифрування AES, 3DES і протокол IKEv2 (який використовується в IPsec).

1.4 VPN-мережі зі встановленням з’єднання

VPN-мережі зі встановленням з’єднань можуть бути створені на базі інфраструктури 2-го і 3-го рівня. Прикладами таких VPN-мереж 2-го рівня можуть слугувати канали зі встановленням з’єднання типу «точка-точка», такі як віртуальні з’єднання Frame Relay і ATM.

Прикладом VPN-мереж зі встановленням з’єднання 3-го рівня можуть слугувати структури VPN, створені з використанням повнозв’язної або

частково-зв’язної топології тунлів на базі протоколів IPsec (шифрування для забезпечення конфіденційності) або з використанням технології загальної інкапсуляції маршрутизації (Generic Routing Encapsulation – GRE).

VPN-мережі доступу до служби використовують механізм встановлення з’єднання з комутацією каналів, що забезпечує тимчасове безпечне з’єднання віддаленого доступу між індивідуальним користувачем і внутрішньою або зовнішньою корпоративною мережею (intraner і extranet) через сувмісно використовувану мережу провайдера служби з тією ж стратегією передачі даних, як і в приватній мережі. Такі мереді використовують віддалений доступ до точки присутності провайдера ISP з подальшою передачею даних по відкритій мережі Internet з кінцевим доступом до внутрішньої корпоративної мережі.

Головною проблемою в VPN-мережах зі встановленим з’єднанням є складність розширення мережі. Зокрема, ефективність VPN-мереж зі встановленням з’єднання без повнозв’язної топології далека від оптимальної. Крім того, у випадку VPN-мереж 3-го рівня при передачі через мережу Internet неможливо напевне гарантувати якість обслуговування (Quality of Service – QoS) при передачі даних по такій структурі.

Використання VPN-мереж на базі віртуальних каналів вимагає від провайдера служби створення окремих віртуальних каналів і керування ними або створення логічних маршрутів і керування ними для кожної пари вузлів, що входять в групу користувачів і здійснюють обмін даними. Така вимога еквівалентна побудові повнозв’язної топології віртуальних каналів, що буде включати всіх користувачів.

VPN-мережі 2-го рівня зі встановленням з’єднання є основою VPN-моделі передачі інформації одного рівня в середовищі іншого. У цій моделі провайдер служби надає віртуальні канали, а обмін маршрутною інформацією відбувається безпосередньо між маршрутизаторами користувача (CPE - Customer Premises Equipment).

VPN-мережі 3-го рівня, в яких використовується процедура встановлення з'єднання, є основою тунельної моделі VPN. При використанні технолгій GRE або IP Security (IPsec) створюється тунельна модель з'єднань типу «точка-точка» через внутрішню мережу IP або через відкриту мережу Internet, в той час як віртуальні приватні канали віддаленого доступу (Virtual Private Dialup Network – VPDN) являють собою гібридну комбінацію віддаленого доступу і безпечного тунельного з'єднання через середовище Internet до точки концентрації трафіку підприємства, такої як корпоративний шлюз.

Тунельні VPN-мережі протокола загальної інкапсуляції маршрутизації (GRE) можуть бути використані для створення IP-з'єднань типу «точка-точка». Комбінація таких GRE-тунелів може бути використана для побудови VPN-мережі. Таким чином реалізовується оверлейна модель VPN.

Як показано на рисунку 1.13, використання GRE-тунелів доцільне для побудови VPN-мереж в приватній магістральній IP-мережі провайдера. Вони також корисні для передачі по тунельним з'єднанням потоків даних 3-го рівня, що відрізняються від IP.

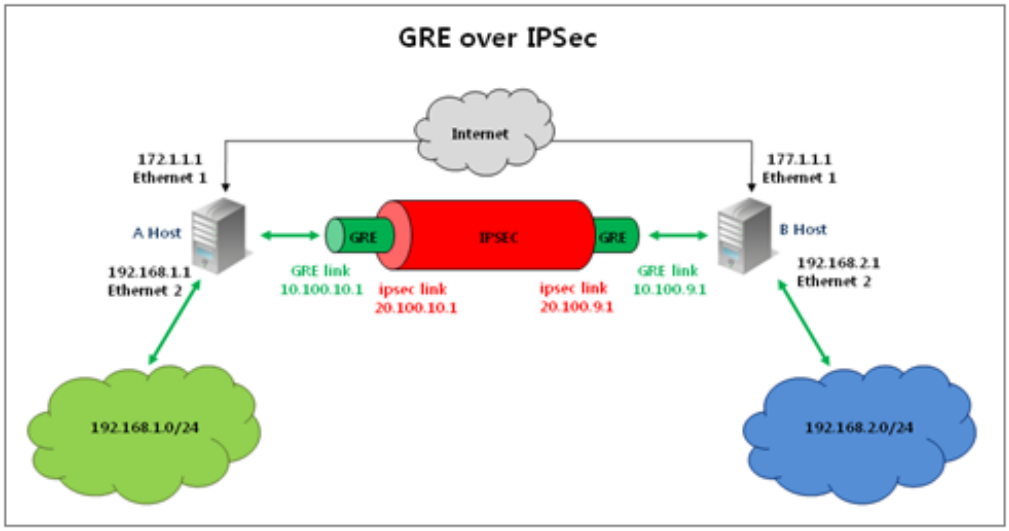

Рисунок 1.13 – Тунельні VPN-мережі протоколів GRE і IPSec

VPN-мережі протокола IPsec з тунельними з'єднаннями являють собою технологію високого ступеня безпеки, що використовує шифрування і

механізм створення тунельних з’єднань, які захищають вміст пакетів при проходженні по IP-мережі. Протокол IPSec, як правило, використовується при передачі даних через відкриті недостатньо безпечні IP-мережі. Більша частина структури IPSec реалізується на CPE-обладнанні користувача, а провайдери, як правило, надають VPN-служби керованого протоколу IPSec.

Проте дана модель VPN має також і ряд недоліків. Зокрема, щоб досягти оптимальної маршрутизації в корпоративній мережі, побудованої поверх магістралі провайдера, така мережа повинна мати структуру типу вузол (рисунок 1.14).

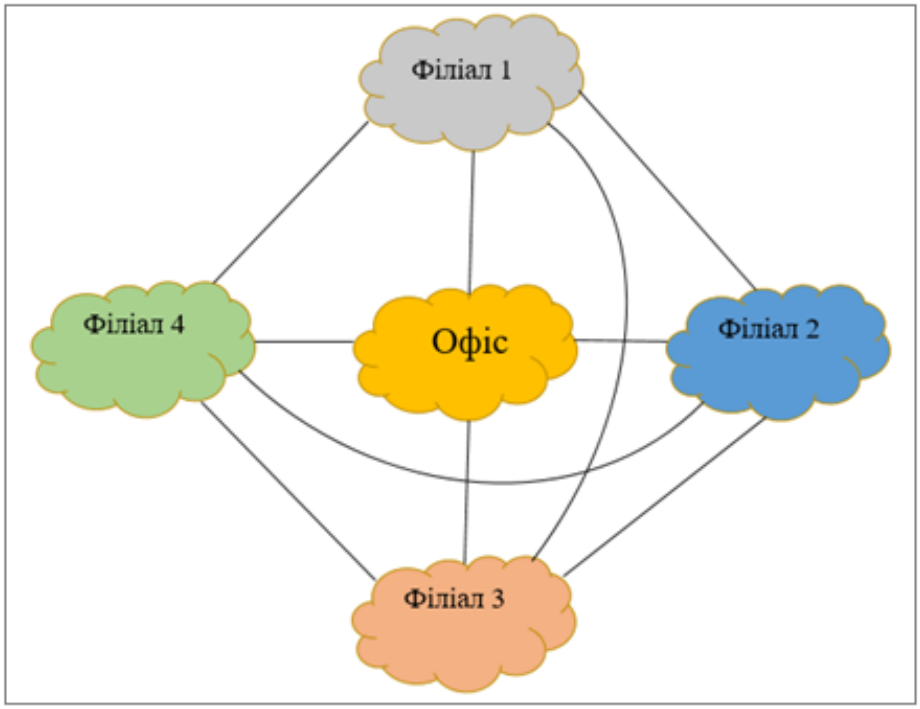

Рисунок 1.14 - Вузлова топологія

Це означає, що в кожному відділені компанії потрібно встановлювати маршрутизатор, що буде з’єднаний з маршрутизаторами в інших відділеннях. Якщо не дотримуватися даної топології, то трафік буде передаватися від одного корпортативного маршрутизатора в магістраль провайдера, потім він буде надходити по магістралі до корпоративного центрального маршрутизатора і вже потім знову через магістраль проайдера потрапить до місця призначення. З іншого ж боку, дотримання повнозв’язної технології значно обмежує можливості компанії до розширення, адже поява нових

відділень передбачає під’єднання до мережі нових маршрутизаторів, що рано чи пізно призведе до перенавантаження мережі.

1.5 VPN-мережі без встановлення з'єднання

VPN-мережі без встановлення з’єднання при встановленні зв’язку між кінцевими точками не потребують наявності раніше заданого логічного або віртуального каналу між ними.

Мережі 3-го рівня без встановлення з’єднання являють собою базу одноранговоі моделі. В такій моделі обмін маршрутною інформацією відбувається між маршрутизаторами CE і маршрутизаторами провайдера.

До VPN-мереж без встановлення з’єднання відносяться звичайні VPN-мережі протокола IP. Провайдери надають користувачам керовані служби IP (managed IP services), що дає їм можливість під’єднувати свої IP-маршрутизатори CE до приватних IP-магістралей провайдера. Типовий приклад VPN-мережі IP показано на рисунку 1.15.

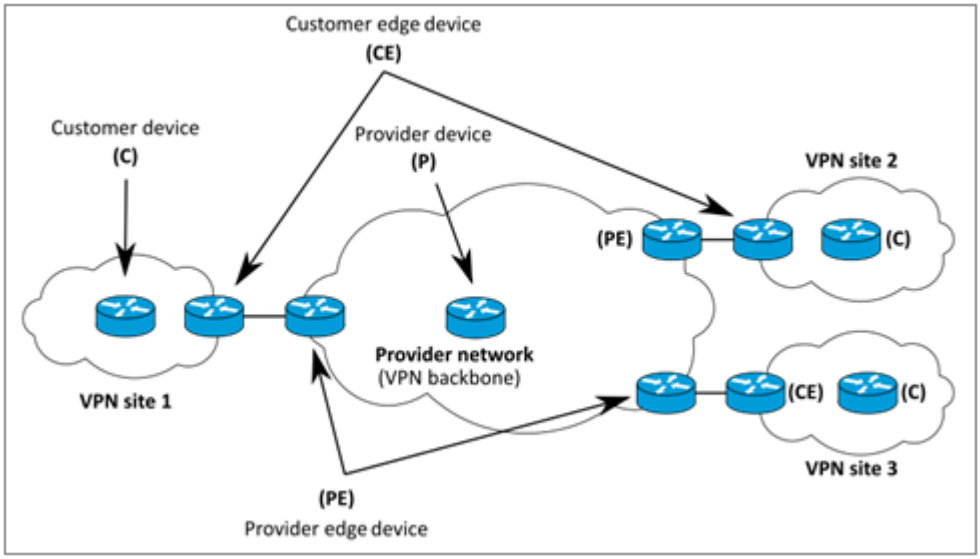

Рисунок 1.15 – Типова VPN-мережа IP

Зазвичай провайдери для різних користувачів конфігурують на своїх магістральних маршрутизаторах декілька протоколів маршрутизації або декілька процесів маршрутизації. Як правило, пристрій маршрутизації Cisco підтримує на окремих маршрутизаторах декілька протоколів маршрутизації

для під’єднання мереж, які використовують різні протоколи. В протоколи маршрутизації ще при створенні закладався принцип незалежного функціонування від інших аналогічних протоколів. Кожен протокол збирає і аналізує необхідну йому інформацію і реагує на зміни топології індивідуально. Наприклад, вже застарівший протокол RIP використовує в якості метрики кількість транзитних переходів, а протокол EIGRP – вектор метричної інформації, що кладається з п’яти елементів.

Користувачі отримують доступ до VPN-мереж IP через комбінацію списків доступу, протоколів маршрутизації і процесів. Головними проблемами, що постають перед провайдерами керованих послуг IP, є розширюваність і складність реалізації. Велика кількість доступних протоколів і процесів маршрутизації, що підтримуються платформами маршрутизаторів, іноді примушує провайдерів розташовувати в точці присутності окремі маршрутизатори для кожної VPN-мережі.

До основних переваг однорангової моделі VPN можна віднести те, що кількість робіт, які має виконати сервіс-провайдер для технічного забезпеченян і керування VPN, прямо пропорціне кількості сайтів замовника, підключених до VPN. В оверлейній моделі об’єм такої роботи пропорційниї квадрату сайтів замовника, підключених до VPN.

Однорангова модель підтримує оптимальну маршрутизацію користувацього трафіку по магістралі сервіс-провайдера, так як в даній моделі немає потреби в транзитних CE-пристроях. Корпоративному замовнику не потрібно керувати власною магістралью. Йому потрібно лише підключити CE-маршрутизатор на кожному сайті. Таким чином, однорангова модель вигідна і сервіс-провайдеру, і замовнику. Адже для провайдера вона означає зменшення об’єму робіт, а для корпоративного замовника – менше проблем з організацією VPN.

1.5.1 VPN на основі MPLS

Щоб економічно виділити технічні ресурси, необхідні для підтримки мереж IP VPN з великою різноманітністю різних функцій, сервіс провайдерам необхідні засоби, здатні розпізнавати різні типи додатків, щоб провайдер міг гарантувати певну якість послуг (QoS) і забезпечити безпеку даних, причому робити це потрібно в мережах, які будуть менш складними, ніж IP-тунелі і вузлові мережі з віртуальними каналами. Як уже говорилося раніше, рішення VPN, побудовані поверх IP, вимагають тунелювання і шифрування (що значно впливає на процес обробки пакетів). Крім того, оскільки IP-трафік передається по віртуальним каналам, мережа VPN не знає, який тип трафіку передається нею. До того є, такі мережі більш зосереджено на з'єднання і тому вони погано піддаються масштабуванню. Щоб відповідати сучасним вимогам клієнтів, мережа на основі технології VPN має розпізнавати, до якого типу додатків відноситься трафік: голос, відео-потоки, електронна пошта, звичайні дані. Вона має вміти швидко відділяти трафік одного додатку від іншого[6].

Технологія MPLS дозволяє пересилати дані з допомогою міток, які прикріплюються до кожного пакету. Внутрішнім вузлам ядра мережі, що підтримують MPLS, більше не потрібно аналізувати вміст кожного пакету. Зокрема, не розглядаються IP-адреса отримувача, що дає можливість MPLS надати ефективний механізм інкапсуляції для приватного трафіка, що передається магістралями сервіс-провайдера.

MPLS може розмежовувати трафік і забезпечувати його захист без шифрування і тунелювання. Технологія MPLS підтримує безпеку в кожній окремій мережі, точно так само, як мережі Frame Relay і ATM підтримували її для кожного окремого з'єднання. Якщо традиційна мережа VPN надає базові послуги мережевого транспорту, то мережа з технологією MPLS – це масштабовані послуги VPN, які допускають підтримку IP-додатків з додатковою цінністю поверх базової транспортної мережі VPN [7, 8].

1.6 Порівняння технологій VPN

В таблиці 1.1 виконано порівняння технологій L3 VPN на основі вимог безпеки, масштабованості, фінансових можливостей, складності реалізації та якості обслуговування.

Таблиця 1.1

Порівняння існуючих рішень технології L3 VPN

Критерій	Вимога	L3 VPN GRE over IPsec	MPLS L3 VPN
Складність реалізації	Для швидкого створення нових служб, підвищення рівня безпеки, якості обслуговування і підтримки угод про рівні обслуговування необхідно мати удосконалені системи моніторингу і аналізу потоків даних	Середня	Середня
Рівень безпеки	Мають надаватися різні рівні безпеки, включаючи використання тунелів, шифрування, розподіл потоків, автентифікація.	Високий	Середній
Масштабованість структури	Повинна дозволяти розширювати служби VPN малих та середніх підприємств до мереж	Середня	Висока

	крупних промислових користувачів		
Якість обслуговування	Має надаватися можливість визначати пріоритети критично важливим або чутливим до затримки додаткам	Не підтримує QoS	Висока
Вартість реалізації	Прямі і непрямі витрати на встановлення VPN	Середня	Низька

Проведений вище аналіз демонструє, що MPLS L3 VPN має деякі переваги над іншими реалізаціями і фактично не має недоліків. Тому дане рішення є найкращим для організації великих корпоративних VPN через мережу провайдера.

1.7 Висновки до першого розділу

VPN (Virtual Private Network) — це віртуальна приватна мережа або логічна мережа, яка створюється поверх незахищених мереж. Класифікувати віртуальні мережі можна за багатьма різними ознаками: за принципами структурної побудови, за методом реалізації, за способом організації.

У даному розділі було надано загальну характеристику VPN-мереж, розглянуто принципи їх побудови, основні складові, а також основні методи реалізації. Зокрема, особливу увагу було приділено технологіям L2 та L3 VPN, визначено їх особливості функціонування, переваги та недоліки. Технологія MPLS є ідеальним рішенням для організації VPN-мереж, які реалізовуються сервіс-провайдером, адже вони надають ряд важливих і дуже корисних послуг, які значно впливають на працездатність мережі (наприклад, надання послуг QoS).

Проведений аналіз можливих технологій VPN в таблиці 1.1 показав, що найкращим варіантом реалізації віртуальних приватних мереж є

провайдерський MPLS L3 VPN, який має ряд переваг у порівнянні зі звичайними L2 і L3 VPN. Зокрема це забезпечення швидкості і якості передачі даних, забезпечення їх конфіденційності, гарна масштабованість структури, відносна дешевизна.

2. ДОСЛІДЖЕННЯ ТЕХНОЛОГІЇ MPLS L3 VPN

2.1 Базові поняття технології MPLS

MPLS - це технологія швидкої комутації пакетів в багатопротокольних мережах, заснована на використанні міток. Концепція MPLS поєднує в собі управління трафіком, характерне для технологій канального рівня, масштабованість і гнучкість протоколів мережевого рівня. «Багатопротокольна» в назві технології означає, що що технологія MPLS застосовна до будь-якого протоколу мережного рівня, тобто MPLS – це свого роду інкапсулюючий протокол, здатний транспонувати інформацію множині інших протоколів вищих рівнів моделі OSI (рисунок 2.1). Таким чином, технологія MPLS залишається незалежною від протоколів рівнів 2 і 3 в мережах IP, ATM і Frame Relay, а також взаємодіє з існуючими протоколами маршрутизації, такими як протокол резервування ресурсів RSVP або мережний протокол вибору найкоротших маршрутів OSPF [8, 11].

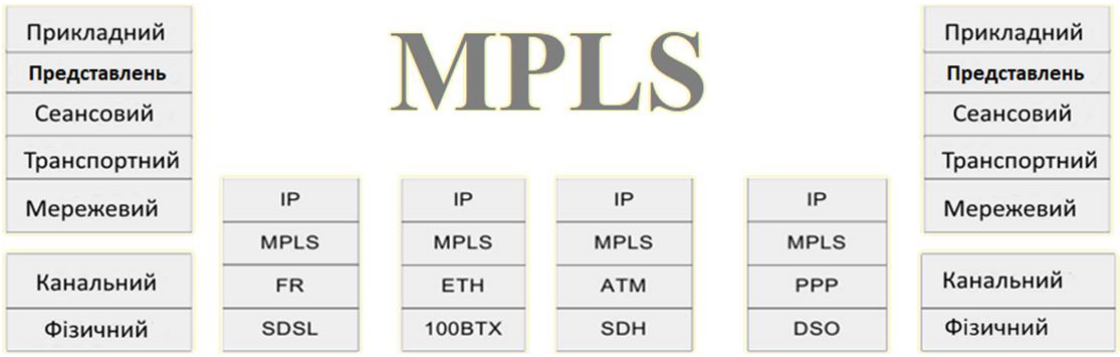

Рисунок 2.1 - Технологія MPLS в моделі OSI

Фізичний рівень містить функції, що забезпечують використання фізичного середовища для двосторонньої передачі бітів (з такою достовірністю, яку забезпечує це середовище) по прямому тракту, що зв'язує два вузла мережі. Другий рівень (канальний рівень) містить функції, що забезпечують формування в цьому тракті надійної логічної ланки зв'язку, за яким відбувається двосторонній обмін інформаційними блоками між вузлами. На даному рівні виявляються і виправляються помилки, гарантується достовірність передачі. Третій рівень (мережевий рівень) містить функції, які

забезпечують транспортування інформаційних блоків від відправника до одержувача через кілька вузлів мережі по невластивому маршруту транспортування, який складається з ланок другого рівня.

Представлена модель на рисунку 2.1 показує, що протокол MPLS не утворює повноцінного рівня, а «вклинюється» в мережі IP, ATM, Frame Relay, Ethernet між канальним і мережевим рівнями моделі OSI, залишаючись незалежним від цих рівнів. Можна сказати, що одночасне функціонування MPLS на мережевому рівні і на канальному рівні призводить до утворення так званого рівня 2.5, де і виконується комутація по мітках [9].

Мережі ряду Інтернет-провайдерів побудовані сьогодні на основі багаторівневої моделі, припускає, що логічна маршрутизована IP-мережа функціонує поверх комутованої топології другого рівня (ATM, або Frame Relay) і незалежно від неї. Комутатори другого рівня забезпечують високошвидкісні з'єднання, в той час як IP-маршрутизатори на периферії мережі, пов'язані один з одним мережею віртуальних каналів другого рівня, здійснюють інтелектуальне пересилання IP-пакетів.

Таким чином, MPLS - це один з кроків на шляху еволюційного розвитку мережі Інтернет в бік спрощення її інфраструктури, шляхом інтеграції функцій другого (комутація) та третього (маршрутизація) рівнів. MPLS - універсальна технологія. З її допомогою можна вирішувати такі завдання:

- інтеграція ATM, Frame Relay, Ethernet з IP;
- прискорене просування пакетів всередині мережі оператора уздовж традиційних найкоротших маршрутів;
- створення віртуальних приватних мереж (VPN);
- вибір і встановлення шляхів з керуванням трафіку (Traffic Engineering, TE).

У даний час досить активно розвивається стандарт GMPLS (Generalized MultiProtocol Label Switching), призначений для вибору і встановлення оптичних шляхів в мережах SDH і WDM.

У мережах MPLS використовуються два види мережевих вузлів. Розташовані на кордоні мережі MPLS маршрутизатори повинні розпізнавати і аналізувати IP-потоки що надходять і направляти їх за відповідними маршрутами. Такі пристрої називаються прикордонними маршрутизаторами з комутацією по мітках (Label Edge Router, LER). Граничні маршрутизатори в ряді випадків включають в себе шлюзи інтерфейсів мереж різних видів (наприклад, Frame Relay, ATM або Ethernet) і пересилають їх трафік в MPLS-мережу після організації трактів LSP, а також розподіляють трафік зворотного напрямку при виході його з MPLS-мережі. Розрізняють вхідний і вихідний LER [7,12].

Вхідний LER аналізує IP-заголовок як і звичайний маршрутизатор і встановлює до якого FEC при виборі адреси наступної передачі пакета він належить. Такому FEC присвоюється мітка, яка передається разом з пакетом до транзитного маршрутизатора.

IP-дейтаграмма полягає в модуль даних протоколу (Protocol Data Unit, PDU) технології MPLS, а заголовок MPLS прикріплюється до дейтаграми. Якщо заголовок об'єднаний з операцією QoS (наприклад, DiffServ), то вхідний LER розглядатиме трафік відповідно до правил DiffServ. Далі LER приймає рішення про вибір шляху для даного пакета, посилаючи його до відповідного транзитному маршрутизатора з комутацією по мітках (Label Switch Routers, LSR).

Транзитний LSR отримує PDU і використовує заголовок MPLS для прийняття рішень пересилання. Він також робить заміну міток. Даний LSR не займається обробкою заголовка третього рівня (IP-заголовка), а приймає рішення про пересилку на основі мітки пакета, а не на основі таблиці маршрутизації і пересилає пакет далі.

Далі, проходячи зазвичай через кілька транзитних LSR, пакет потрапляє до вихідного LER, який виробляє операцію розбирання PDU, видаляє з пакету мітку, аналізує заголовок пакету і направляє його до адресата, що знаходиться зовні MPLS - мережі (рисунок 2.2).

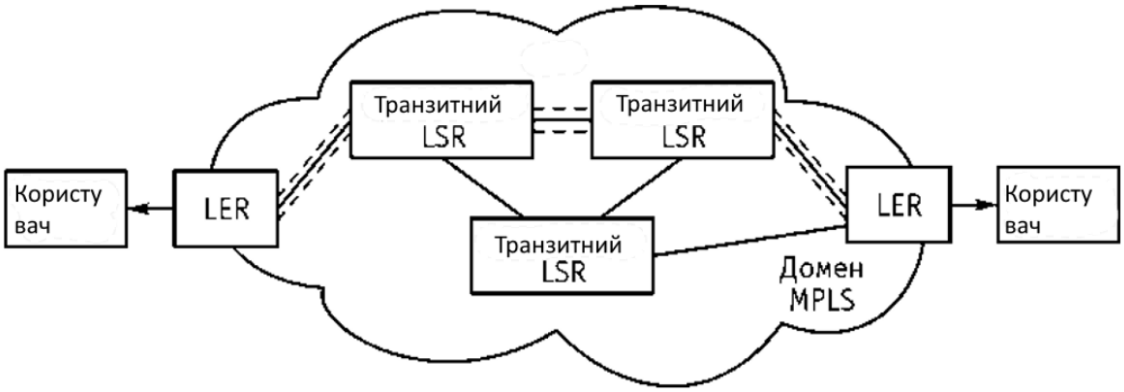

Рисунок 2.2 - Елементи мережі MPLS

Для більш детального прикладу розглянемо рисунок 2.3. Маршрутизатори R1 і R6 виступають в ролі периферійних пристроїв домену MPLS (LER). Маршрутизатори R2, R3, R4 і R5 виступають в якості LSR.

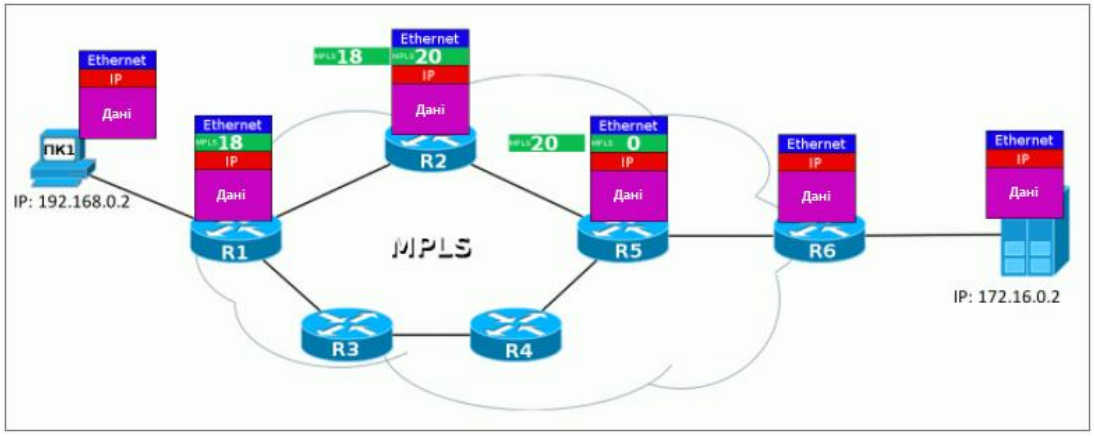

Рисунок 2.3 – Комутація пакета по міткам

Принцип комутації по міткам матиме наступний вигляд:

1. PC1 – звичайний комп’ютер – відправляє звичайний пакет на віддалений сервер.
2. Пакет приходить на маршрутизатор R1, який згідно з таблицею FIB присвоює даному пакету мітку 18. Вона вставляється між заголовком IP і Ethernet.
3. R2 отримує цей пакет, аналізуючи заголовок Ethernet визначає, що це MPLS-пакет (Ethertype 8847), зчитує мітку і звертається до своєї таблиці міток. Згідно з даною таблицею він визначає, на яку мітку потрібно замінити вже наявну і на який інтерфейс необхідно відправити пакет.

4. R5 виконує аналогічні дії – визначає яку нову мітку необхідно помістити в пакет і на який інтерфейс його необхідно відправити.
5. R6 отримує пакет MPLS, згідно зі своєю таблицею міток він визначає, що мітку необхідно зняти. Після процесу видалення мітки пакет аналізується стандартними методами і маршрутизується до місця призначення.

Головна особливість технології MPLS – відділення процесу комутації пакету від аналізу IP-адреса в його заголовку, що дозволяє здійснювати комутацію пакетів значно швидше. Відповідно до протоколу MPLS маршрутизатори привласнюють кожній точці входу в таблицю маршрутизації особливу мітку і повідомляють цю мітку сусіднім пристроям. Наявність таких міток дозволяє маршрутизаторам і комутаторам, що підтримують технологію MPLS, визначати наступний крок в маршруті пакету без виконання процедури пошуку адреси. На сьогоднішній день існують три основні сфери застосування MPLS:

- управління трафіком;
- підтримка класів обслуговування (CoS);
- організація віртуальних приватних мереж (VPN).

2.1.1 Мітки MPLS

Міткою називають короткий елемент, який має фіксовану довжину, і застосовується для локального ідентифікації класу еквівалентності пересилання FEC. На рисунку 2.3 зображено структуру мітки. Вона має такі параметри: 4 байта (32 біта) - довжина, 20 біт - заголовок, 12 біт - підзаголовок.

Рисунок 2.4 – Структура MPLS мітки

Заголовок мітки складається з наступних складових:

1) **Label** – мітка - використовується для вибору відповідного маршруту комутації по мітках. Довжина 20 біта.
2) **TC** – Traffic Class – несе в собі пріоритет пакета. Довжина 3 біта.
3) **S** – Bottom of Stack – індикатор дна стека міток довжиною в 1 біт. Заголовків MPLS на пакеті може бути декілька, наприклад зовнішня мітка для комутації в мережі MPLS і внутрішня, яка буде вказувати на певний VPN. Щоб LSR розумів свої подальші дії відносно отриманого пакета, в біт S записується «1», якщо це остання мітка і «0» якщо стек міток має більше однієї мітки. Тобто LSR не може визначити кількість міток в стекі, проте він може визначити остання вона, чи їх більше. Цього цілком достатньо, адже будь-які рішення приймаються лише на основі самої верхньої мітки, незалежно від того, що там під нею.
4) **TTL** – Time To Live – аналог IP TTL. Довжина – 8 біт. Основна задача – не допускати «блукання» пакета мережею у випадку виникнення петлі. При передачі IP-пакета через мережу MPLS значення IP TTL може бути скопійовано в MPLS TTL, а потім навпаки.

З мітками проводять три типи операцій:

1. **Label push** (додавання мітки) як правило проводиться маршрутизатором за допомогою вхідного LER. Мітка, яка буде визначена, і вихідний інтерфейс, через який буде передаватися пакет, визначаються на базі таблиці IP-маршрутизації для вхідного IP-пакета.
2. **Label swap** (комутація по мітці) здійснюється за підтримкою маршрутизатора LSR. Проходячи обробку на основі таблиці міток, вхідні пакети з мітками, здійснюють передачу пакета зі зміною мітки через поставлений інтерфейс. При цьому ймовірне приєднання інших міток до стеку.
3. **Label pop** (зняття мітки) здійснюється вихідним LER маршрутизатором або тим, який був попереднім йому LSR маршрутизатором. На базі

таблиці маршрутизації, якби мітка була останньою в стеку, то пакет даних пересилається вже крайньому одержувачу без міток.

Пакет, що має вигляд стеку дозволяє мати більше однієї мітки, що дає альтернативу створювати відповідність міток. На рисунку 2.4 показано, як виглядає дворівневий стек MPLS-міток.

Рисунок 2.5 – Дворівневий стек міток MPLS

Можливість об'єднання кількох LSP стає можливим завдяки функціям стека MPLS. Створюється агрегований тракт MPLS в результаті додавання зверху мітки до стеку кожного шляху в технології. В місці, де закінчується цей тракт, він роз'єднується на частини його індивідуальних тунелів. Також тракти, що мають спільну складову маршруту, можуть об'єднуватися. Це означає, що MPLS має здатність забезпечувати ієрархічну відправку даних. А це є найважливішою і затребуваною функціональною можливістю. Якщо її застосувати, то глобальну маршрутну інформацію не має сенсу переносити. В результаті мережа MPLS стає найбільш стабільною в порівнянні з іншими мережами, які мають традиційну маршрутизацію [10].

Число міток, які використовуються дорівнює 1048576. Резервовані мітки мають значення від 0 до 16.

- 0 – «IPv4 Explicit null Label». MPLS-мітка, яка знаходиться на дні стека. Вона інформує, що треба видалити мітку з пакета, не перегладаючи таблицю міток. Шлях цього пакета повинен базуватися на заголовку IPv4.
- «Router Alert Label». Ця мітка може знаходитись будь-де в стеці міток окрім дна стека. Якщо в пакеті, що прибуває, мітка розташовується вгорі стека, то його перенаправляють місцевому програмному модулю для

обробки. Надалі маршрутизація буде виконуватися по мітці, що знаходиться нижче, чи на основі інформації, яка закладена в заголовок протоколу мережевого рівня або інкапсульованих в нього протоколів. Мітка «Router Alert Label» при переміщенні пакета знову розміщується нагорі стека.

- 3 «Implicit null Label». Задача LSR полягає в привласненні і поширенні цієї мітки, але вони не будуть вказані пакетами. При необхідності заміни мітки, яка розташовується вгорі стека, причому новою міткою є «Implicit NULL Label», то LSR робить видалення стека міток, замість того, щоб провести операцію заміни.
- 4 — 15 — значення резерву для майбутнього виконання [2,8].

2.1.2 Клас еквівалентності пересилання FEC

FEC (Forwarding equivalence class) – це форма представлення групи пакетів з однаковими вимогами до передачі. В заголовку IP-пакета міститься набагато більше інформації, а ніж потрібно для вибору наступного маршрутизатора. Цей вибір можна організувати шляхом виконання наступних двох груп функцій в маршрутизаторі:

- маршрутизатор відносить пакет до певного класу FEC;
- складає у відповідності кожному FEC наступний крок маршрутизації;

При традиційній IP-маршрутизації конкретний маршрутизатор також може вважати, що два пакети належать одному і тому ж умовному класу еквівалентності, якщо в його таблицях маршрутизації використовується деякий адресний префікс, що ідентифікує напрям, в якому передбачувані маршрути транспортування цих двох пакетів співпадають найдовше. По мірі просування пакета по мережі, кожний наступний маршрутизатор аналізує його заголовки і приписує цей пакет до класу еквівалентності (що належить лише даному маршрутизатору), який відповідає тому ж напрямку.

На відмінно від традиційної маршрутизації, при використанні багатопротокольної комутації на основі міток пакет ставиться у відповідність

певному класу FEC тільки один раз на вході в мережу MPLS. Цьому FEC присвоюється мітка, що потім передається разом з пакетом при його пересиланні до наступного маршрутизатора. В решті маршрутизаторів заголовок пакета не аналізується.

Таким чином, враховуючи вищесказане, можна дати наступне визначення FEC. Клас еквівалентності пересилання FEC – це форма представлення групи пакетів з однаковими вимогами до їх передачі, тобто всі пакети такої групи обробляються однаково на шляху їх слідування до пункту призначення.

Клас FEC представляє собою набір FEC-елементів, кожен з яких ідентифікується певною міткою. При розподілі пакетів по різним FEC важливу роль грають IP-адреси, пріоритети обслуговування та інші параметри трафіку. Кожен FEC обробляється окремо, що дозволяє підтримувати необхідний рівень якості обслуговування в мережі MPLS.

Метод пересилання пакетів на основі пар «FEC-мітка», прийнятий в MPLS, має ряд переваг перед методами, заснованими на аналізі заголовку блоків мережевого рівня. Зокрема, пересилання методом MPLS можуть виконувати маршрутизатори, які здатні читати і змінювати мітки, але при цьому не здатні достатньо швидко виконувати аналіз заголовків блоків мережевого рівня [13].

2.1.3 Протокол LDP

Протокол розподілу міток (Label Distribution Protocol – LDP) – це протокол, з допомогою якого два LER в мережі MPLS обмінюються інформацією про відображення міток. Обмін інформацією між LER двонаправлений.

Після активації LDP LSR виконує мультикастову розсилку UDP-дейтаграм на всі інтерфейси на адресу 224.0.0.2 і порт 646, де активовані LDP. Так виконується пошук сусідніх пристроїв. TTL таких пакетів рівний 1,

оскільки LDP-сусідство встановлюється між безпосередньо підключеними вузлами. Такі повідомлення називається Hello.

Коли сусіди виявлені, встановлюється TCP-з'єднання з ними, також по порту 654 – Initialization. Подальші повідомлення (окрім Hello) передаються з TTL рівним 255. Далі LSR періодично обмінюються повідомленнями Keepalive адресно по TCP і продовжують пошук сусідів повідомленнями Hello.

В якийсь момент один із LSR виявляє, що він є Egress LSR, тобто він є вихідним для якогось FEC. В залежності від режиму, він чекає на запит мітки для даного FEC або ж відразу її розсилає. Ця інформація передається в повідомленні Label Mapping Message. Сусідній маршрутизатор отримує для відповідного FEC мітку 3 (implicit null) і записує її до своєї таблиці міток. Мітка 3 є зарезервованою і означає, що мітку MPLS необхідно зняти і відправити на FEC чистий пакет. Паралельно даний LSR обирає вхідну мітку для FEC, записує до своєї таблиці міток і розсилає її сусіднім маршрутизаторам.

Важливою рисою LDP є те, що він не використовує в своїй роботі протоколи динамічної маршрутизації. Як уже говорилося раніше, головне його завдання – заповнити мережу мітками і для цього він використовує таблицю маршрутизації LSR. Таким чином, якщо на маршрутизатор прийде дві однакові мітки для одного FEC, то LDP обере для LSP лише ту мітку, яка отримана через кращій інтерфейс для цього FEC на основі інформації, взятої з таблиці маршрутизації. Отже LDP завжди буде будувати лише один найкращій шлях. При цьому протокол IGP може реалізовуватися будь-який [14].

2.2 Принципи роботи MPLS L3 VPN

Віртуальна приватна мережа (VPN) являє собою набір вузлів, що використовують інформацію маршрутизації 3-го рівня. Хоч VPN мережі технології MPLS не використовують процедуру встановлення з'єднання, при їх створенні вдається об'єднати переваги комутації 2-го рівня з принципами маршрутизації зі встановленим з'єднанням 3-го рівня. VPN MPLS дозволяють

також забезпечити безпеку зв'язку за рахунок того, що обмін інформацією про маршрутизацію відбувається лише між вузлами, що належать до даної VPN-мережі.

Вказана вище особливість дозволяє провайдеру створювати локальні розподілені мережі і надають можливість виходу в середовище Інтернет різним мережам VPN по спільній інфраструктурі, яка також може бути використана для надання служб IP, Ethernet, ATM і Frame Relay.

Функції VPN разом з багатопротокольною комутацією по міткам дозволяють реалізовувати в мережі провайдера розширювані магістральні VPN-служби 3-го рівня на базі протоколу IPv4. На рисунку 2.6 наведено приклад VPN-мережі, створеної провайдером. Можливість надавати користувачам розширювані VPN-мережі повністю відповідає інтересам провайдера. Промислові мережі, які побудовані на орендованих приватних інфраструктурах 2-го рівня, також можуть використовувати такі технології.

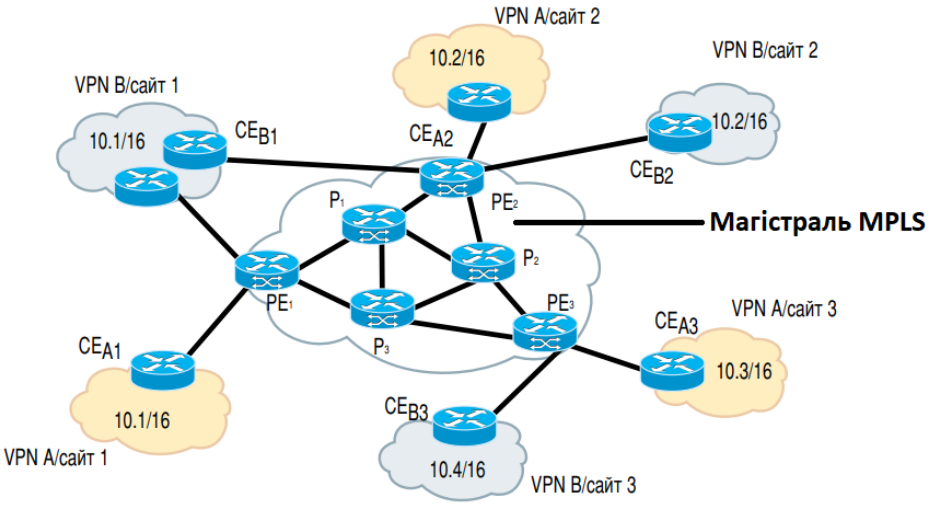

Рисунок 2.6 - Топологія мережі MPLS L3 VPN

Можна виділити наступні компоненти технології MPLS, що використовуються для створення VPN-мереж:

- **Базові маршрутизатори MPLS (P).** Базові маршрутизатори також називаються маршрутизаторами провайдера (P router), не містять маршрутів VPN-мереж. Разом з іншими LSR-пристроями провайдера, вони зазвичай утворюють повнозв'язну або напівз'язну топологію і

об’єднуються з граничними маршрутизаторами провайдера (provider edge – PE router). P-маршрутизатори ніколи не під’єднуються безпосередньо до маршрутизаторів користувача.

- **Граничні маршрутизатори мережі MPLS (MPLS edge routers – PE).** Маршрутизатори точок присутності, також відомі як граничні маршрутизатори провайдера (Provider Edge router – PE router), містить VPN-маршрути для мереж VPN, що ними підтримуються. Вони є пристроями того ж рангу, що і граничні маршрутизатори користувача (Customer Edge router – CE router) і підтримують інтерфейс з базовими маршрутизаторами провайдера. PE-маршрутизатори є пристроями того ж рангу що і P-маршрутизатори, тому можуть напряму бути з’єднаними з ними або з іншими PE-маршрутизаторами.
- **Граничні маршрутизатори користувача (Customer Edge router – CE router).** Граничним маршрутизаторам користувача не потрібні функції MPLS, а для підтримки з’єднань вони можуть використовувати звичайні методи маршрутизації. Рангова модель потребує, щоб вузол користувача підтримував паритетний зв’язок лише з одним PE-маршрутизатором. CE-маршрутизатори ніколи не під’єднуються до P-маршрутизаторів.
- **Маршрутизатори користувача (Costumer router – C-router).** Внутрішнім маршрутизаторам, що належать користувачеві, так звані C-маршрутизатори, не потрібно підтримувати функції MPLS, а для підтримки з’єднань між собою і CE-маршрутизаторами вони можуть використовувати звичайні методи маршрутизації.

Отже, VPN-мережі MPLS включають в себе пристрої користувача, під’єднані до CE-маршрутизаторів. CE-маршрутизатори будь-якої із VPN-мереж можуть бути під’єднані до будь-якого PE-маршрутизатора провайдера. PE-маршрутизатори об’єднані між собою через базову мережу P-маршрутизаторів [9, 12].

2.2.1 Маршрутизація і пересилання пакетів в мережах VPN

Кожна VPN-мережа логічно зв'язана з одним або більше комплексів маршрутизації і пересилання (VPN Routing and Forwarding instance – VRF). Комплекс VRF визначає приналежність в VPN-мережі вузла користувача, під'єднаного до PE-маршрутизатора. Екземпляр VRF складається з таблиці IP-маршрутизації, отриманої з неї таблиці експрес комутації (Cisco Express Forwarding – CEF), набору інтерфейсів, що використовують таку таблицю, і набору правил і параметрів протоколу маршрутизації, що керують інформацією таблиці маршрутизації.

Між вузлами користувача і VPN-мережами не обов'язково існує однозначна відповідність. Адже цілком можлива ситуація, коли один вузол може одночасно належати до декількох VPN-мереж. Проте, комплекс VRF може задавати тільки одну мережу VPN. VRF-комплекс вузла користувача містить всі маршрути, доступні цьому вузлу із VPN-мереж, членом якої він є. Для взаємного обміну пакетами протоколу IP версії 4 PE-маршрутизатори використовують глобальну IP-таблицю. VRF-таблиці IP-маршрутизації і пересилання використовуються для обміну інформаією всередині VPN-мережі. Оскільки PE-маршрутизатор може вміщувати декілька комплексів VRF, кожна комбінація VRF-таблиці IP-маршрутизації і CEF-таблиці пересилання даних може розглядатися як віртуальний маршрутизатор всередині фізичного PE-маршрутизатора (рисунок 2.7).

Рисунок 2.7 - Комплекси VRF на PE-маршрутизаторі

Для кожного комплексу VRF інформація про пересилання пакетів зберігається в таблиці IP-маршрутизації і в таблиці CEF. Для кожного екземпляра VRF підтримується окремий набір таблиць маршрутизації і таблиць CEF. Такі таблиці запобігають виходу маршрутної інофрмації замежі VPN-мережі і направленню пакетів з мережі VPN на маршрутизатор, що знаходиться в середині структури VPN. Приклад функціонування мережі VPN на основі таблиці VRF показано на рисунку 2.8.

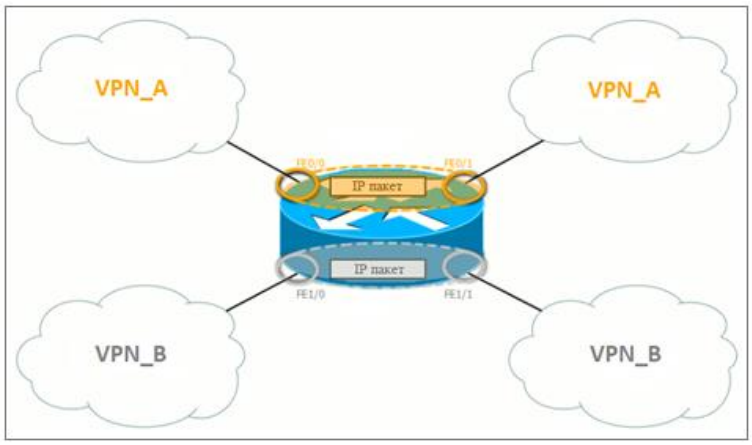

Рисунок 2.8 – VRF Lite VPN

Як бачимо, кожна VPN-мережа, підключена до одного маршрутизатора, є відокремленою одна від одної. Таким чином, дані однієї мережі не можуть перетинатися при передачі. Даний провайдерський VPN (без технології MPLS) називається VRF Lite.

Використовуючи VRF Lite, можна легко утворити VPN між різними кінцями мережі. Для цього необхідно налаштувати однакові VRF на всіх проміжних вузлах і правильно прив’язати їх до інтерфейсів (рисунок 2.9).

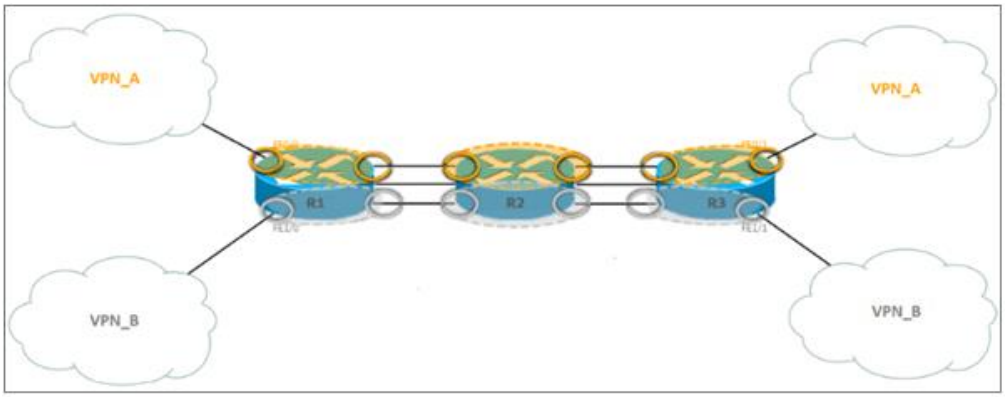

Рисунок 2.9 – VRF Lite VPN в мережі провайдера

Тобто R1 і R2 будуть взаємодіяти один з одним через одну пару інтерфейсів в глобальній таблиці маршрутизації, через другу пару інтерфейсів вони будуть взаємодіяти в VRF VPN_A, і через третю пару – в VRF VNP_B. Аналогічно буде і між R2 і R3.

Таким чином, утворюється дві віртуальні мережі, які не перетинаються між собою. Враховуючи цей факт, в кожній такій мережі необхідно підіймати свій процес IGP, щоб забезпечити зв'язність. В такому випадку буде один процес для фізичного маршрутизатора, один для VPN_A і один для VPN_B.

Якщо говорити про передачу даних, то пакет, прийшовши від вузла із мережі VPN_B, відразу потрапляє у відповідний VRF, так як вхідний інтерфейс R1 є його членом. Згідно FIB (Forwarding information base) даного VRF, пакет направляється на R2 через вихідний інтерфейс. На ділянці між R1 і R2 відбувається передача звичайних IP-пакетів, при цьому кожен із них належить до певної VPN-мережі. Різниця лише в тому, що вони проходять через різні фізичні інтерфейси, або несуть різний тег в заголовку 802.1Q. Приналежність пакета до певної VPN визначається через інтерфейс, який прив'язаний до конкретного VRF. Таким чином, R2 приймає пакет інтерфейсом, який також є членом VRF VPN_B. Далі R2 виконує схожі дії і відправляє пакет згідно IGP. Процес повторюється аж до виходу пакета з іншого боку мережі.

Можливі випадки, коли сайт пов'язаний з декількома мережами VPN. У такому випадку його таблиця VRF буде містити дані про маршрути усіх цих мереж. Наприклад, сайт CE1 належить до мереж VPN_A і VPN_B. У такому випадку таблиця VRF пристрою PE1 буде містити інформацію про маршрути мережі VPN_A і VPN_B. Іншими словами, на пристрої PE1 не буде двох окремих таблиць VRF. Зазвичай, на пристрої PE підтримується по одній таблиці VRF на кожен сайт, навіть якщо з цим сайтом уданого пристрою існує декілька з'єднань. Крім того, якщо різні сайти використовуються одним і тим же набором маршрутів, вони також будуть об'єднані водну таблицю VRF.

Обмеження протоколу маршрутизації (що використовується в середині VPN-мережі) однією VRF-таблицею дозволяє здійснювати накладання декількох VPN-мереж (наприклад підтримка зовнішніх по відношенню до мережі користувача структур VPN). Інтерфейси PE-маршрутизаторів логічно пов'язані з індивідуальними комплексами VRF. Інформація про маршрутизацію, отримана через ці інтерфейси, логічно пов'язана з сконфігурованими екземплярами VRF і називається контекстом маршрутизації (routing context). Деякі протоколи маршрутизації, такі як RIPv2, підтримують одночасно декілька контекстів одного протоколу, в той час як інші протоколи, такі як OSPF, потребують окремої копії процесу маршрутизації для кожного комплексу VRF.

Організація VPN Lite зручна лише в тому випадку, якщо кількість клієнтів і маршрутизаторів є незначною. Проблема полягає в тому, що така мережа абсолютно не піддається масштабуванню, адже один новий VPN означає необхідність створення нового комплексу VRF на кожному вузлі, нові інтерфейси, новий пул лінкових IP-адрес, новий процес IGP/BGP. Дана проблема дуже легко вирішується з допомогою технології MPLS [15].

2.2.2 Пересилання пакетів в мережі MPLS L3 VPN

При використанні комутації MPLS пакети направляються до пунктів призначення на основі маршрутної інформації, що міститься в таблиці IP-маршрутизації і в CEF-таблиці комплексу VRF. PE-маршрутизатор зв'язує мітку з префіксом кожного користувача, що був отриманий від CE-маршрутизатора, і включає мітку в інформацію про доступність мережі даного префіксу, яку він повідомляє іншим PE-маршрутизаторам. Відправляючи пакет, отриманий від CE-маршрутизатора по мережі провайдера, PE-маршрутизатор присвоює цьому пакету мітку, отриману від PE-маршрутизатора пункту призначення. Коли PE-маршрутизатор отримує помічений пакет, він видаляє мітку і використовує її для відправки пакета на потрібний CE-маршрутизатор.

P-маршрутизатори провайдера не приймають участі в процесі роботи протоколу MP-BGP і не передають VPN-маршрути. Вони не потрібні для прийняття рішень про маршрутизацію, що базуються на адресах VPN-мереж. P-маршрутизатори відправляють пакети на основі значень міток, призначених IP-пакетам. Ці маршрутизатори беруть участь в обміні мітками комутації MPLS, проте не є кінцевими пристроями VPN-мереж.

PE-маршрутизатори зазвичай ідентифікуються унікальними ідентифікаторами, такими як IP-адреса петльового інтерфейсу з 32-бітовими масками. Такі адреси використовуються разом з BGP-атрибутом наступного транзитного переходу для VPN-маршрутів, оголошених PE-маршрутизаторами. Маршрутам хостів мітки призначаються P-маршрутизаторами. Ці мітки потім передаються всім сусіднім пристроям. MPLS протокол LDP забезпечує отримання усіма PE-маршрутизаторами мітки, пов’язаної з даним маршрутизатором. Мережа VPN готова до обміну VPN-пакетами в той момент, коли вхідний PE-маршрутизатор отримує мітку для вихідного PE-маршрутизатора.

Пересилання на основі мітки по магістралі провайдера базується або на технології динамічної комутації помітці, або на маршрутах перерозподілу потоків. При перетині магістралі пакет даних користувача містить два рівні міток. Перша мітка направляє пакет до потрібного PE-маршрутизатора наступного транзитного переходу, а друга – вказує на комплекс VRF, логічно пов’язаний з вихідним інтерфейсом CE-маршрутизатора пункту призначення. Такий дворівневий механізм зазвичай називається ієрархічним тегом, або комутацією по міткам [14, 15].

Отримавши через будь-який інтерфейс від CE-маршрутизатора IP-пакет, PE-маршрутизатор логічно зв’язує його з комплексом VRF, в результаті чого утворюється нижня мітка, логічно зв’язана з вихідним PE-маршрутизатором, який ідентифікує VRF-комплекс адресата маршруту і вихідний інтерфейс вихідного PE-маршрутизатора. Така мітка називається сервісною (рисунок 2.10).

Рисунок 2.10 – Сервісна мітка

Із глобальної таблиці пересилки PE-маршрутизатор отримує також другу мітку, яка називається верхньою (рисунок 2.11). Вона вказує PE-маршрутизатор наступного транзитного переходу.

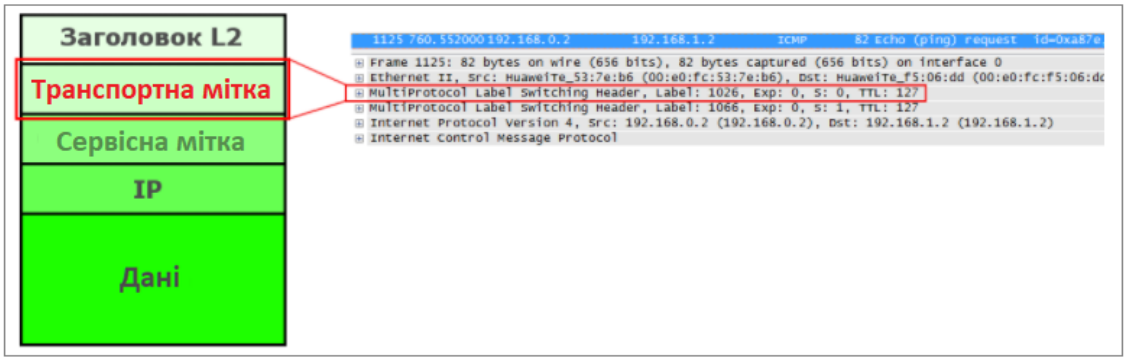

Рисунок 2.11 –Транспортна мітка

Далі цей стек міток «кріпиться» до VPN-пакета і направляється до наступного транзитного переходу. P-маршрутизатори в мережі MPLS аналізують верхню мітку і направляють пакет по мережі до місця призначення. Як приклад, розглянемо рисунок 2.12.

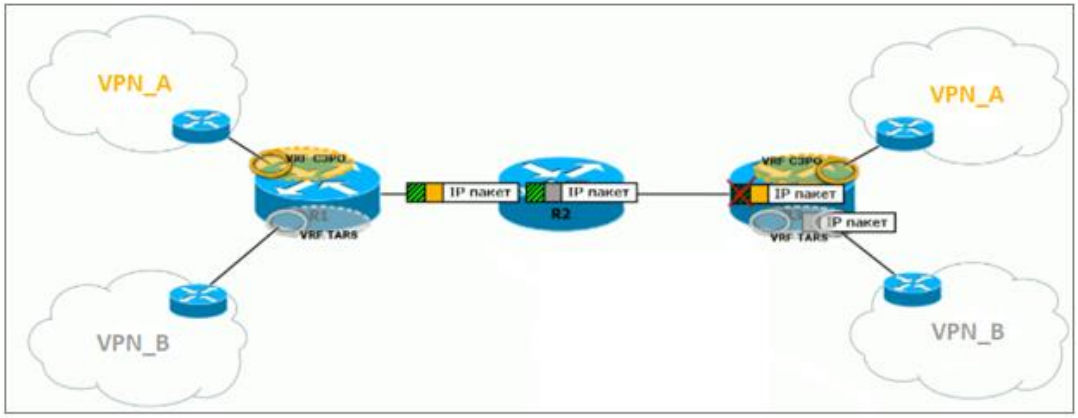

Рисунок 2.12 – Пересилання VPN-пакетів по мережі провайдера

Із мереж VPN_A і VPN_B одночасно на маршрутизатор R1 надходять IP-пакети. Ідентифікувавши кожен пакет і визначивши приналежність кожного з них до тієї чи іншої VPN-мережі (згідно з комплексом VRF), маршрутизатор R1 присвоює кожному пакету відповідну сервісну мітку (жовтий та сірий кольори). Поверх сервісної мітки кріпиться транспортна мітка. Далі пакети комутуються по мережі і таким чином потрапляють на маршрутизатор R2. Він виконує заміну транспортних міток (згідно з таблицею міток) і передає пакети на R3. При цьому сервісна мітка залишається незмінною. Маршрутизатор R3 видаляє транспортну мітку і на основі сервісної перенаправляє пакети до потрібної VPN-мережі. На вихідному інтерфейсі маршрутизатора сервісна мітка видаляється і в мережу VPN відправляється чистий IP-пакет.

2.2.3 Розповсюдження маршрутної інформації

Передача маршрутів по мережі провайдера від одного PE до іншого відбувається з допомогою протоколу EGP – BGP (Border Gateway Protocol). Зокрема, даний протокол може забезпечувати ізоляцію мереж VPN.

BGP є протоколом з дуже високим ступенем розширюваності, який може підтримувати дуже велику кількість VPN-мереж. Даний протокол також підтримує взаємний обмін маршрутної інформації між маршрутизаторами, які безпосередньо не пов’язані між собою. Це можливо в тих випадках, коли наявний відповідний протокол IGP, такий як OSPF або IS-IS, який забезпечує з’єднання 3-го рівня між BGP-пристроями одного рангу. Протокол BGP також володіє достатньою гнучкістю для передачі необов’язкових параметрів (атрибутів), що робить його бажаним при використанні разом із структурою VPN MPLS.

Протокол BGP розповсюджує інформацію про досяжність VPN-префіксів протоколу IP версії 4 для кожної VPN-мережі. Комунікація протоколу BGP відбувається на двох рівнях: в середині автономної системи і між автономними системами. Сеанси PE-PE являють собою сеанси IBGP, а

сеанси PE-CE є сеансами EBGP. Для кожної користувацької VPN-мережі необхідний окремий сеанс протоколу EBGP між PE- і CE-маршрутизаторами.

BGP встановлює сесію зі своїми «сусідами» через TCP на порт 179. Це дозволяє в якості сусідів обирати не напряму підключений маршрутизатор, а ті, що знаходяться в декількох хопах. Так і працює IBGP, де в межах магістральної мережі припускається зв'язок «кожен з кожним». Коли декілька маршрутів, що ведуть в одну мережу, приходять на вузол, BGP просто обирає з них найкращій і інсталює його в таблицю маршрутизації.

Проте для організації VPN-мереж BGP має один суттєвий недолік. З самого початку цей протокол орієнтовано на роботу з публічними адресами, які є унікальними у всьому світі. Клієнти зазвичай прагнуть передавати маршрути в приватні мережі (RFC 1918), тому цілком можливо, що адресні простори можуть перетинатися як з мережами інших VPN, так і з внутрішнім адресним простором самого провайдера. Тобто, наприклад, якщо маршрутизатор R3 отримає два маршрути в мережу 10.10.10.10/32 (рисунок 2.13), один від VPN_A і другий від VPN_B, то він вибере лише один – з найкращими показниками, згідно зі стандартом.

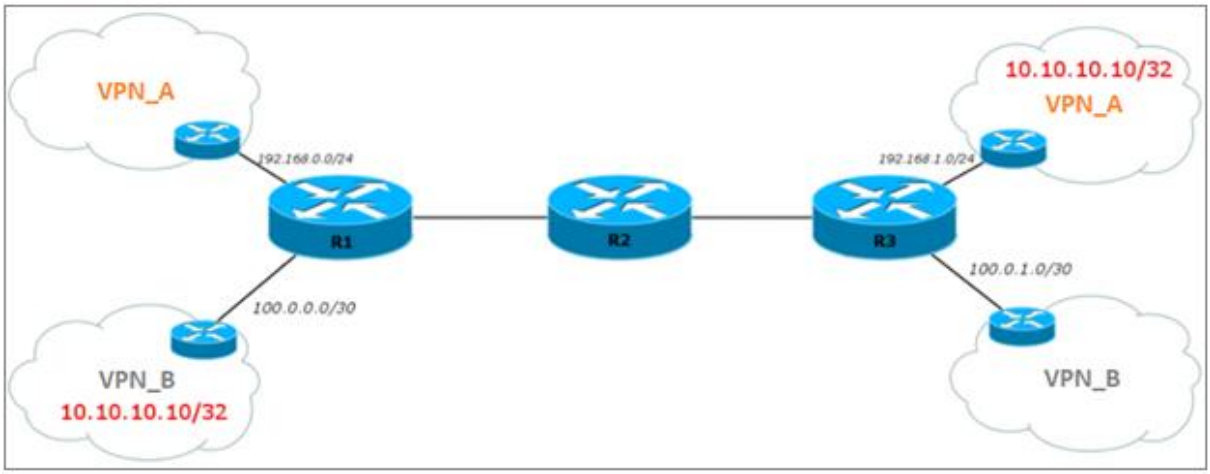

Рисунок 2.13 – Перетин адресних просторів двох мереж VPN

Це призведе до змішування трафіку однієї VPN-мережі з іншою, що є досить серйозною проблемою. Необхідно дотримуватися двох основних умов:

1. Маршрути різних VPN повинні бути унікальними і не змішуватися при передачі між PE.

2. Маршрути в кінцевій точці повинні бути передані відповідному VRF-комплексу.

BGP є неймовірно гнучким протоколом. Він досить легко масштабується і з допомогою так званих Address Family він може передавати маршрути не тільки IPv4, а й IPv6 і IPX. Такий BGP отримав багатопротокольний протокол граничного шлюзу (Multiprotocol Border Gateway Protocol – MP-BGP).

Для того, щоб розрізняти різні маршрути різних VPN-мереж з однаковими адресами, кожній з них присвоюється приставка довжиною 8 байтів – RD – Route Distinguisher. Існує 3 типи Route Distinguisher (рисунок 2.14).

Тип 0 (2 байта)	ASN (2 байта)	Значення (4 байта)
Тип 1 (2 байта)	IP (4 байта)	Значення (2 байта)
Тип 2 (2 байта)	ASN (4 байта)	Значення (2 байта)

Рисунок 2.14 – Типи Route Distinguisher

Кожен тип має наступні складові:

- Поле 1. Вказує на тип RD (0, 1, 2).
- Поле 2. Адміністративне поле – це завжди публічний параметр – публічна IP-адреса або публічний номер AS. Воно необхідне для того, щоб RD були унікальними не лише в межах мережі, а й в межах всієї планети.
- Поле 3. Виділений номер (Assigned Number). Ця частина дозволяє RD бути унікальним в межах мережі користувача, і, відповідно, визначати VPN.

Тоді маршрут від VPN_A буде мати наступний вигляд: 64500:100:10.10.10.10/32, а від VPN_B – 64500:200:10.10.10.10/32 (рисунок 2.15). Тепер це абсолютно різні речі, які процес BGP зможе відрізнити.

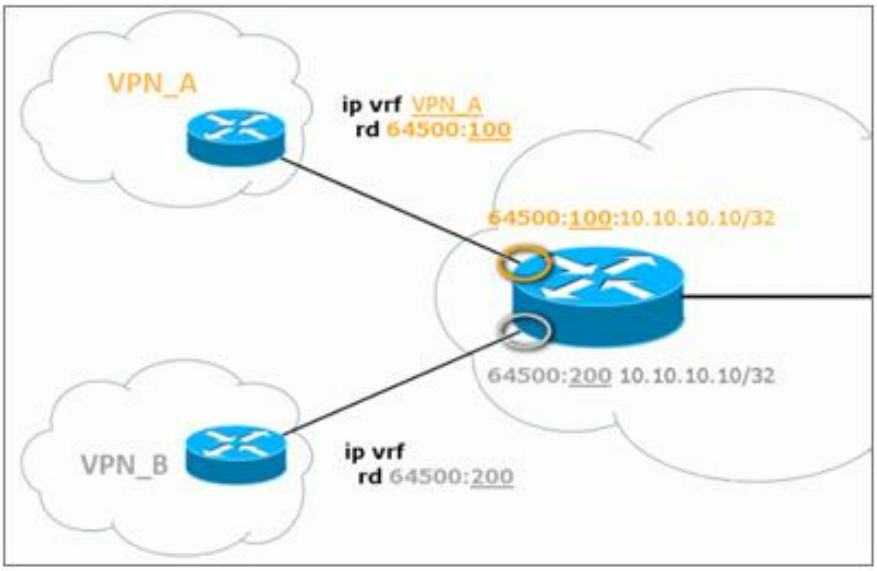

Рисунок 2.15 – Принцип застосування Route Distinguisher в VPN-мережах

Детально цей процес можна описати так:

- **Етап 1.** Від маршрутизатора CE приходить анонс нової мережі – 10.10.10.10/32. PE-маршрутизатор додає цей маршрут в таблицю маршрутизації конкретного VRF-комплексу.
- **Етап 2.** BGP помічає, що з'являється новий префікс в VPN. Із конфігурацій VRF-комплексу він бачить який RD потрібно використовувати. Далі він компілює з RD і нового IPv4-префіксу префікс VPNv4.
- **Етап 3.** Створюючи BGP Update, маршрутизатор вставляє туди отриманий VPNv4-префікс, адресу Next Hop і решту атрибутів BGP. Також в поле NLRI додається інформація про мітку. Ця мітка прив'язана до маршруту, тобто VPNv4-префікс – це FEC, а в NLRI передається зв'язка даного FEC і мітки. Таким чином PE-маршрутизатор повідомляє своїм сусідам, що якщо вони отримали від CE-маршрутизатора IP-пакет в дану мережу, то йому необхідно присвоїти певну сервісну мітку.
- **Етап 4.** BGP Update передається усім сусідам, що налаштовані в секції VPNv4 family.
- **Етап 5.** Віддалений PE отримує Update, аналізує NLRI, визначає що це не звичайний IPv4 маршрут, а VPNv4. Як вже говорилося раніше, якщо

на маршрутизатор прийде два однакових маршрути в одну мережу від різних клієнтів, то з допомогою RD вони ніяк не перетнуться. Далі Egress PE визначає в який VRF цей маршрут необхідно експортувати.

Зазвичай використовується тип 0 Route Distinguisher, де адміністративне поле – це номер AS провайдера, а Виділений номер обирається клієнтом. При налаштуванні RD перші «0:» або «1:» (тип RD) скорочуються. Саме типи 1 і 0 дозволяє використовувати Cisco. При цьому варто зауважити, що RD налаштовуються вручну і при цьому потрібно також слідкувати за його унікальністю. Це пов’язано з тим, що маршрутизатори не вміють відслідковувати RD на інших вузлах.

Єдине завдання Route Distinguisher – це зробити маршрути унікальними. Незважаючи на те, що він налаштовується для VRF-комплексів, він не є якимось унікальним ідентифікатором і на усіх точках підключення це значення може бути різним. Тому PE-маршрутизатор не може визначити в який VRF-комплекс помістити маршрут на основі RD. До того ж, це не властиво для BGP, адже для аналізу переданої адреси перед її анонсом існують спеціальні політики. Тобто в класичному BGP довелося б налаштовувати політики на експорт маршрутів в VRF для кожного окремо [16, 17].

Для вирішення даної проблеми можна використовувати community. При відправленні маршруту з одного PE на інший можна встановлювати певний community – свій для кожного VRF, а на віддаленому PE за цим community вже налаштовувати експорт у відповідний VRF. Проте в MP-BGP ідею community розвинули до поняття Route Target (RT). По суті, це те саме community – RT навіть передається в атрибуті Extended Community, проте всі політики працюють автоматично. Принцип роботи Route Target продемонстровано на рисунку 2.16.

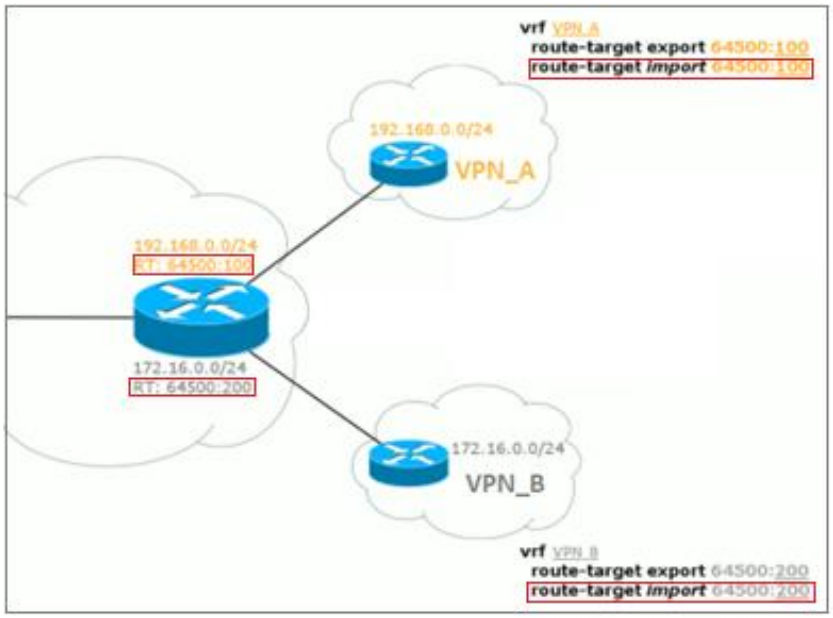

Рисунок 2.16 – Принцип функціонування Route Target

З одного боку мережі в VRF-комплексі налаштовується RT на експорт маршруту – той RT, з яким цей маршрут буде пересилатися до віддаленого PE-маршрутизатора. З іншого боку, на віддаленому маршрутизаторі саме це значення RT встановлюється на імпорт. Відповідно R1 надсилає R3 маршрут до мережі 10.10.10.10/32 (VBP_B), вказуючи мітку та інші параметри, зокрема в атрибут Extended Community записується RT на експорт маршруту, який налаштовано для даного VRF: 64500:200. R3 отримує анонс і перевіряє community. Побачивши 64500:200, відповідно до своїх конфігурацій, він знає, що маршрут з таким RT необхідно імпортувати в мережу VPN_B. Аналогічно відбувається і для мережі VPN_A.

2.4 Переваги побудови L3 VPN на базі MPLS

Можна виділити наступні переваги побудови L3 VPN на базі MPLS:

- безпека;
- простота створення мережі VPN;
- гнучкість адресації;
- відповідність стандартам;
- гнучкість структури;
- наскрізні служби задання пріоритетів;

- консолідація;
- перерозподіл потоків;
- централізоване обслуговування;
- підтримка інтегрованих класів обслуговування;
- модернізація та модифікація мережі;

Безпека. VPN-мережі технології MPLS забезпечують високий рівень конфіденційності даних. Пакети однієї VPN-мережі не можуть випадковим чином потрапити в іншу мережу VPN, оскільки безпека забезпечується на межі інфраструктури провайдера, де пакети, отримані від користувача, відправляються в потрібну VPN-мережу. В магістралі дані окремих VPN-мереж переміщаються окремо. «Сніфінг» стає практично не можливим, оскільки IP-пакети користувачів повинні бути отримані на конкретному інтерфейсі чи підінтерфейсі, де вони однозначно ідентифікуються по VPN-міткам.

Простота створення мережі VPN. При створенні VPN-мереж не потребується спеціальних таблиць перетворень для з'єднання «точка-точка» або додаткових топологій. Для створення закритих груп користувачів до внутрішніх і зовнішніх мереж можуть бути додані нові вузли. При такому керуванні VPN-мережами, вузол може знаходитися в декількох VPN-мережах, що надає максимальну гнучкість при побудові інфраструктури. Функції MPLS виконуються в мережі провайдера, а в конфігуруванні обладнання користувача або взагалі нема необхідності, або потребується, але не значне.

Гнучка адресація. Для того, щоб зробити службу VPN більш доступною, користувачі провайдера можуть створити власну схему адресації, незалежну від схем адресації інших користувачів цього провайдера. Чимало користувачів використовують власні адресні простори, у відповідності з специфікацією RFC 1918 і не мають бажання витрачати час та ресурси на перетворення відкритих IP-адрес для створення з'єднань внутрішньої мережі. VPN-мережа MPLS дає можливість використовувати адресний простір без

трансляції мережевих адрес (Network Address Translation – NAT). Використання служби трансляції NAT стає необхідним лише в тому випадку, коли двом VPN-мережам з адресними просторами, що перетинаються, необхідно встановити зв'язок. Ця служба дає можливість використати власні незареєстровані приватні адреси і вільно здійснювати зв'язок через відкриту IP-мережу.

Відповідність стандартам. Комутація MPLS може бути використана всіма розробниками для забезпечення взаємодії між мережами, що включають в себе обладнання різних розробників.

Гнучкість мережевої інфраструктури. Програмне забезпечення Cisco IOS в поєднанні з маршрутизаторами і комутаторами Cisco дозволяє провайдерам легко встановлювати між-мережеве з'єднання з іншими провайдерами для забезпечення глобального розповсюдження технології IP на потрібні мережі.

Наскрізні служби задання пріоритетів. Механізми якості обслуговування забезпечують користувачам необхідну якість комунікацій на всій протяжності маршруту, а провайдерам дозволяють гарантувати виконання умов угод про рівень обслуговування. Технологія MPLS забезпечує розширюваність QoS і його розповсюдження на чималу кількість технологій наскрізних з'єднань.

Консолідація. Об'єднання в одному потоці звичайних цифрових даних, голосу і відео дозволяє провайдерам зменшити витрати на підтримку роботи мережі.

Перерозподіл потоків. Маршрутизація з перерозподілом потоків і резервуванням ресурсів дозволяє провайдерам максимально використовувати мережеві ресурси і досягати оптимальної роботи мережі. Також вона дозволяє оператору застосовувати явно задані маршрути і примусово направляти по ним потоки даних, що замінює традиційні методи IP-маршрутизації і надає користувачеві механізми захисту і швидкого відновлення роботи мережі у

випадку відмови пристроїв. При цьому досягається оптимізація роботи недостатньо навантажених каналів і більш ефективна маршрутизація.

Централізоване обслуговування. Побудова VPN-мереж на третьому рівні дозволяє надати необхідні служби групам користувачів даної VPN. VPN-мережа має не тільки надавати провайдерам механізм приватного підключення користувачів до intranet-служб, а й забезпечувати спосіб гнучкого надання додаткових служб окремим користувачам. При цьому питання розширюваності набуваються виняткової важливості, оскільки користувачі хочуть використовувати служби приватно в своїх внутрішніх та зовнішніх мережах. Оскільки середовища MPLS розглядаються як приватні внутрішні мережі, нові IP-служби можуть бути використані для наступних цілей: для багатоадресної розсилки; для забезпечення якості обслуговування; для підтримки телефонного зв'язку між мережами VPN; для централізованих служб в середині середовищ VPN;

Інтегрована підтримка класів обслуговування. Рівень якості обслуговування представляє собою важливу вимогу багатьох користувачів VPN-мереж технології IP. Функції QoS дозволяють дві фундаментальні вимоги до мережі VPN:

- передбачуваність мережі і реалізація заданої стратегії;
- підтримка різних рівнів обслуговування в VPN-мережах MPLS;

Перед тим, як потоки даних будуть об'єднанні у відповідності зі стратегією, що задається клієнтами, і направлені в пункти призначення по магістралі провайдера, на межі мережі виконується їх класифікація і призначення їм міток. В магістралі чи на межі мережі потоки даних можуть диференціюватися по різним класам на основі ймовірності відкидання пакетів або величини затримки в каналах.

Модернізація і модифікація мережі. Розміщення служби VPN потребує ясного плану модифікації мережі. VPN-мережі MPLS унікальні, оскільки їх можна побудувати на базі декількох мережевих структур, включаючи IP, ATM, Frame Relay і гібридні мережі. Модернізація мережі для

кінцевого користувача полегшується, оскільки на граничному маршрутизаторі користувача не потребується підтримка служб MPLS, а у внутрішній мережі користувача не потребується ніяких модифікацій.

2.4 Висновки до другого розділу

В мережі MPLS основним обладнанням є маршрутизатори P, PE, CE. Оскільки MPLS – це технологія, що використовується в магістральних мережах операторів зв'язку, то її структура задовольняє найважливіші концепції магістральних технологій. В її структурі, таким чином, виділяються:

- рівень ядра (на основі P-маршрутизаторів);
- рівень агрегації (на основі PE-маршрутизаторів);
- рівень доступу (на основі CE-маршрутизаторів);

В результаті дослідження принципів роботи технології MPLS L3 VPN, можна сказати, що дана технологія на сьогодні є провідною для побудови віртуальних приватних мереж. Адже вона характеризується високим рівнем масштабованості, гнучкості, безпеки, а використання міток для комутації в мережі провайдера MPLS дозволяє реалізовувати прискорену передачу трафіку по магістральній мережі. Та найголовнішою перевагою даної технології є простота її реалізації, відносна дешевизна і висока надійність.

3. ПОБУДОВА ВІРТУАЛЬНОЇ ПРИВАТНОЇ МЕРЕЖІ НА БАЗІ MPLS

3.1 Розробка технічного завдання

Згідно з теоретичними відомостями, наданими в розділах 1 і 2, і, відповідно до обраної теми атестаційно-випускної роботи, необхідно спроектувати модель мережі VPN на базі технології MPLS, використовуючи середовище Dynamips з графічним інтерфейсом GNS3, і оцінити її працездатність.

Вся мережа має бути розбита на дві основні частини, а саме - мережа провайдера і мережа клієнтів. При цьому мережі клієнтів не повинні бачити

мережу провайдера і мати до неї доступ. Також необхідно зконфігурувати мережу таким чином, щоб мережі різних клієнтів не мали доступ до мережі іншого клієнта і не бачили її.

Мережа провайдера має підтримувати різні протоколи маршрутизації, такі як IS-IS, OSPF та інші, щоб забезпечити підключення різних клієнтів до мережі провайдера. Також необхідно забезпечити можливість підключення клієнта по протоколу BGP. Загальна модель мережі наведена на рисуноку 3.1.

Рисунок 3.1 – Згальна модель мережі

Спроектована мережа повинна бути добре масштабованою і забезпечувати швидке підключення нового клієнта в мережу. В ході проектування необхідно визначитися з обладнанням. Обладнання має відповідати наступним вимогам: надійність, швидкодія, якість. Необхідно також розробити таблицю адресації, згідно з якою буде виконуватися процес конфігурування.

3.2 Вибір обладнання

В розроблюваній моделі мережі будуть використовуватися маршрутизатори Cisco 7200 в ролі маршрутизаторів провайдера. Маршрутизатори серії 7200 забезпечують високу надійність, відмовостійкість, підтримку широкого спектру середовищ передачі даних. За рахунок модульності їх конструкції замовник може підібрати конфігурацію, відповідну його запитам, що дозволяє домогтися оптимального поєднання функціональності і вартості мережі. Для забезпечення відмовостійкості системи в Cisco 7200 передбачена можливість підключення двох джерел

живлення, а також можливість заміни інтерфейсних модулів без припинення функціонування пристрою.

Рисунок 3.2 – Маршрутизатор Cisco серії 7200

Маршрутизатори Cisco серії 7200 є найбільш поширеними універсальними рішеннями для агрегації сервісів та мають наступні характеристики:

- агрегація широкосмугових мереж: до 16 000 сесій PPP для кожного шасі;
- Мультипротокольна комутація на основі міток (MPLS): найбільш популярний вибір для реалізації граничних сегментів мереж провайдерів послуг;
- Віртуальні приватні мережі на базі IPsec: масштабується до 5 000 тунелів для кожного шасі;
- Підтримка шлюзів IP-to-IP: забезпечує точку взаємодії між мережами сигналізації (H.323, SIP), середовищами передачі, трансляцію адрес і номерів портів (забезпечення конфіденційності і приховування топології), функції тарифікації та нормалізації записів про виклики (CDR), а також управління пропускною спроможністю (маркування системи управління якістю обслуговування з використанням TOS);
- Інтеграція передачі голосу, відео і даних: шасі VXR і адаптери голосових портів з підтримкою TDM;

- Модульна архітектура: форм-фактор 3RU і широкий набір гнучких модульних інтерфейсів;
- Гнучкість: підтримка FastEthernet, GigabitEthernet, Packet over SONET та ін.;

В якості маршрутизаторів клієнта буде використано Cisco 2691. Маршрутизатор Cisco 2691 - це недорогий модульний маршрутизатор для невеликих (до 20 осіб) і середніх (до 250 осіб) офісів, і включає в себе можливість передачі голосових і факсимільних повідомлень.

Рисунок 3.3 – Маршрутизатор Cisco серії 2691

Запропонований набір модулів дозволяє використовувати маршрутизатор Cisco 2691 для доступу до серверів і брандмауерів, а також для передачі голосу і факсу через мережі TCP/IP. Останні серії 2600 - Cisco 2600XM і Cisco 2691 серії надають можливість застосовувати цю серію у великих корпоративних мережевих проектах. Ці моделі мають розширені можливості, більш потужну платформу для зростаючих потреб у розвитку мереж. Маршрутизатор Cisco 2691 мають 2 порти Fast Ethernet, 2 слоти WAN, один слот для мережевого модуля і один слот для модуля AIM.

Основні можливості маршрутизатора Cisco 2691:

- підтримка усіх функцій ПЗ Cisco IOS;
- модульна архітектура;
- вбудовані порти ЛОМ;
- підтримка передачі голосу поверх протоколу IP;
- застосування флеш-пам’яті спрощує заміну і обслуговування ПЗ;

- сервісний модуль апаратного стискання даних дозволяє зменшити вартість витрат нароботу через глобальні мережі і більш ефективно використовувати можливості ПЗ Cisco IOS;

В маршрутизаторах серії Cisco 2600 використовуються спільні для серій Cisco 1700, Cisco 3600 і Cisco 3700 модулі.

3.3 Конфігурування маршрутизаторів мережі

Для налаштування мережі провайдера, що надає послуги VPN на базі технології MPLS, необхідно виконати наступні дії:

- Етап 1. Конфігурування інтерфейсів мережі провайдера і користувача (лінкові та loopback) і протоколу IGP.
- Етап 2. Налаштування MPLS (на основі протоколу LDP).
- Етап 3. Конфігурування комплексів VRF.
- Етап 4. Налаштування MP-BGP в мережі провайдера.
- Етап 5. Дослідження зконфігурованої мережі.

На рисунку 3.1 пристрої R1, R2, R3, R4, R5, R6, R7, R8 є маршрутизаторами мережі провайдера, зокрема: R1, R4, R6 і R8 – граничні маршрутизатори провайдера (PE), R2, R3, R5, R6, R7 – внутрішні маршрутизатори мережі провайдера (P). Маршрутизатори CE – граничні маршрутизатори користувачів.

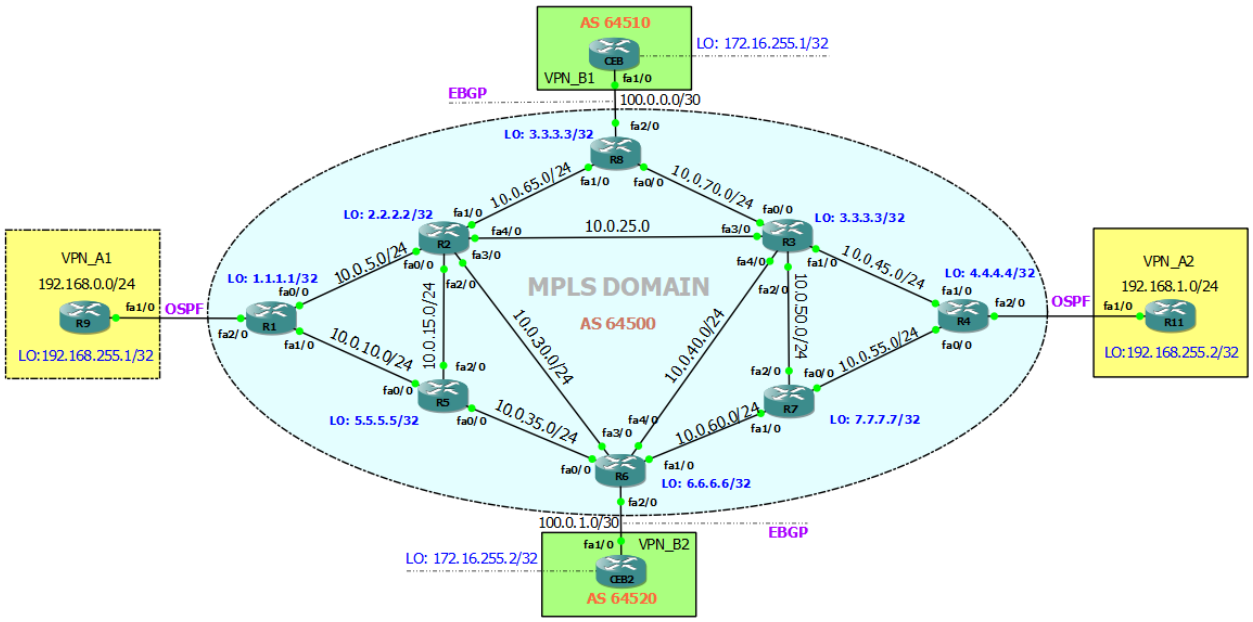

Рисунок 3.4 – Модель організації мережі MPLS L3 VPN

Кожному інтерфейсу маршрутизатора присвоєно свою IP-адресу та маску мережі. Для запуску процесів динамічної маршрутизації кожному маршрутизатору також було присвоєно loopback0 інтерфейс з відповідною маскою. Усі дані було занесено до таблиці IP-адресацій (таблиця 2.1).

Таблиця 2.1

IP-адресація мережі

Маршрутизатор	**Інтерфейс**	**IP-адреса**	**Маска**
R1	FastEthernet0/0	10.0.5.1	255.255.255.0
	FastEthernet1/0	10.0.10.1	255.255.255.0
	FastEthernet2/0	172.16.0.1	255.255.255.0
	Loopback0	1.1.1.1	255.255.255.255
R2	FastEthernet0/0	10.0.5.2	255.255.255.0
	FastEthernet1/0	10.0.65.1	255.255.255.0
	FastEthernet2/0	10.0.15.1	255.255.255.0
	FastEthernet3/0	10.0.30.1	255.255.255.0
	FastEthernet4/0	10.0.25.1	255.255.255.0
	Loopback0	2.2.2.2	255.255.255.255
	FastEthernet0/0	10.0.70.1	255.255.255.0

R3	FastEthernet1/0	10.0.45.1	255.255.255.0
	FastEthernet2/0	10.0.50.1	255.255.255.0
	FastEthernet3/0	10.0.25.2	255.255.255.0
	FastEthernet4/0	10.0.40.1	255.255.255.0
	Loopback0	3.3.3.3	255.255.255.255
R4	FastEthernet0/0	10.0.55.1	255.255.255.0
	FastEthernet1/0	10.0.45.2	255.255.255.0
	FastEthernet2/0	172.16.1.1	255.255.255.0
	Loopback0	4.4.4.4	255.255.255.255
R5	FastEthernet0/0	10.0.35.1	255.255.255.0
	FastEthernet1/0	10.0.10.2	255.255.255.0
	FastEthernet2/0	10.0.15.2	255.255.255.0
	Loopback0	5.5.5.5	255.255.255.255
R6	FastEthernet0/0	10.0.35.2	255.255.255.0
	FastEthernet1/0	10.0.60.1	255.255.255.0
	FastEthernet2/0	100.0.1.2	255.255.255.252
	FastEthernet3/0	10.0.30.2	255.255.255.0
	FastEthernet4/0	10.0.40.2	255.255.255.0
	Loopback0	6.6.6.6	255.255.255.255
R7	FastEthernet0/0	10.0.55.2	255.255.255.0
	FastEthernet1/0	10.0.60.2	255.255.255.0
	FastEthernet2/0	10.0.50.2	255.255.255.0
	Loopback0	7.7.7.7	255.255.255.255
R8	FastEthernet0/0	10.0.70.2	255.255.255.0
	FastEthernet1/0	10.0.65.2	255.255.255.0
	FastEthernet4/0	100.0.0.1	255.255.255.252
	Loopback0	8.8.8.8	255.255.255.255
R9 (CE_VPN_A1)	FastEthernet0/0	172.16.0.2	255.255.255.0
	Loopback0	192.168.255.1	255.255.255.255

R11 (CE_VPN_A2)	FastEthernet0/0	172.16.1.2	255.255.255.0
	Loopback0	192.168.255.2	255.255.255.255
R10 (CE_VPN_B1)	FastEthernet1/0	100.0.0.2	255.255.255.0
	Loopback0	172.16.255.1	255.255.255.255
R12 (CE_VPN_B2)	FastEthernet1/0	100.0.1.2	255.255.255.0
	Loopback0	172.16.255.2	255.255.255.255

3.3.1 Конфігурування інтерфейсів мережі і протоколу IGP

Для того, щоб зконфігурувати інтерфейси мережі провайдера (P- і PE-маршрутизатори) і протокол IGP, необхідно виконати наступні дії (для прикладу усі конфігурації будуть виконуватися на маршрутизаторі R1).

Етап 1. В режимі глобальної конфігурації виконати команду *interface fastethernet {interface number}* і з допомогою команди *ip address {address} {mask}* вказати IP-адресу даного інтерфейса і його маску (згідно з таблицею IP-адресації). Командою *no shutdown* активувати інтерфейс (рисунок 3.5).

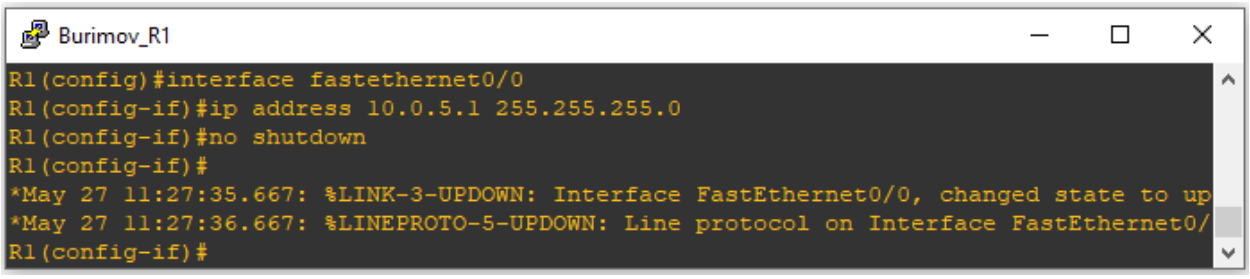

Рисунок 3.5 – Конфігурування інтерфейсу

Після активації команди *no shutdown* має з'явитися характерне повідомлення про зміну стану інтерфейса на up. Перевірка підключень виконується командою ping з домену провайдера.

Етап 2. Виконати команду interface loopback0 і з допомогою команди *ip address {address} {mask}* вказати IP-адресу даного інтерфейса і його маску (згідно з таблицею IP-адресації). Loopback - сукупність методів, потрібних для коректної роботи маршрутизатора і передачі даних. Сам інтерфейс же є відображенням логічних процесів в маршрутизаторі.

Командою *show ip interface brief* можна переглянути інформацію про стан інтерфейсів (рисунок 3.6).

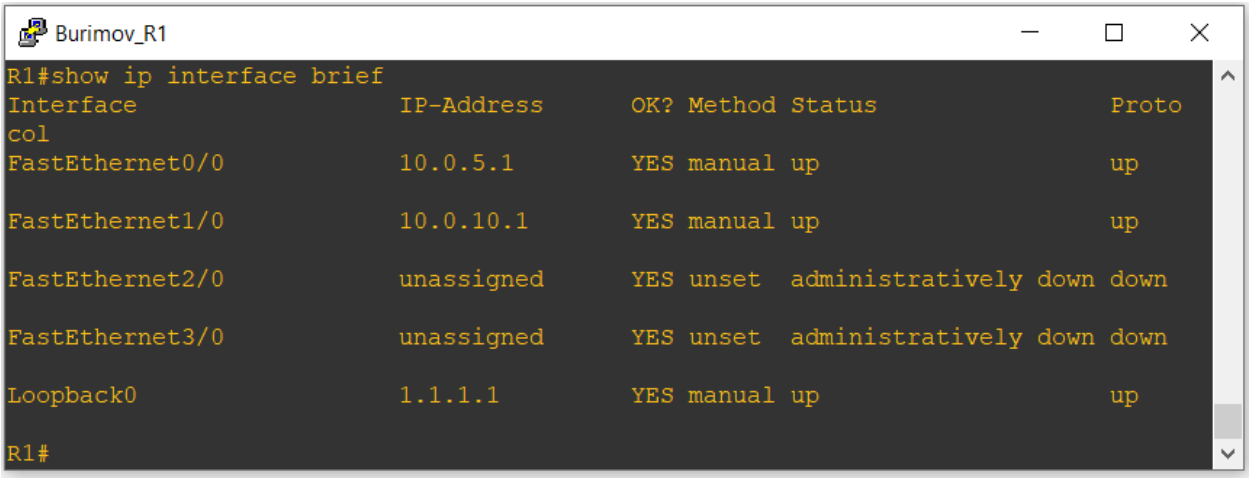

Рисунок 3.6 – Інформація про стан інтерфейсів

Етап 3. Командою *router isis {name}* запустити на маршрутизаторі протокол динамічної маршрутизації IS-IS. Поле *name* IS-IS процесу в IOS не є обов'язковим, але при запуску протокола необхідно пам'ятати, задавалося це ім'я чи ні. Від цього буде залежати синтаксис команди для запуску протоколу на інтерфейсі. Після запуску протокола необхідно обов'язково вказати ідентифікатор NET (Network Entity Title) на кожному маршрутизаторі. Для запуску протокола IS-IS на інтерфейсах необхідно ввести команду *interface fastethernet {interface number}* і ввести команду *ip router isis {name}*. Результат виконання команд показано на рисунку 3.7.

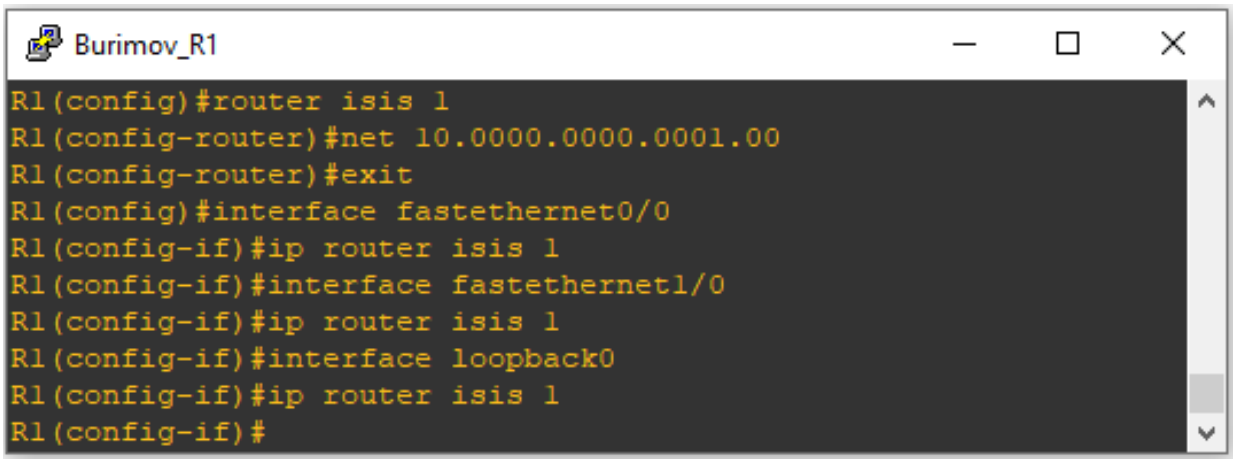

Рисунок 3.7 – Конфігурування протоколу IS-IS

Сформовану таблицю маршрутизації можна переглянути командою *show ip rout* (рисунок 3.8).

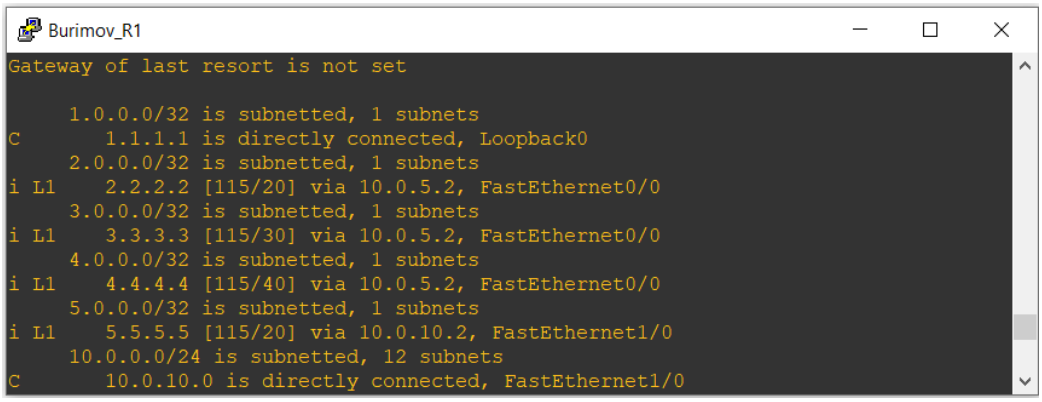

Рисунок 3.8 – Таблиця маршрутизації R1

Якщо процеси динамічної маршрутизації функціонують неправильно (наприклад, в таблиці маршрутизації відображено не всі маршрути), необхідно перевірити налаштування інтерфейсів, налаштування IS-IS та фізичні підключення. Конфігураційний файл маршрутизатора R2 на даному етапі виглядає наступним чином:

interface Loopback0

ip address 1.1.1.1 255.255.255.255

ip router isis 1

!

interface FastEthernet0/0

ip address 10.10.1.1 255.255.255.0

ip router isis 1

duplex half

!

interface FastEthernet1/0

ip address 10.10.3.1 255.255.255.0

ip router isis 1

duplex half

!

router isis 1 *net 10.0000.0000.0001.00*

Приклади конфігураційних файлів інших маршрутизаторів надано в додатку 1.

CE-маршрутизатори можуть належати користувачу або провайдеру. Як правило, якщо провайдер надає послуги VPN, то CE-маршрутизатори належить провайдеру і підтримується ним. Користувачам надається детальна інформація про IP-структуру і відповідна документація для нумерації IP-пристроїв користувача і внутрішньої маршрутизації. Більшість провайдерів бажають самостійно керувати CE-маршрутизаторами, особливо якщо структура їх VPN-мереж MPLS досить складна. Усунення помилок і несправностей в таких ситуаціях стає досить складним процесом, якщо інженери провайдера не мають повного доступу до CE-маршрутизатора.

Для клієнтських маршрутизаторів необхідно виконати аналогічні налаштування згідно з таблицею IP-адресації. В якості протокола динамічної маршрутизації для VPN_A буде використано протокол OSPF. Щоб його запустити, необхідно в режимі глобальної конфігурації ввести команду *router ospf [name]*. Після цього вводиться команда *network {ip-address} {wild-card mask} area {area number}*, де: *network {ip-address}* – анонс підмереж; *{wild-card mask}* – інверсна маска, яка вказує яка частина IP-адреси може змінюватися; *area {area number}* – номер зони, в якій запущено OSPF. Приклад конфігурування маршрутизатора CE_VPN_A1 показано на рисунку 3.9.

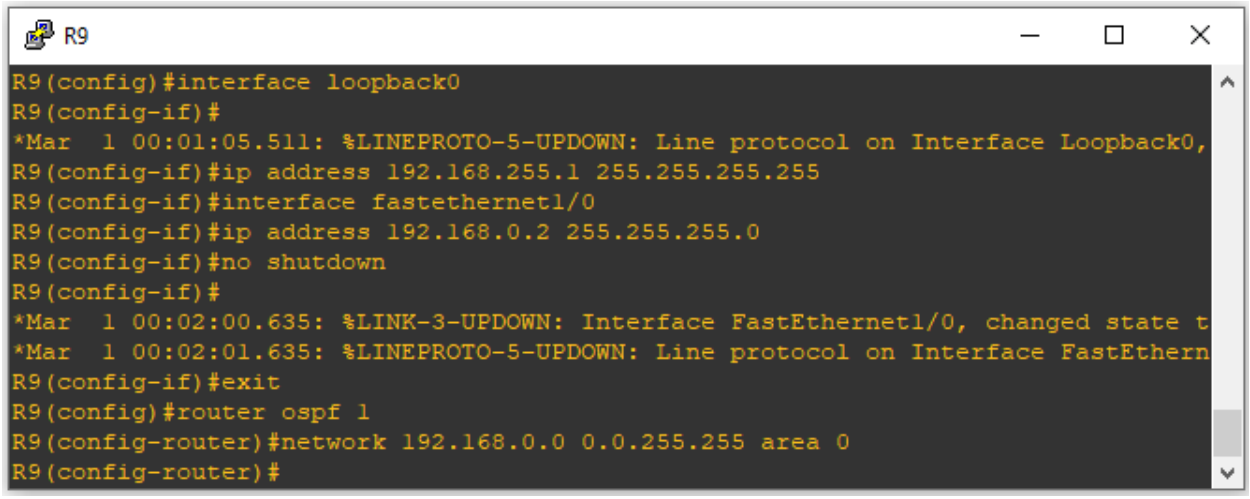

Рисунок 3.9 – Конфігурування CE-маршрутизатора VPN_A1

Приклад конфігурування маршрутизатора CE_VPN_A2 наведено на рисунку 3.10.

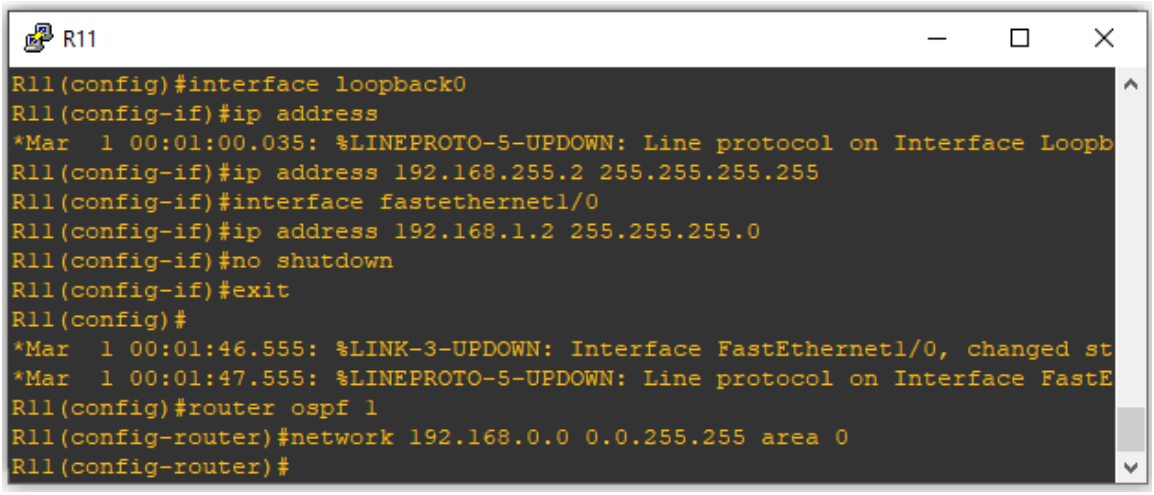

Рисунок 3.10 – Конфігурування CE-маршрутизатора VPN_A2

3.3.2 Конфігурування MPLS на маршрутизаторах провайдера

В режимі глобальної конфігурації необхідно запустити CEF на всіх маршрутизаторах провайдера з допомогою команди *ip cef*. CEF-комутація є невід'ємним елементом функціонування технології MPLS. Сам MPLS запускається командою *mpls ip*. Команду *mpls ip* необхідно також застосувати для кожного інтерфейса окремо.

Ідентифікатором маршрутизатора (Router ID) для Label Distribution Protocol (LDP) можуть використовуватися IP-адреси фізичних інтерфейсів. А саме, найбільша IP-адреса одного із інтерфейсів. Оскільки фізичні інтерфейси є вразливими до збоїв, в якості Router ID доцільно застосувати інтерфейс loopback. Для того, щоб задати loopback-інтерфейс як router ID для LDP, використовується команда *mpls ldp router-id loopback0 force* в режимі глобальної конфігурації. Ключовим словом є *force*, адже без нього Router ID зміниться лише при перевстановленні з'єднання LDP. Приклад повної конфігурації для маршрутизатора R1продемонстровано на рисунку 3.11.

Рисунок 3.11 – Запуск MPLS

Після активація протокола LDP маршрутизатор починає з допомогою UDP розсилати повідомлення типу «Hello Message» на мультикастову адресу 224.0.0.2. Процес можна відстежити з допомогою Wireshark (рисунок 3.12).

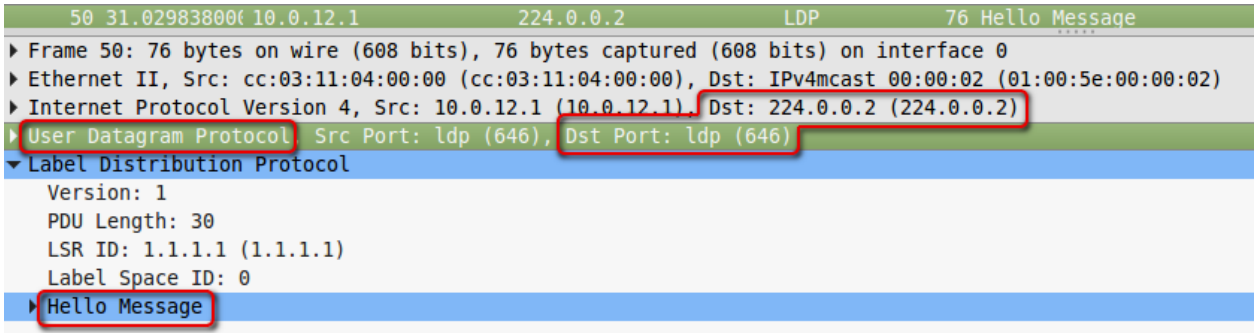

Рисунок 3.12 – Мультикастова розсилка Hello-повідомлень

Як тільки маршрутизатор виявляє сусіда, він піднімає з ним LDP-з'єднання. На рисунку 3.12 продемонстровано, як після виконання команди *mpls ip* на інтерфейсі, з'являється повідомлення про виявлення сусіда і встановлення з ним LDP-сесії (рисунок 3.13).

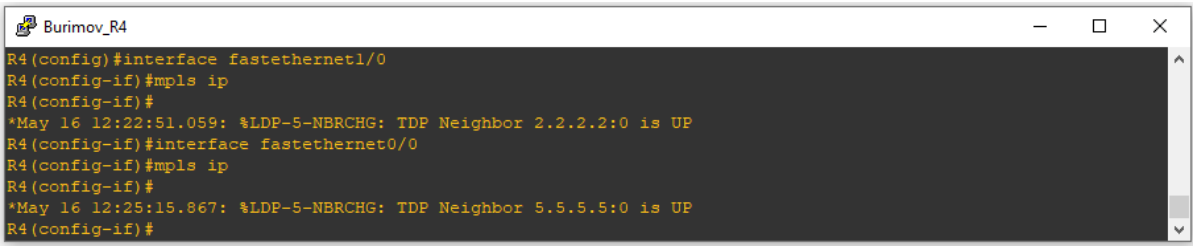

Рисунок 3.13 – Встановлення LDP-сесій

На даному етапі між всіма парами LSR побудовані LSP. Переглянути їх можна командою *show mpls ip binding* в таблиці LIB. Зокрема, дана команда демонструє мітки, які використовуються для передачі даних (рисунок 3.14).

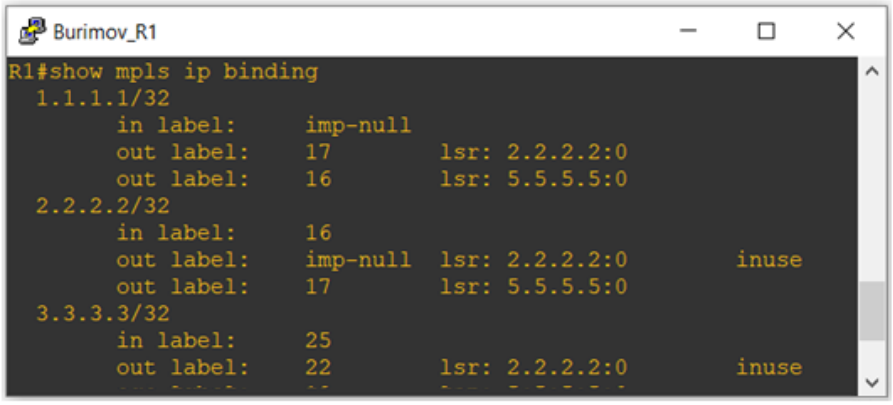

Рисунок 3.14 – Маршрути LSP між маршрутизаторами

Поле in label – містить вхідну мітку, параметр inuse вказує на те, що мітка зараз використовується для роботи, поле out label містить вихідну мітку, тобто мітку, отриману від маршрутизатора, ID якого виведено в поле lsr.

Переглянути сусідство маршрутизаторів можна з допомогою команди *show mpls ldp neighbor* (рисунок 3.15).

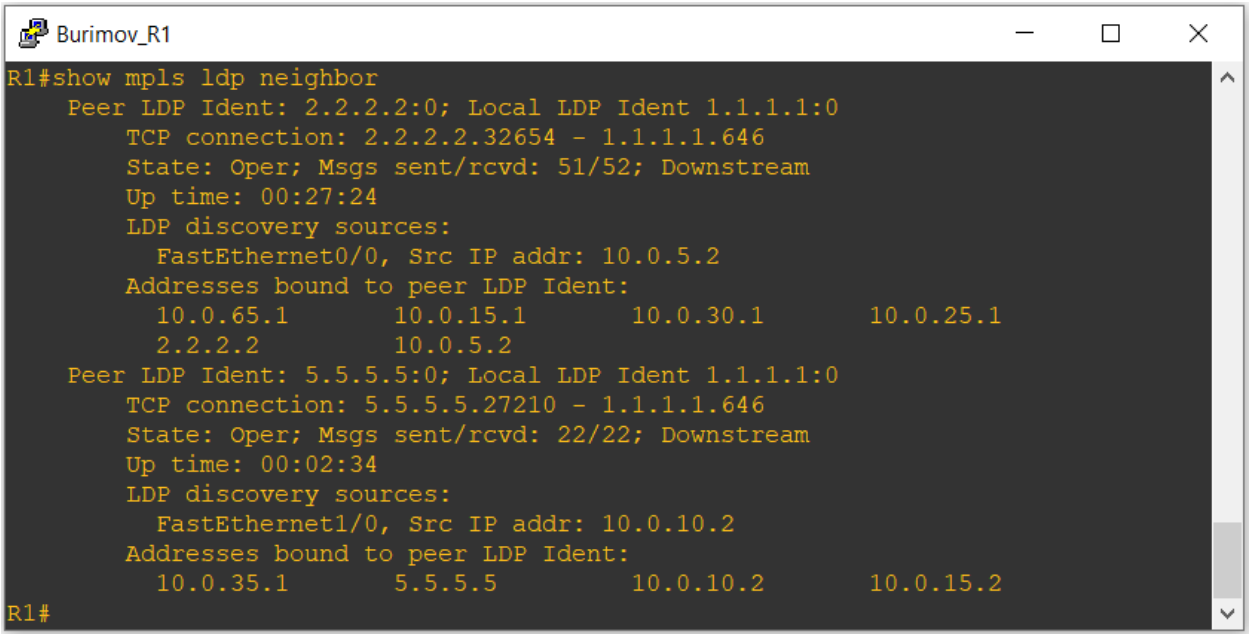

Рисунок 3.15 – Таблиця сусідів маршрутизатора R1

Опис полів при виводі даної команди наступний:

- Peer LDP Ident – ідентифікатор сусіда;
- Local LDP Ident – ідентифікатор маршрутизатора;
- TCP connection – містить інформацію про з’єднання TCP між локальним маршрутизатором і сусідом;
- State – стан з’єднання;
- Downstream – тип обміну мітками;
- Uptime – час існування сесії;
- Msgs sent/rcvd – кількість переданих пакетів;
- LSP discovery sources – інформація про доступність сусідів через інтерфейси;

3.3.3 Конфігурування комплексів VRF

Як уже говорилося раніше, технологія MPLS підтримує велику кількість VPN-мереж і характеризується надзвичайно високим ступенем розширюваності. Кожен користувач VPN-мережі логічно пов'язаний з комплексом маршрутизації і пересилання (VRF). Кожен VRF використовує і підтримує свою власну інформаційну базу маршрутизації (RIB) і Cisco Express Forwarding (CEF).

Спочатку необхідно створити VRF-комлекси на PE-маршрутизаторах: R1 і R4 для клієнта VPN_A, R10 і R12 для клієнта VPN_B. Для цього використовується команда *ip vrf {vrf-name}*. VRF-name – ім'я, що присвоюється комплексу VRF. Воно використовується для ідентифікації користувача служби VPN і повинно бути унікальним. Імена vrf-name чутливі до регістра. Усі CE-маршрутизатори користувача, під'єднані до PE-маршрутизатора, повинні мати визначені даним способом імена.

Наступним кроком буде створення таблиці маршрутизації і пересилання для користувачів мереж VPN з використанням Route Distinguisher. Задається даний параметр командою *rd {rd number}*.

Параметр RD додається в підрежимі VRF. Він має бути зконфігурований таким чином, щоб стало можливим функціонування VRF-комплекса. Параметр RD додає 64-бітне значення до 32-бітового префікса IPv4, в результаті чого створюється 96-бітовий VPN-префікс протоколу IP. RD вставляється перед початком префіксів протокола IPv4, перетворюючи їх в глобальні унікальні VPN-префікси протокола. Така структура дозволяє користувачам VPN-мереж використовувати однакові приватні схеми адресації IP.

Окрім параметра RD необхідно також задати параметр RT для направлення маршрутів в необхідний комплекс VRF. Для цього необхідно ввести команду *rout-target both {rt number}*. Rout Target для імпорта і експорта повинні бути однаковими. Для цього вказується ключове слово *both*. Номер

AS вказується довільним чином, проте потрібно пам’ятати, що вони не мають повторятися.

Виконуємо вказані вище команди для маршрутизатора R1 (рисунок 2.16), що межує з клієнтом VPN_A1.

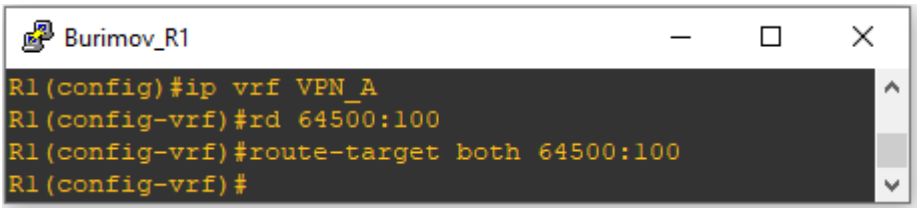

Рисунок 3.16 – Вказання признаків RT і RD для VPN_A1

Аналогічні дії виконуємо для маршрутизатора R4 (рисунок 3.17).

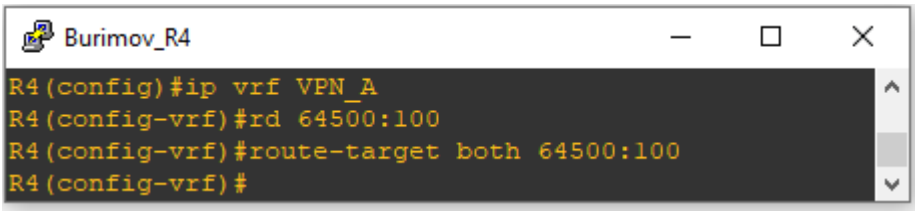

Рисунок 3.17 – Вказання признаків RT і RD для VPN_A2

Далі необхідно прив’язати інтерфейс (через який під’єднується мережа користувача) до комлекса VRF з допомогою команди *ip vrf forwarding {vrf-name}*. Цей етап є дуже важливим, оскільки служба MPLS логічно зв’язує фізичний інтерфейс з комплексом VRF. Логічне зв’язування інтерфейса з комлексом VRF призводить до видалення IP-адреси даного інтерфейсу. Після того як інтерфейсу буде призначено комплекс VRF, IP-адресу потрібно налаштувати повторно. Доцільно також застосовувати команду *description {description}* для опису процесу, що в подальшому полегшить процес аналізу конфігураційного файлу. Виконання команд на маршрутизаторі R1 показано на рисунку 3.18.

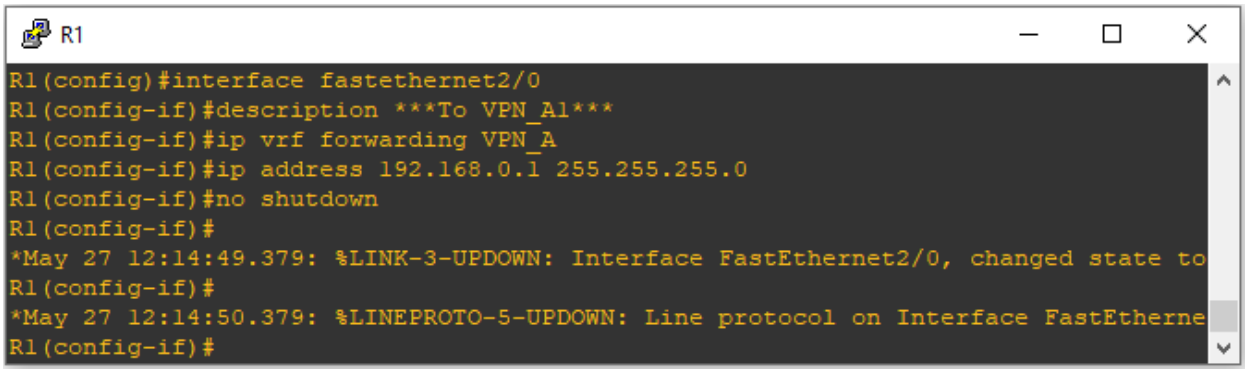

Рисунок 3.18 – Прив’язка інтерфейсів до VRF-комлексу на R1

Виконання команд на маршрутизаторі R4 показано на рисунку 3.19.

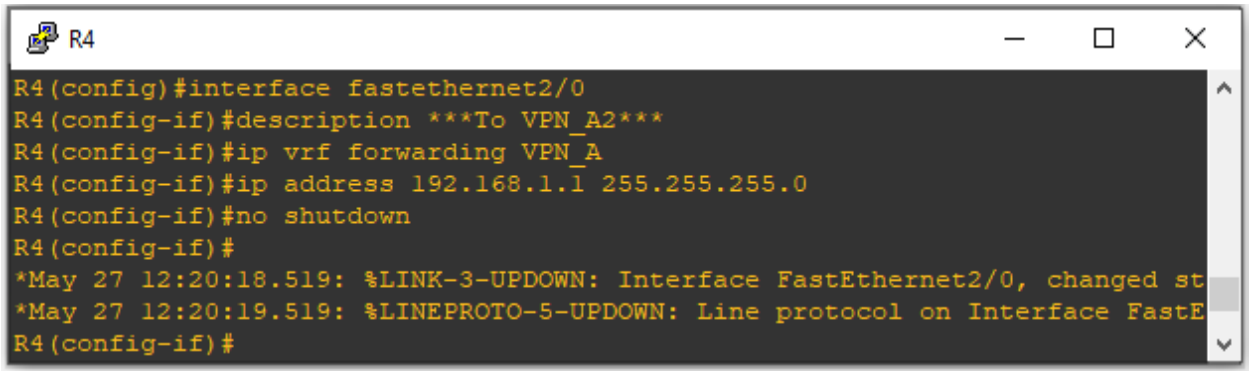

Рисунок 3.19 – Прив’язка інтерфейсів до VRF-комлексу на R4

Командою show ip route vrf VPN_A можна перевірити чи з’явилися налаштовані мережі (рисунок 3.20).

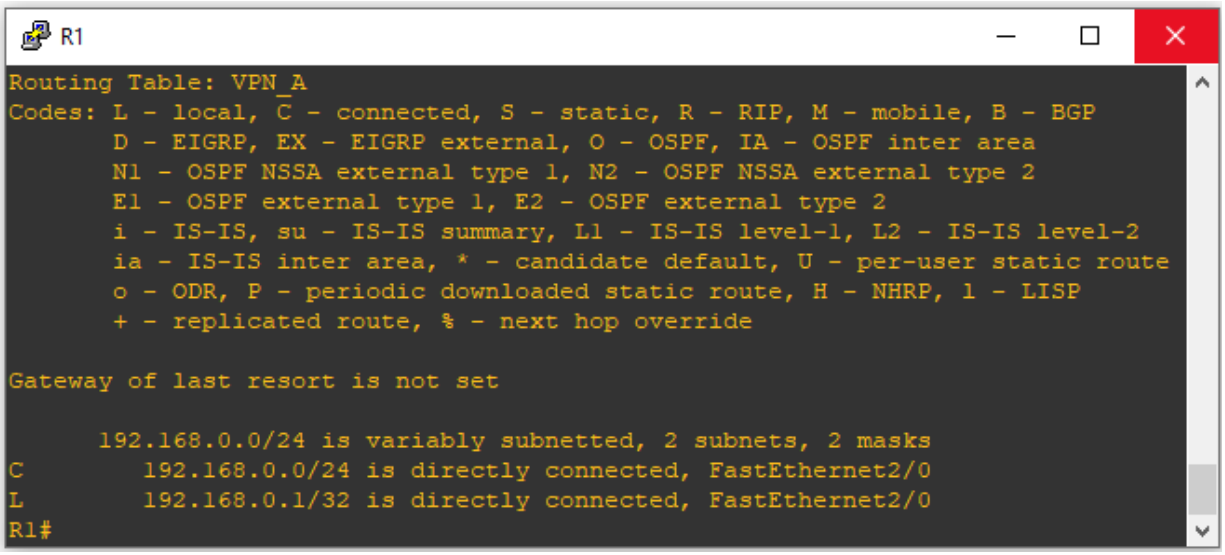

Рисунок 3.20 – Таблиця маршрутизації R1

Результат для маршрутизатора R4 продемонстровано на рисунку 3.21.

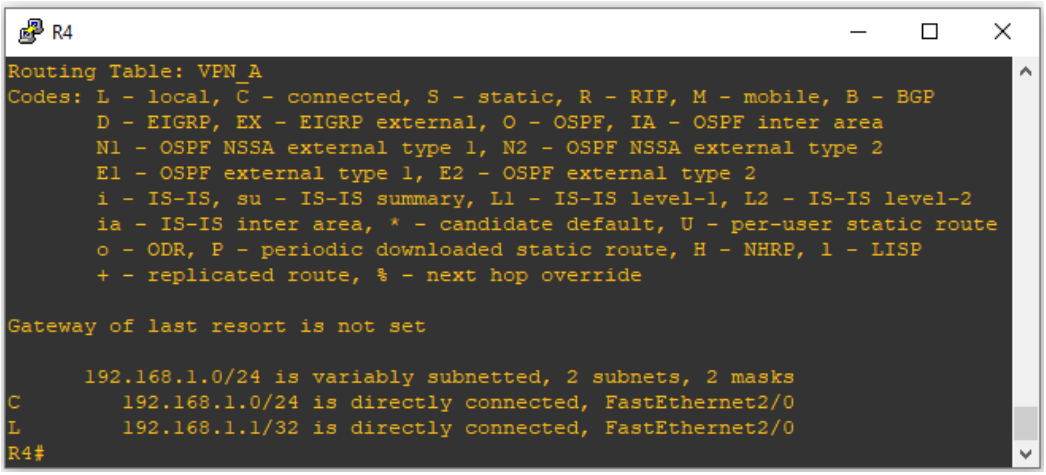

Рисунок 3.21 – Таблиця маршрутизації R4

Тепер необхідно підняти протокол маршрутизації з клієнтом. Оскільки передбачається, що клієнт у власній мережі використовує IGP-протокол OSPF, то і для комплексів VRF на PE-маршрутизаторах необхідно налаштувати OSPF. Даний процес ніяк не повинен перетинатися з процесами глобальної маршрутизації, саме тому його необхідно помістити в комплекс VRF з допомогою команди *router ospf 2 vrf {vrf-name}*.

Результат для маршрутизатора R1 (рисунок 3.22):

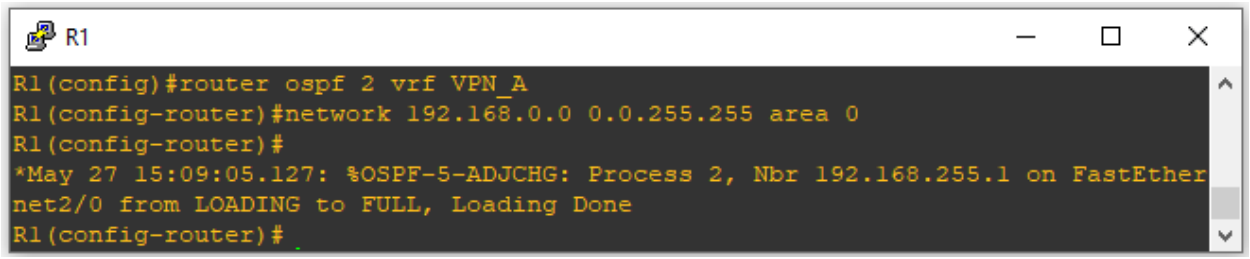

Рисунок 3.22 – Підняття протоколу OSPF на VRF VPN_A1

Результат для маршрутизатора R4 (рисунок 3.23):

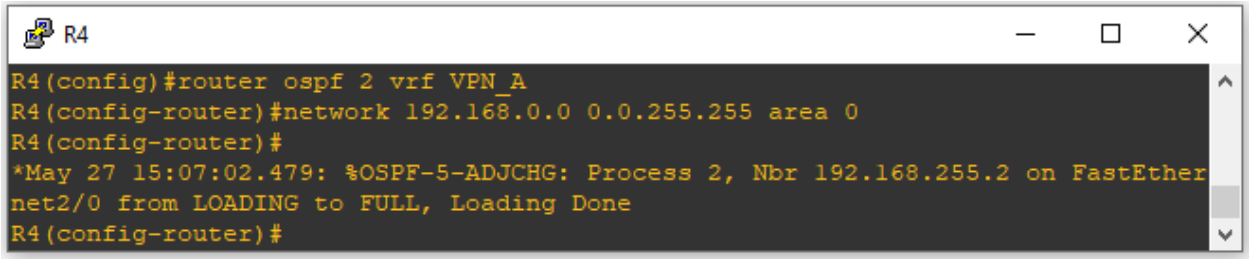

Рисунок 3.23 – Підняття протоколу OSPF на VRF VPN_A2

На маршрутизаторі запускаємо команду show ip route vrf VPN_A. Оскільки між маршрутизаторами CE і PE було запущено процес OSPF, в таблиці маршрутизації R1 з'являється loopback0 адреса клієнта (рисунок 3.24).

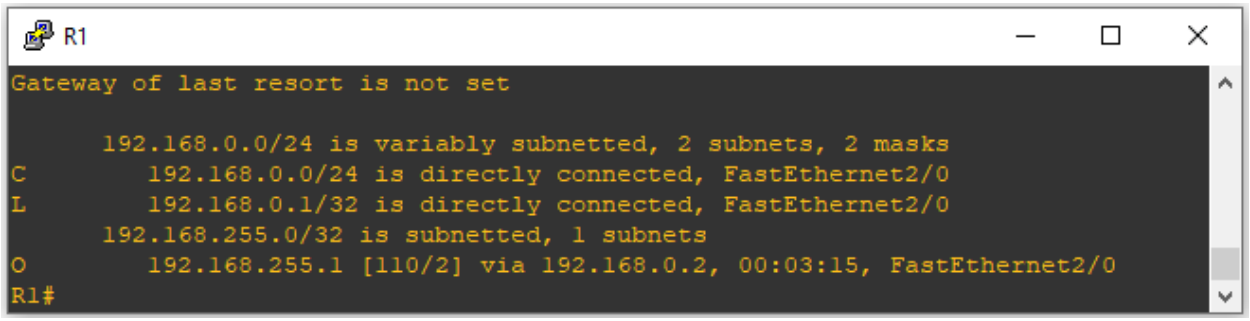

Рисунок 3.24 – Таблиця маршрутизації R1

Аналогічно і на маршрутизаторі R4 в таблиці маршрутизації з'явилася адреса loopback0 172.16.255.2/32. Як бачимо, маршрутизатор відслідковує loopback0 адресу 172.16.255.1, але не відслідковує віддалений loopback0 172.16.255.2. Це пов'язано з тим, що поки через мережу провайдера не передаються маршрути клієнта. І, відповідно, якщо ми з маршрутизатора CE_VPN_A1 спробуємо пропінгувати маршрутизатор CE_VPN_A2, то нічого не відбудеться (рисунок 3.23).

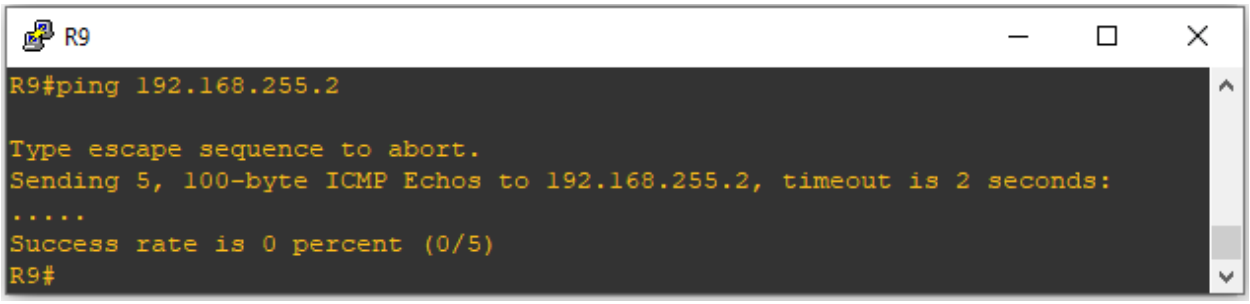

Рисунок 3.25 Пінгування CE_VPN_A2

3.3.4 Налаштування MBGP в мережі провайдера

Для активації MBGP на PE-маршрутизаторах необхідно виконати наступні дії.

Етап 1. Зконфігурувати процес маршрутизації iBGP з передачею номера автономної системи іншим PE- маршрутизаторам iBGP командою *router bgp autonomus-system*. Як уже говорилося раніше, номер автономної системи може бути довільним. В даному випадку буде використовуватися 64500. Командою *neighbor {ip address} remote-as {number}* необхідно задати IP-адресу сусіднього PE-маршрутизатора, ідентифікуючи її тим самим для локальної автономної

системи. Командою *neighbor {ip address} update-source loopback0* ми вказуємо адресу, яка буде джерелом розсилки пакетів.

Етап 2. Налаштування Address Family VPNv4. Це дозволить маршрутизаторам R1 і R4 передавати клієнтські маршрути. Для цього необхідно використати команди *address-family vpnv4* і *neighbor {ip address} activate*. Необхідно також активувати передачу community командою *neighbor {ip address} send-community both*. Цей атрибут використовується RT.

Етап 3. Необхідно задати Address Family для конкретного комплексу VRF командами *address-family ipv4 vrf {vrf name}* (працює зі звичайними IPv4 але з VRF-комплексу VPN-A). Командами *redistribute connected* і *redistribute ospf 2 vrf VPN_A* налаштовуються імпорт маршрутів із процесу OSPF з номером 2.

Етап 4. Необхідно налаштувати імпорт маршрутів в OSPF із BGP командами *router ospf 2* і *redistribute bgp 64500 subnets* (де 64500 – номер автономної системи провайдера, з якої відбувається імпорт маршрутів).

Результат для маршрутизатора R1 (рисунок 3.26):

Рисунок 3.26 - Налаштування MBGP на R1

Аналогічні дії виконуємо і з маршрутизатором R4. Результат для маршрутизатора R4 (рисунок 3.27):

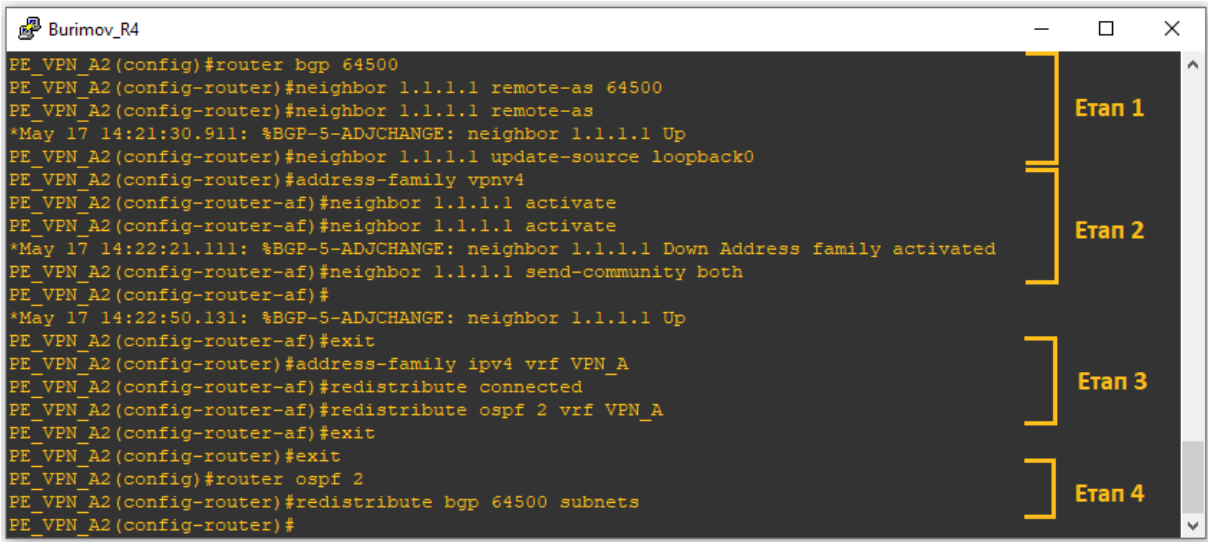

Рисунок 3.27 – Налаштування MBGP на R2

3.3.5 Дослідження зконфігурованої мережі

Таблиця маршрутизації CE-маршрутизатора клієнта VPN_A1 має наступні записи:

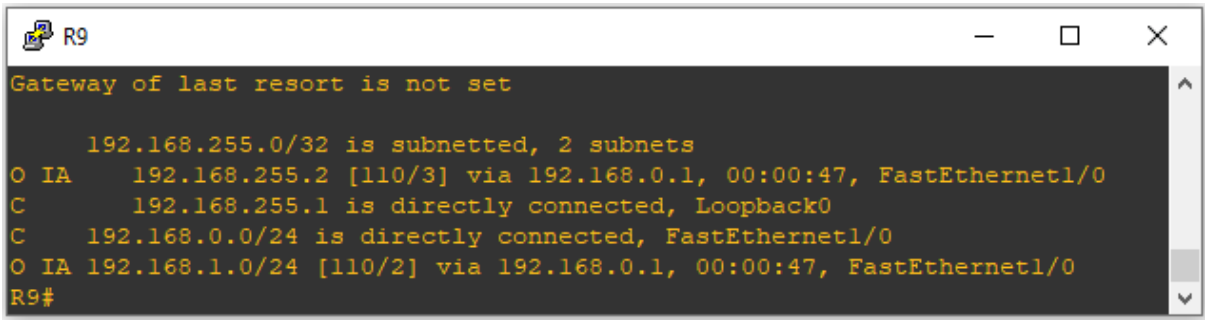

Рисунок 3.28 - Таблиця маршрутизації CE_VPN_A1

Як бачимо, вона містить інформацію про маршрути до мережі 192.168.1.0/24, але при цьому не має жодної інформації про маршрути мережі провайдера.

Аналогічно і для CE-маршрутизатора клієнта VPN_A2:

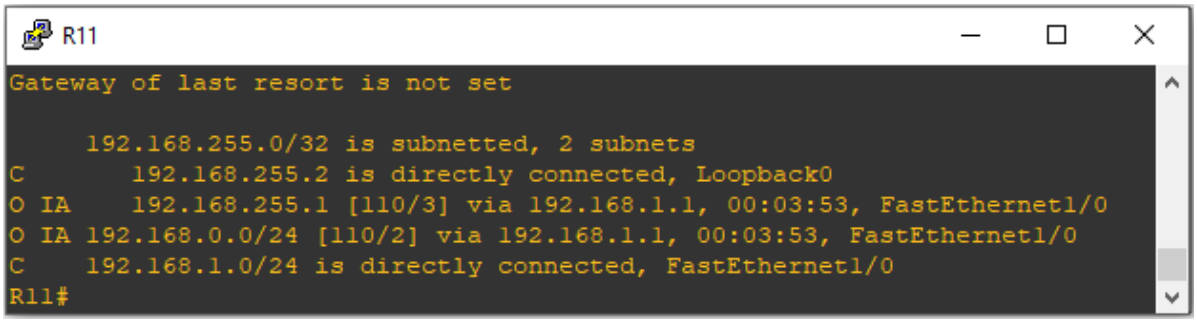

Рисунок 3.29 - Таблиця маршрутизації CE_VPN_A2

З допомогою утиліти Ping спробуємо пропінгувати з маршрутизатора CE_VPN_A1 маршрутизатор CE_VPN_A2. Результат:

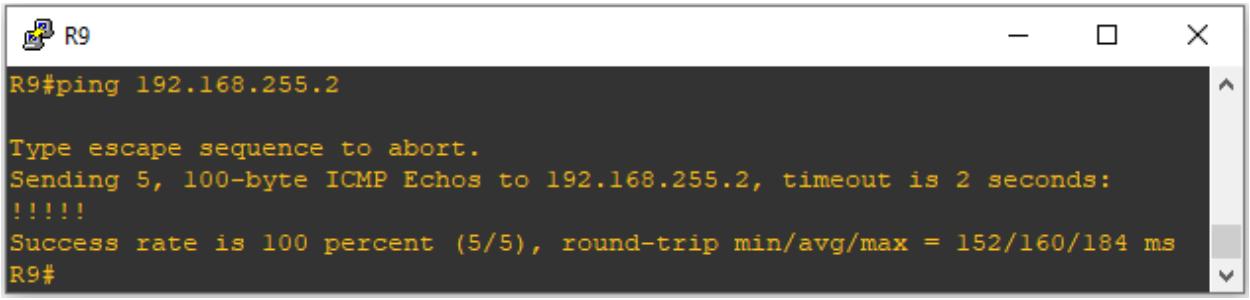

Рисунок 3.30 - Пінгування VPN_A2

Пінг пройшов вдало, а отже всі налаштування VRF-комлексів було виконано правильно. Мережі клієнтів бачать одна одну і можуть обмінюватися інформацією. Спробуємо пропінгувати loopback0 адресу провайдерського маршрутизатора R1 з клієнтського маршрутизатора CE_VPN_A1. Результат:

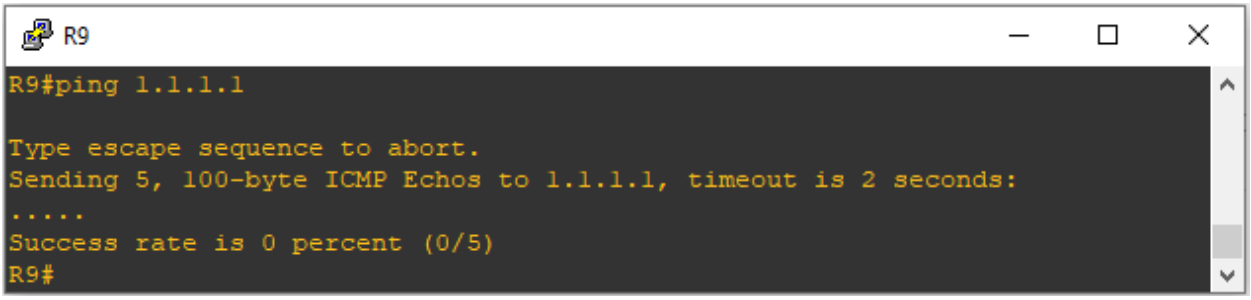

Рисунок 3.31 – Пінгування машрутизатора R1

Як бачимо, пінг не пройшов. Як говорилося раніше, клієнт не повинен бачити мережу провайдера, що, згідно із технічним завданням, було однією із умов конфігурування мережі VPN MPLS.

З допомогою команди traceroute {ip-address} можна переглянути маршрут, який проходить IP-пакет. Зокрема, можна також побачити транспортну та сервісні мітки для даного пакета (рисунок 3.32).

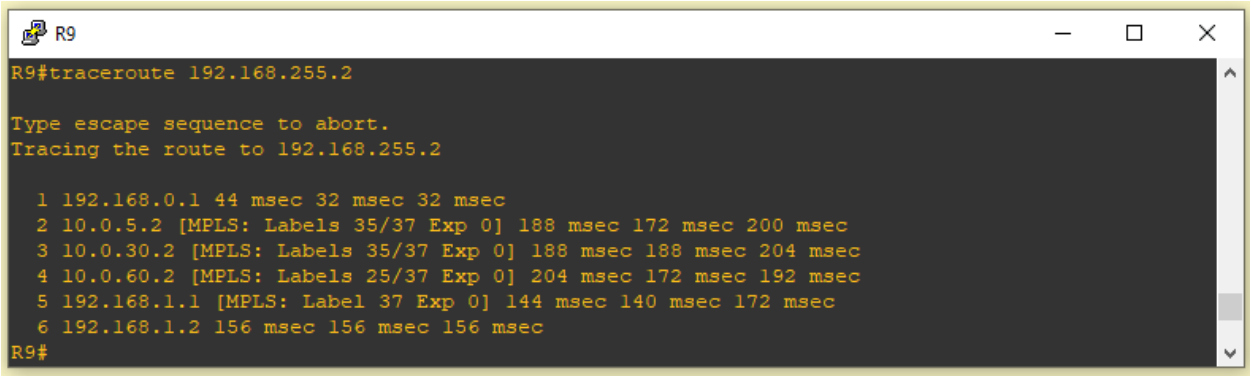

Рисунок 3.32 – Трасування маршруту до користувача VPN_A2

3.3.6 Підключення клієнта по BGP

При постановці технічного завдання було вказано, що мережа повинна передбачати можливість підключення клієнта не тільки по протоколам IGP, а і по протоколу BGP. Протокол BGP призначений для обміну інформацією про досяжності підмереж між автономними системами (АС, англ. AS - autonomous system), тобто групами маршрутизаторів під єдиним технічним і адміністративним управлінням, що використовують протокол IGP для визначення маршрутів всередині себе і протокол EGP для визначення маршрутів доставки пакетів в інші АС. Передана інформація включає в себе список АС, до яких є доступ через дану систему.

Для цього виконаємо налаштування VPN-мережі для клієнта VPN_B. Приклади базового конфігурування (задання ip-адрес, налаштування комплексів VRF, налаштування MP-BGP) наводитися не будуть, адже вони ідентичні тим, що виконувалися для клієнта VPN_A (конфігураційний файл маршрутизаторів клієнта VPN_B надано в додатку 1). Єдина відмінність буде полягати в тому, що маршрути будуть передаватися по BGP. Інакше кажучи, необхідно підняти EBGP з клієнтським маршрутизатором (рисунок 3.31).

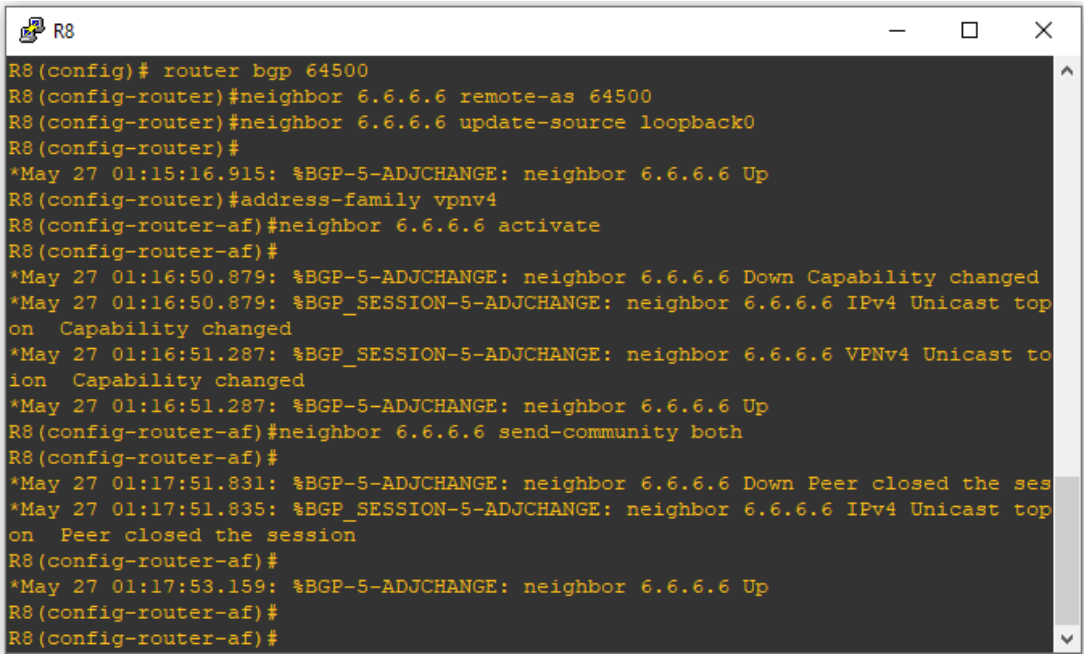

Рисунок 3.33 – Приклад налаштування BGP на PE2-маршрутизаторі

На CE-маршрутизаторах EBGP налаштовується з допомогою наступних команд (рисунок 3.34):

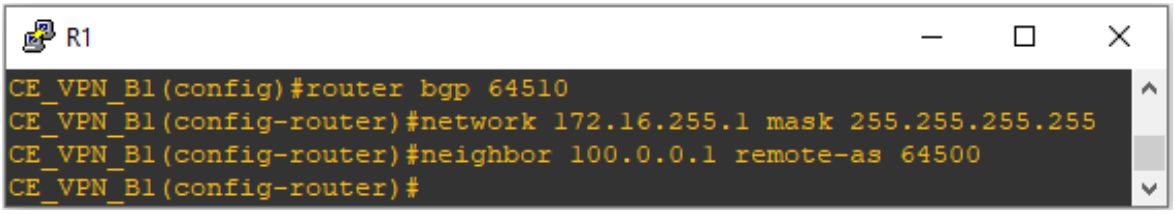

Рисунок 3.34 – Налаштування EBGP на CE

Для CE_VPN_B2 налаштування виконуються аналогічно. Даними командами було вказано, що CE_VPN_B1 буде анонсувати свою мережу 172.16.255.1/32.

Таблиця маршрутизації маршрутизатора CE_VPN_B1 (рисунок 3.35):

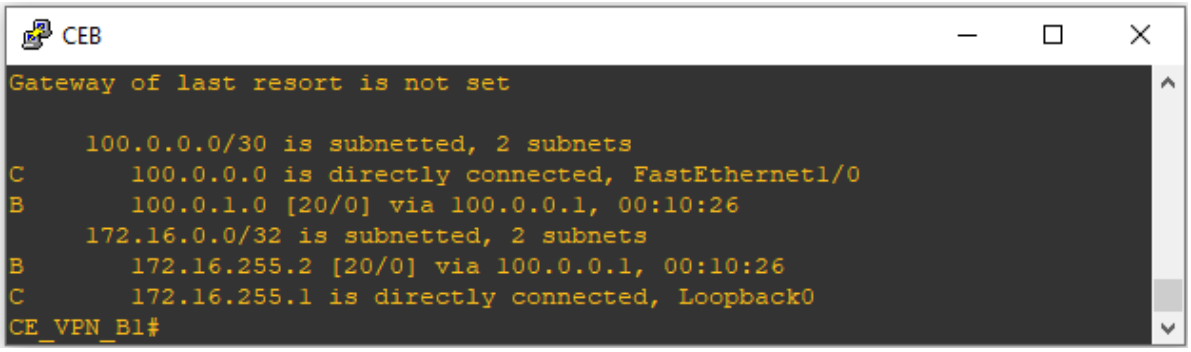

Рисунок 3.35 – Таблиця маршрутизації CE_VPN_B1

Пінгуємо маршрутизатор CE_VPN_B2 (рисунок 3.36):

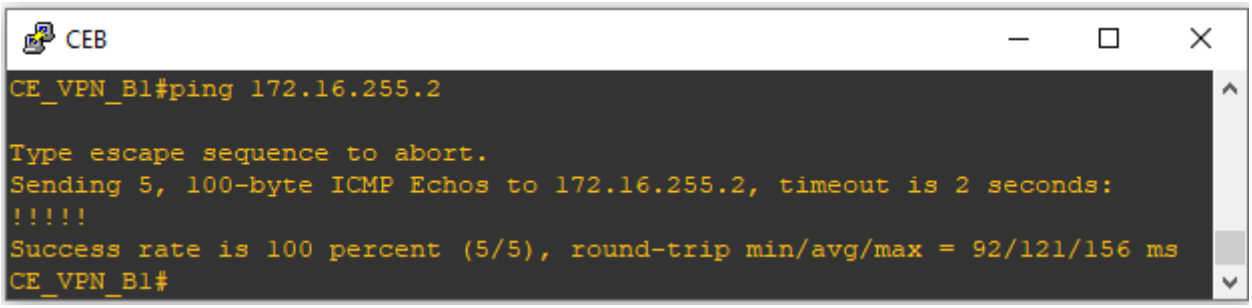

Рисунок 3.36 - Пінгування VPN_A2

Пінг пройшов вдало, а отже всі налаштування VRF-комлексів було виконано правильно. Мережі клієнтів бачать одна одну і можуть обмінюватися інформацією.

3.4 Висновки до розділу

В даному розділи виконувалися налаштування мережі MPLS L3 VPN, згідно з наступним алгоритмом:

- Етап 1. Конфігурування інтерфейсів мережі провайдера і користувача (лінкові та loopback) і протоколу IGP.
- Етап 2. Налаштування MPLS (на основі протоколу LDP).
- Етап 3. Конфігурування комплексів VRF.
- Етап 4. Налаштування MP-BGP в мережі провайдера.
- Етап 5. Дослідження зконфігурованої мережі.

У результаті було отримано повністю працездатну мережу провайдера на базі технології MPLS, що підтримує дві VPN-мережі клієнтів (VPN_A і VPN_B). Спроби пропінгувати робочі станції з одного VPN в інший результатів не дали, проте робочі станції в межах однієї VPN-мережі пінгуються без проблем. Це свідчить про те, що всі налаштування було виконано правильно, і кожна мережа VPN є ізольованою одна від одної.

ВИСНОВКИ

Технологія VPN MPLS на сьогоднішній день є провідною технологією побудови віртуальних приватних мереж. Вона володіє широкою масштабністю, гнучкістю, що не накладає жодних обмежень на протоколи вищого рівня, а застосування міток для комутації в мережі провайдера MPLS дозволяє реалізувати прискорену передачу трафіку по магістральній мережі.

В результаті виконання атестаційної випускної роботи була спроектована і налаштована модель мережі провайдера на базі технології MPLS з підтримкою двох віртуальних приватних мереж.

Також було вирішено наступні задачі:

- Виконано аналіз існуючих рішень на основі якого було зроблено вибір на користь технології MPLS L3 VPN;
- Детально розглянуто та досліджено однорангову модель VPN, яка реалізовується в даній роботі;
- Детально розглянуто технологію MPLS;
- Визначено основні переваги технології MPLS L3 VPN та доцільність її застосування в сучасних мережах провайдерів;
- Розроблена мережа провайдера на основі технології багатопротокольної комутації по міткам з підтримкою двох клієнтів. Забезпечено надійний захист клієнтських даних від несанкціонованого використання – як з боку інших клієнтів, так і з боку провайдера;
- Мережа налаштована таким чином, що у випадку підключення нових клієнтів з приватними адресами вона буде так само ефективно функціонувати і однакові приватні адреси в мережі не будуть створювати колізій;

Таким чином, в результаті вирішення вказаних задач можна стверджувати, що поставлена в випускній кваліфікаційній роботі мета була досягнута.

ДЖЕРЕЛА ПОСИЛАНЬ

1. Cisco 2018 annual cybersecurity report. URL: https://www.cisco.com/c/dam/m/hu_hu/campaigns/security-hub/pdf/acr-2018.pdf (дата звернення: 08.06.2021).

2. Executive summary cisco 2018 asia pacific security capabilities benchmark study. URL: https://www.cisco.com/c/dam/global/en_au/products/pdfs/executive_summary_cisco_2018_asia_pacific_Security_capabilities_benchmark_study.pdf (дата звернення: 08.06.2021).

3. PandaLabs 2018 annual report. URL: https://partnernews.pandasecurity.com/uk/src/uploads/2018/12/PandaLabs-2018_Annual_Report-uk.pdf (дата звернення: 08.06.2021).

4. Vacca J. R. Computer and information security handbook. Amsterdam; Boston : Elsevier, 2009.

5. Specht D. F. Generation of Polynomial Discriminant Functions for Pattern Recognition. IEEE Transactions on Electronic Computers. 1967. EC-16, № 3. С. 308–319. URL: https://doi.org/10.1109/pgec.1967.264667 (дата звернення: 09.06.2021).

6. What is windows forms - windows forms .NET. Developer tools, technical documentation and coding examples | Microsoft Docs. URL: https://docs.microsoft.com/enus/dotnet/desktop/winforms/overview/?view=netdesktop-5.0#:~:text=Windows%20Forms%20is%20a%20UI,easy%20to%20build%20desktop%20apps. (дата звернення: 02.06.2021).

7. A detailed analysis of the KDD CUP 99 data set / M. Tavallaee та ін. 2009 IEEE symposium on computational intelligence for security and defense applications (CISDA), м. Ottawa, ON, Canada, 8—10 лип. 2009 р. 2009. URL: https://doi.org/10.1109/cisda.2009.5356528 (дата звернення: 08.06.2021).

8. Özgür A., Erdem H. A review of KDD99 dataset usage in intrusion detection and machine learning between 2010 and 2015. PeerJ preprints. 2016. С. 1. URL: https://peerj.com/preprints/1954/ (дата звернення: 08.06.2021).

9. Baestaens D. E. Neural network solutions for trading in financial markets. London : Financial Times, 1994. 245 c.

10. Benchmarking datasets for anomaly-based network intrusion detection: KDD CUP 99 alternatives / A. Divekar та ін. 2018 IEEE 3rd international conference on computing, communication and security (ICCCS), м. Kathmandu, 25—27 жовт. 2018 р. 2018. URL: https://doi.org/10.1109/cccs.2018.8586840 (дата звернення: 08.06.2021).

11. Chaudhuri S., Madigan D., Fayyad U. Kdd-99. ACM SIGKDD explorations newsletter. 2000. Т. 1, № 2. С. 49—51. URL: https://doi.org/10.1145/846183.846194 (дата звернення: 02.06.2021).

12. Vinod Nair, Geoffrey E. Hinton. Rectified Linear Units Improve Restricted Boltzmann Machines // 27th International Conference on International Conference on Machine Learning. — USA: Omnipress, 2010. — С. 807–814. — (ICML'10).

13. Savchenko A. Probabilistic neural network with complex exponential activation functions in image recognition. IEEE transactions on neural networks and learning systems. 2020. Т. 31, № 2. С. 651—660. URL: https://doi.org/10.1109/tnnls.2019.2908973 (дата звернення: 08.06.2021).

14. Kyurkchiev N., Markov S. Sigmoidal functions: some computational and modelling aspects. Biomath communications. 2015. Т. 1, № 2. URL: https://doi.org/10.11145/j.bmc.2015.03.081 (дата звернення: 08.06.2021).

15. Mitchell T. M. Machine learning. New York : McGraw-Hill, 1997. 414 с.

16. Probabilistic logics and probabilistic networks / J. Williamson та ін. Springer, 2013. 155 с.

17. Probabilistic and General Regression Neural Networks. DTREG. URL: http://www.dtreg.com/pnn.htm (дата звернення: 07.06.2021).