ЗМІСТ

ДОДАТКИ

Додаток 1. Копії графічних матеріалів

- ІАЛЦ.467200.005 Д1. Модель MPLS-VPN. Схема структурна
- ІАЛЦ.467200.006 Д2. LSP-тунель. Схема структурна
- ІАЛЦ.467200.007 Д3. Налаштування мережі VPN. Схема алгоритму
- ІАЛЦ.467200.008 Д4. Комутація за мітками в мережі MPLS. Схема алгоритму

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ, ТЕРМІНІВ

ПЗ – програмне забезпечення

SQL – Structured Query Language

MPLS – MultiProtocol Label Switching – багатопротокольна комутація за мітками;

ATM – Asynchronous Transfer Mode – технологія асинхронної передачі даних;

FEC – Forwarding Equivalence Class – клас еквівалентності передачі;

LER – MPLS edge router – граничний вузол мережі MPLS;

LSP – Label Switching Path – комутований за мітками тракт;

IGP – Interior Gateway Protocol – вид протоколу для зміни інформації, що надсилається між шлюзами та автономною системою.

OSPF – Open Shortest Path First – протокол динамічної маршрутизації;

LSR – Label Switching Router – маршрутизатор комутації за мітками;

OSI – Open Systems Interconnection model – базова еталонна модель взаємодії відкритих систем;

ER-LSP – explicitly routed LSP – LSP з явно заданим маршрутом;

ВСТУП

За останні роки було зроблено багато спроб використати багатопротокольну комутацію за мітками (MPLS), що значно вплинуло на використання IP-мереж.

MPLS (Multi-Protocol Label Switching) - це технологія мережі стандартизації в IETF, основне призначення яких об'єднати поняття IP-маршрутизації 3 рівня і механізми комутації 2 рівня, так як реалізовано в ATM / Frame Relay. MPLS повинна дозволити поліпшити співвідношення продуктивності і ціни обладнання, маршрутизації, підвищення ефективності маршрутизації (зокрема, для великих мереж) і збагатити служби маршрутизації (будуть прозорими для нових послуг та механізмів перемикання міток, вони можуть бути розгорнуті без змін на основі мережі).

IETF працює сьогодні на Ipv4. Проте, метод MPLS може працювати на кілька інших протоколів (IPv6, IPX, AppleTalk, та ін,). MPLS жодним чином не обмежує в 2 рівні і може працювати на всіх типах протоколів для маршрутизації пакетів 3 рівня.

MPLS обробляє перемикання в режим "підключено" (на основі міток); таблиці перемикання, розрахованих на інформації з протоколів маршрутизації IP і протоколи управління. MPLS можна розглядати як інтерфейс, приносячи IP в режим "підключено", які використовують сервіси 2-го рівня (PPP, ATM, Ethernet, ATM, Frame Relay, SDH ...).

Технологія MPLS відносно проста, але модульна і дуже ефективна. Деякі ключові моменти висунуто IETF і великих виробників таких як Cisco, а також постачальників послуг на перші місці з яких мережі операторів. Великі зусилля, щоб привести до нормалізації була зроблені різними суб'єктами, що привело до революції в IP-мережі.

MPLS являє собою технологію, з якою у перспективі будуть працювати більшість IP-мереж, у тому числі Internet. Використання технології MPLS надає мережі Internet новий принцип передачі пакетів, що впливає на перерозподіл потоків даних та на реалізацію віртуальних приватних мереж, а також дозволяє провайдерам більш ефективно забезпечувати задану якість обслуговування[1, 2].

Технологія MPLS дозволяє інтегрувати мережі IP і ATM, за рахунок чого постачальники послуг зможуть не тільки зберегти кошти, інвестовані в обладнання асинхронної передачі, але і отримати додаткову вигоду зі спільного використання цих протоколів.

1. АНАЛІЗ ІСНУЮЧИХ РІШЕНЬ ТА ОБҐРУНТУВАННЯ ТЕМИ ДИПЛОМНОГО ПРОЕКТУ

1.1. **Технологія з комутацією каналів**

технологія, при якій з'єднання встановлюється перед початком передачі даних. Щоб було зрозуміліше, то це, фактично, і є виділені лінії. Коли між двома віддаленими вузлами потрібно встановити з'єднання і передати дані, то часто використовують, як раз, виділені лінії. У таких випадках можна використовувати Інтернет і створити віртуальний канал VPN (на основі PPTP або openvpn), а можна орендувати «виділенку» і використовувати протокол PPP (point-to-point protocol) або закритий протокол Cisco, HDLC (high-level data link control). У другому випадку говорять, що використовується комутація каналів. Між маршрутизаторами налаштовується постійне з'єднання і потім здійснюється передача даних. Технологія працює на першому рівні моделі OSI (L1).

Які особливості технології комутації каналів.

-Зменшена кількість службової інформації (не передається адреса джерела і призначення, бо немає необхідності в цьому при двухточечных каналах).

-Комутація каналів може використовуватися на базі як цифрових, так і аналогових мережах (можна побудувати з'єднання поверх Ethernet, а можна і через телефонну лінію).

-Постійна швидкість передачі і висока стабільність каналу.

-Нераціональне використання пропускної здатності каналу (пропускної здатності каналу могло б вистачити більше, ніж на двох абонентів).

-Можлива відмова у встановленні з'єднання (при перевищенні кількості інформаційних потоків).

-Обов'язкова затримка перед передачею даних (через встановлення з'єднання).

Як видно, комутація каналів має і позитивні (1-3), і негативні сторони (4-6). Приклад комутації каналів зображено на рис.1.

Рис. 1. Комутація каналів

1.2. **Технологія з комутацією пакетів**

технологія, при якій дані розбиваються на пакети певного розміру, які містять в собі адресу джерела та адресу призначення. На відміну від технології комутації каналів, комутація пакетів здійснює динамічну передачу даних абонентів, адреси яких беруться з отриманих комутаційним обладнанням пакетів. В якості такого обладнання виступають комутатори.

В залежності від протоколу, який використовується в WAN мережі, пакети обробляються різними комутаторами або одним комутатором, підтримує різні протоколи. Наприклад, в мережах MPLS використовуються комутатори, які можуть здійснювати комутацію по мітках, в мережах ATM використовуються ATM комутатори, які можуть обробляти клітинки і т. д. Особливістю такого устаткування є те, що воно має буферну пам'ять для тимчасового зберігання пакетів.Це дозволяє рівномірно передавати трафік між комутаційним обладнанням.

Таким чином, комутація пакетів – технологія доступу декількох абонентів до загальної мережі. При цьому по одній фізичній лінії дані можуть передаватися багатьма вузлами одноразово. Технологія працює на другому рівні моделі OSI (L2).

Особливості комутації пакетів.

-Ефективність використання смуги пропускання (абонент, який не використовує смугу, віддає її іншим).

-При великій кількості абонентів не буває відмови в обслуговуванні мережі (типу, лінія «зайнята»)

-Дані передаються відразу, без встановлення з'єднання (пакети передаються на комутаційне обладнання відразу після їх формування).

-Пакет може чекати своєї черги на відправку в буфері комутатора. Можлива втрата через переповнення буфера.

-Багато службової інформації в пакетах (включаючи адресацію)

-Складність комутаційного обладнання (мікропроцесорні пристрої).

-Працює тільки в цифрових мережах.

Так само, як і комутація каналів, комутація пакетів має свої переваги (1-3) і недоліки (4-7). Приклад комутації пакетів зображено на рис. 2

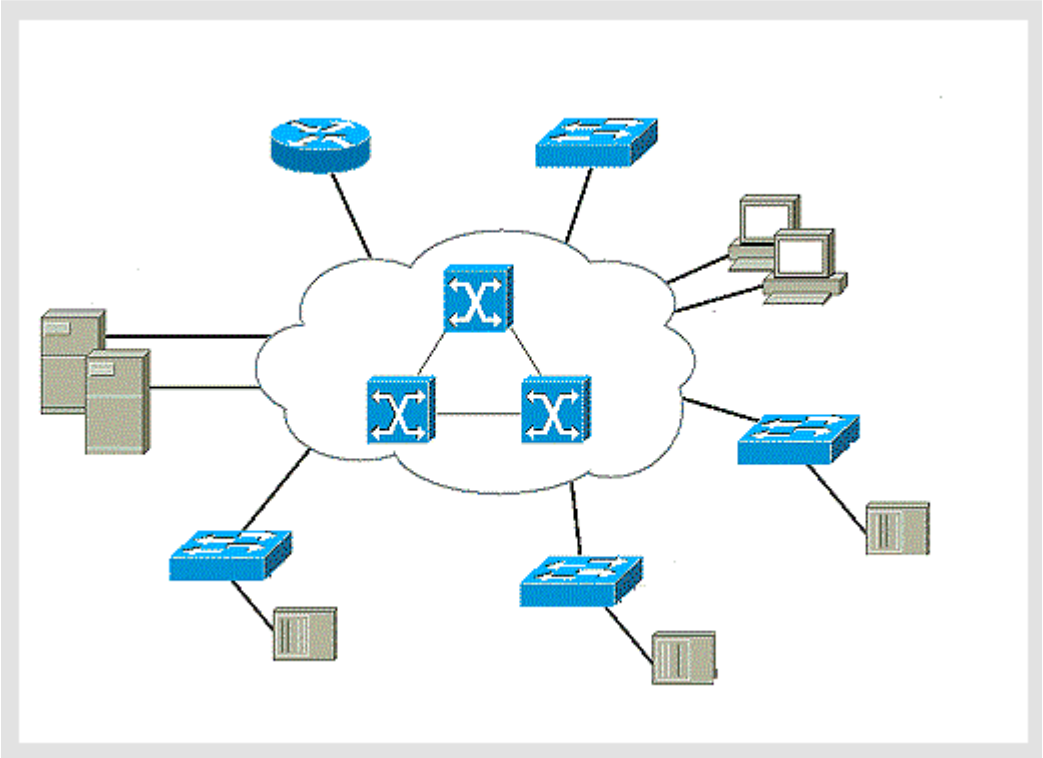


Рис. 2. Приклад комутації пакетів

1.3. **Технологія MPLS**

Технологія MPLS була розроблена для організації єдиного протоколу передачі даних як для додатків з комутацією каналів, так і додатків з комутацією пакетів (маються на увазі програми з дейтаграмному передачею пакетів). MPLS може бути використаний для передачі різного виду трафіку, включаючи IP-пакети, осередки ATM, фрейми SONET / SDH, і кадри Ethernet.

MPLS являє собою механізм з високопродуктивної телекомунікаційної мережі, який здійснює передачу даних від одного вузла мережі до іншого за допомогою міток. MPLS дозволяє досить легко створювати віртуальні канали між вузлами мережі. Так само дана технологія дозволяє інкапсулювати різні протоколи передачі даних.

Для вирішення ідентичних завдань раніше були розроблені такі технології як Frame Relay і ATM. Багато інженерів вважали, що технологія ATM буде замінена іншими протоколами з меншими накладними витратами на передачу даних і при цьому забезпечують передачу пакетів даних змінної довжини з встановленням з'єднання між вузлами мережі. Технологія MPLS розроблялася з урахуванням сильних і слабких сторін ATM. В даний час устаткування з підтримкою MPLS замінять на ринку обладнання з підтримкою згаданих вище технологій. Цілком можливо, що в майбутньому MPLS повністю витіснить дані технології. Зокрема MPLS обходиться без комутації осередків і набору сигнальних протоколів, характерних для банкоматів.

Мережа MPLS ділиться на дві функціонально різні області - ядро і граничну область. Ядро утворюють пристрої, мінімальною вимогою до яких є підтримка MPLS і участь в процесі маршрутизації трафіку для того протоколу, який комутується за допомогою MPLS. Маршрутизатори ядра займаються тільки комутацією. Всі функції класифікації пакетів з різних FEC, а також реалізацію таких додаткових сервісів, як фільтрація, явна маршрутизація, вирівнювання навантаження і управління трафіком, беруть на себе граничні LSR.

Багатопротокольність технологій MPLS полягає в тому, що вона дозволяє використовувати протоколи маршрутизації не тільки стека TCP/IP, а і любого іншого стека, наприклад IPX/SPX. В цьому випадку замість протоколів маршрутизації RIP IP, OSPF та IS-IS застосовується протокол RIP IPX або ж NLSP, а загальна архітектура LSR зостанеться такою ж. ПІд час розробки технології MPLS в середині 90-х років, коли на практиці функціонувало декілька стеків протоколів, така багатопротокольність вважалася важливою, проте сьогодні в умовах домінування стеку протоколів TCP/IP ця властивість не є важливою. Правда, сьогодні багатопротокльність MPLS можна розуміти по-іншому - як властивість передавати за допомогою з'єднання MPLS трафік різних протоколів канального рівня.

1.4. **Висновок**

Головна перевага MPLS в здатності надавати різноманітні транспортні послуги в IP-мережах, в першу чергу - послуги віртуальних приватних мереж. Ці послуги відрізняються різноманіттям, вони можуть подаватися як на мережевому, так і на канальному рівні. Крім того, MPLS доповнює IP-мережі такою важливою властивістю, як передача трафіку у відповідності з технікою віртуальних каналів, що дозволяє вибирати потрібний режим передачі трафіку в залежності від потреб послуги. Віртуальні канали MPLS забезпечує контроль трафіку, так як вони підтримують детерміновані маршрути.

2. ОСНОВИ MPLS

2.1. **Комутовані за мітками тракти LSP**

Комутований за мітками тракт (Label Switch Path, LSP) – це віртуальний комутований за мітками тракт, так званий тунель, який являє собою встановленне логічне з'єднання і є симплексним з'єднанням. Для організації напівдуплексного з'єднання необхідними є два LSP. LSP завжди починається на одному кінці домену MPLS і закінчується на протилежному, проходячи через кілька транзитних пристроїв (LSR).

Набір пакетів, що передається по LSP, відноситься до одного FEC, і кожен маршрутизатор LSR в LSP-тунелі призначає для нього свою мітку. LSP-тунель створюється всередині LSP-тракту. Слід зазначити, що дуже часто початок і кінець тунелю не співпадають з початком і кінцем LSP-тракту. Як правило, тунель коротший. Для кожного тунелю підраховується число пропущених пакетів і байт. Іноді потік даних може бути настільки великий, що для нього створюється декілька LSP-тунелів між відправником і одержувачем.

У одному LSP може бути створено декілька LSP-тунелів з різними точками прийому і передачі, а в кожному тунелі можуть бути створені LSP-тунелі іншого рівня. У цьому проявляється ієрархічність структури MPLS.

Можливі два варіанти створення тунелів: за принципом hop-by-hop, який передбачає, що кожен маршрутизатор самостійно обирає подальший шлях просування пакету, або за принципом явної маршрутизації, в якому маршрутизатори передають пакет відповідно до вказівок, отриманих від верхнього, в цьому тракті, LSR. Таким чином, в першому випадку маршрут прямування пакетів визначається випадковим чином, а у разі явної маршрутизації він відомий заздалегідь.

У мережі MPLS може існувати набір маршрутизаторів, які є вхідними для конкретного FEC, тоді, вважається, що для цього FEC існує LSP-тунель з

різними точками входу і виходу. Якщо для деяких з цих LSP вихідним є один і той же LER, то можна говорити про дерево LSP, коренем якого служить цей вихідний маршрутизатор.

LSP можна розглядати як тракт, що створюється шляхом зчеплення одного і більше ділянок маршруту, який дозволяє пересилати пакет, замінюючи на кожному вузлі мережі MPLS вхідну мітку вихідною міткою (так званий алгоритм перестановки міток).

Таким чином, тракт мережі MPLS можна розглядати як тунель, для створення якого в IP-дейтаграма вставляється заголовок - мітка, про який йшлося раніше.

LSP встановлюються або перед передачею даних (з управлінням від програми), або при виявленні певного потоку даних (керовані даними LSP).

На сьогодні застосування тунелювання реалізоване у багатьох технологіях. Утворення у віртуальному тракті тунелів, по яких проходять інші віртуальні тракти, ґрунтується на інкапсуляції пакетів, що передаються, в пакети, що прямують через цей тракт до цієї адреси призначення.

Логічно завершений домен мережі MPLS, представлено на рис. 3.

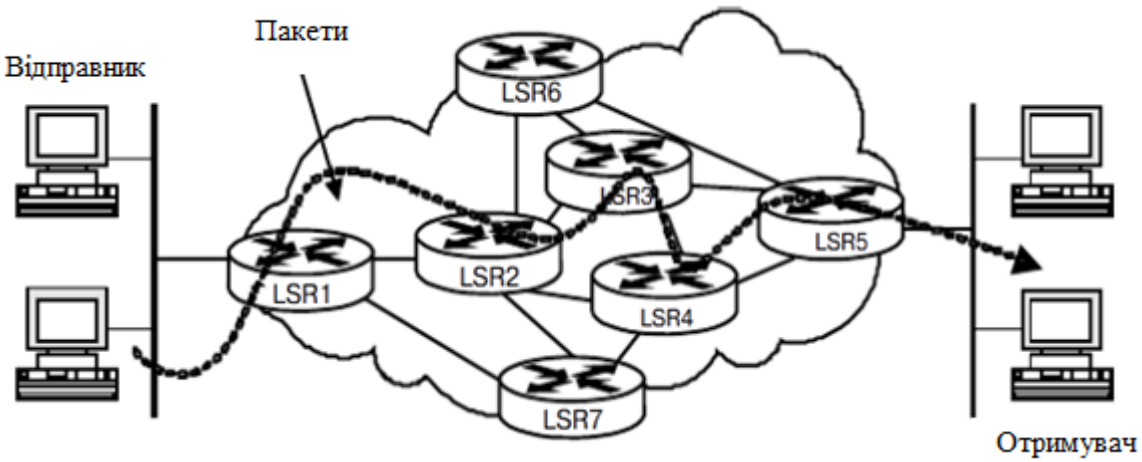


Рис 3. Приклад домена мережі MPLS

2.2. **Класи еквівалентних пересилок FEC**

FEC - це форма представлення групи пакетів з однаковими вимогами до передачі.

В заголовку IP-дейтаграми міститься значно більше інформації, ніж вимагається для вибору наступного маршрутизатора. Цей вибір можна організувати шляхом виконання наступних двох груп функцій в маршрутизаторі:

- маршрутизатор відносить пакет до певного класу FEC;
- ставить у відповідність кожному FEC наступний крок маршрутизації.

При традиційній IP-маршрутизації конкретний маршрутизатор теж 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 можливі маршрути транспортування цих двох пакетів співпадають найдовше. По мірі просування пакету через мережу кожен наступний маршрутизатор аналізує його заголовок і приписує цей пакет до такого з власних класів еквівалентності, який відповідає тому ж напряму.

На відміну 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 привласнюється мітка, що передається потім разом з пакетом при його пересилці до наступного маршрутизатора. У інших маршрутизаторах заголовок пакету не аналізується.

Визначення FEC реалізується на основі вимог до обслуговування цієї сукупності пакетів або просто адресного префікса. Таким чином, підводячи підсумок вищесказаного, можна дати наступне визначення FEC. Клас еквівалентності пересилки FEC - це форма представлення групи пакетів з

однаковими вимогами до їх передачі, тобто усі пакети такої групи обробляються однаково на шляху їх прямування до пункту призначення.

Клас FEC є набором FEC-елементів, кожен з яких ідентифікується певною міткою. На сьогодні існує всього два FEC-елементи: Address Prefix і Host Address.

При співвіднесенні пакетів різним FEC велику роль грають IP-адреси, пріоритети обслуговування і інші параметри трафіку. Кожен FEC обробляється окремо, що дозволяє підтримувати необхідну якість обслуговування в мережі MPLS. Спосіб пересилки пакетів на основі пар “FEC – мітка”, прийнятий в MPLS, має ряд переваг перед способами, ґрунтованими на аналізі заголовку блоків мережевого рівня. Зокрема, пересилку за способом MPLS можуть виконувати маршрутизатори, які здатні читати і замінювати мітки, але при цьому або взагалі не здатні аналізувати заголовки блоків мережевого рівня, або не здатні робити це досить швидко.

2.3. **Мітки і функціонування MPLS**

2.3.1. Мітка

Мітка - це ідентифікатор фіксованої довжини, що визначає клас еквівалентності пересилки FEC. Мітки мають локальне значення, тобто прив'язка мітки до FEC використовується тільки для пари маршрутизаторів. Мітка використовується для пересилки пакетів від верхнього маршрутизатора до нижнього, де, будучи вхідною, замінюється на вихідну мітку, що має також локальне значення на наступній ділянці шляху.

Мітка передається у складі будь-якого пакету, при цьому її місце в пакеті залежить від використовуваної технології канального рівня.

2.3.2. Комутація за мітками

З самого визначення MPLS видно, що мітки – основа основ цієї технології. Саме з мітками виконуються процедури їх розподілу за маршрутизаторам LSR і

процедури створення трактів LSP, за яким будуть слідувати пакети MPLS. Після розподілу міток і створення трактів LSP може виконуватися головна функція MPLS – пересилання забезпечених мітками пакетів по мережі MPLS. Крім цієї функції повинні вирішуватися і допоміжні завдання, пов'язані з мітками, а саме, контроль часу збереження міток, упорядкування місць і обробка помилок.

На рис. 4. представлено алгоритм комутації за мітками.

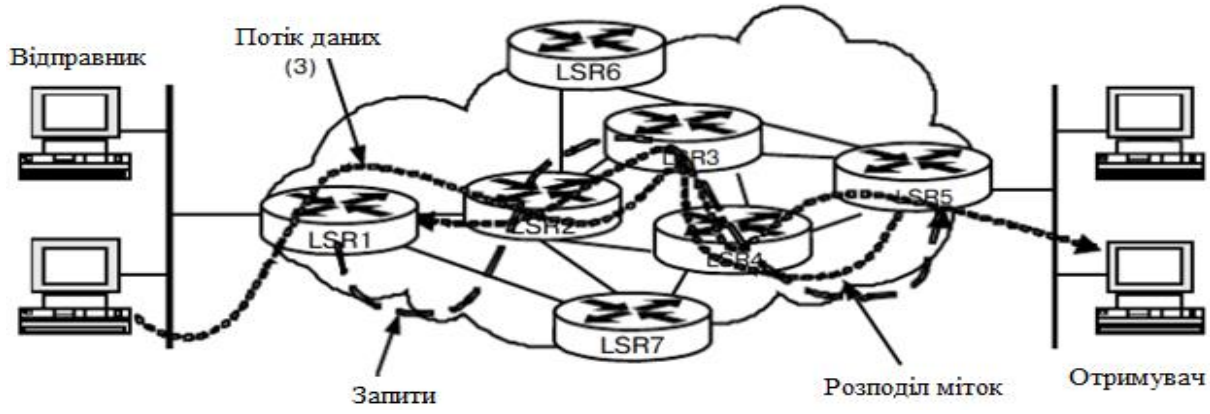


Рис. 4. Комутація за мітками в мережі MPLS

На основі рис. 4. розглянемо алгоритм комутації за мітками:

- Створення і розподіл міток.

До початку передачі через мережу MPLS пакетів трафіку будь-якого виду маршрутизатори LSR встановлюють відповідність між мітками і FEC в своїх таблицях. Крім того, проводиться узгодження характеристик трафіку та функціональних можливостей MPLS.

Значення міток можуть вибиратися і розсилатися або заздалегідь, до передачі даних (крива 2 на рис. 4.), або генеруватися як пакети, що належать надходить в мережу MPLS певного потоку даних або трафіку певного класу (крива 3). Ці два підходи до призначення міток, називаються, відповідно, призначенням з управлінням від програми і призначенням, керованим трафіком (даними).

- Створення таблиці в кожному LSR.

При отриманні даних про прив'язку міток до FEC кожен маршрутизатор LSR створює записи в таблиці LIB. Вміст таблиці відображає відповідність між

мітками і FEC і ставить у відповідність кожній парі “вхідний інтерфейс, вхідна мітка” пару “вихідний інтерфейс, вихідна мітка”. При будь-якому новому погодженні прив'язки міток до FEC, записи в таблиці оновлюються. Таблиці міток, згідно яким кожен пакет направляється відповідним трактом LSP, завжди повинні бути визначені до того, як пакет почне свій шлях мережею.

- Створення комутованого за мітками тракту LSP.

Як показано лінією 3 на рис. 4, тракти LSP створюються в напрямку, зворотньому створеним записам в таблицях LIB. Кожен LSR отримує мітку від нижчого маршрутизатора. LSP створюється шляхом послідовної маршрутизації по ділянках, а якщо потрібно оптимізація розподілу трафіку, для визначення тракту використовується протокол CR-LDP, що гарантує виконання вимог до QoS/CoS, або протокол RSVP-TE.

- Табличний пошук і інкапсуляція мітки в пакет.

Вхідний маршрутизатор (LSR1 на рис. 4), визначивши, якому FEC належить прийнятий їм ззовні пакет, використовує таблицю LIB, щоб відшукати потрібну прив'язку “FEC-мітка”, та інкапсулює цю мітку способом, відповідним до застосовуваної на другому рівні технології.

- Пересилання пакета.

При проходженні пакета від вхідного маршрутизатора LSR1 до вихідного маршрутизатора LSR5, LSR1 може не мати мітки для цього пакета. В такому випадку він знаходить наступний маршрутизатор за IP-адресою. Нехай наступним маршрутизатором для LSR1 є LSR2. Маршрутизатор LSR1 ініціює запит мітки від LSR2. Отриману мітку LSR1 вставляє в пакет і пересилає його до LSR2. Кожен наступний LSR (в даному випадку – LSR3 і LSR4) аналізує мітку, що міститься в прийнятому пакеті, замінює її вихідної міткою і пересилає пакет далі. Коли пакет досягає LSR5, той видаляє мітку пакету, оскільки пакет залишає домен MPLS, і доставляє пакет адресату. Тракт LSP, по якому проходить пакет, показаний пунктирними лініями 3 [3].

Отримавши пакет, маршрутизатор LSR витягує з нього мітку і використовує її в якості індексу у своїй таблиці пересилання. Як тільки знайдено запис, в якому значення вхідної мітки дорівнює значенню мітки, витягнутої з пакета, маршрутизатор, згідно _агато про цього запису, замінює вхідну мітку в пакеті вихідною міткою і пересилає пакет через вихідний інтерфейс, зазначений у _агато про, до наступного LSR, який також зазначений у цьому _агато про. Якщо _агато пр вказує певну вихідну чергу, маршрутизатор ставить пакет саме в цю чергу. Простота алгоритму пересилання пакетів, використовуваного в MPLS, обумовлює просту і економічну його реалізацію в апаратному забезпеченні, що, в свою чергу, дозволяє підвищити продуктивність пересилання без використання дорогої апаратури.

Якщо LSR підтримує не одну, а кілька таблиць (по одній для кожного зі своїх інтерфейсів), то єдина зміна алгоритму полягає в тому, що після отримання пакета, LSR попередньо вибирає ту таблицю, яка буде використовуватися для обробки пакета. Вибір таблиці здійснюється згідно ідентифікатору інтерфейсу, через який пакет був отриманий.

Таким чином, мітка, що переноситься у складі пакету, завжди передає семантику пересилання, тому що вона однозначно визначає потрібний запис в таблиці, яку веде LSR, і тому що цей запис містить інформацію про те, куди пересилати пакет. В якості опції мітка може також передавати семантику резервування ресурсів, оскільки запис, який нею визначається, може містити інформацію про те, які ресурси буде використовувати пакет, наприклад, ту вихідну чергу, в яку він повинен ставати. Коли мітка переноситься в заголовку ATM або Frame Relay, вона повинна передавати семантику як поилання, так і резервування ресурсів. Коли мітка переноситься в спеціальному заголовку, інформація про те, які ресурси будуть доступні пакету, може кодуватися як частина цього заголовку, а не пересилатися міткою, яка служить в цьому випадку тільки для посилання. Ще один можливий варіант полягає у спільному використанні для кодування цієї інформації як мітки, так і “не міточної” частини

спеціального заголовка. І навіть при використанні спеціального заголовка мітка може передавати і семантику посилання, та семантику резервування ресурсів. Алгоритм пункту 5 представлено на прикладі рис. 5

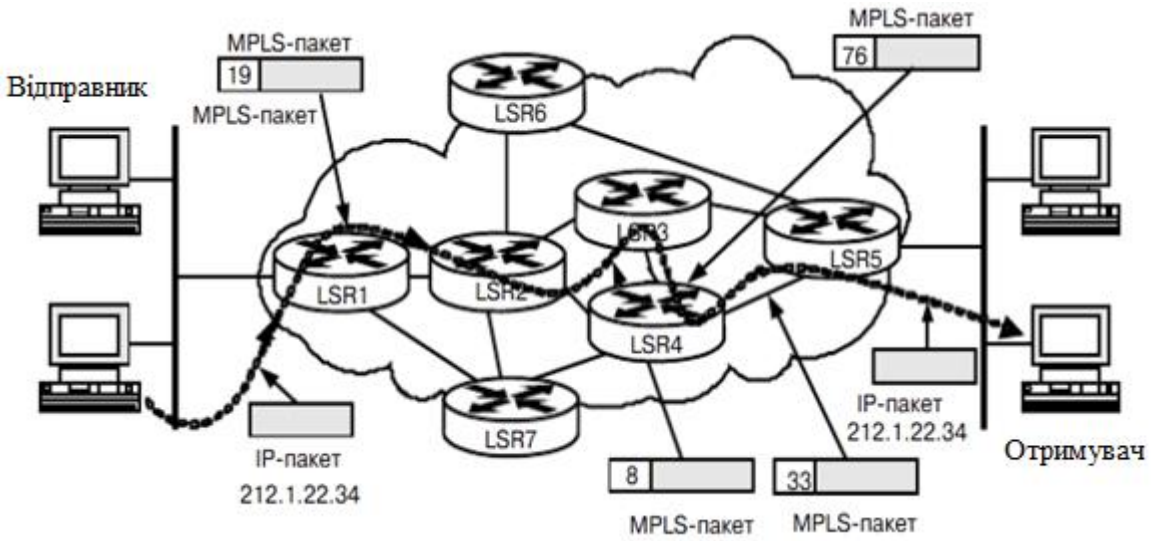


Рис. 5. Проходження трафіку в домені MPLS

Вхідний граничний маршрутизатор LSR1 розпізнає, що отриманий ззовні IP-пакет рівня 3 з адресою 212.1.22.34 повинен бути, згідно FEC цього пакету, переданий по LSP 1-2-3-4-5, додає до пакету MPLS-мітку 19 та пересилає його до транзитного маршрутизатора LSR2, де за допомогою таблиці пересилання вхідна мітка 19 замінюється вихідною міткою 8, і пакет передається по тому ж LSP далі, до LSR3. Транзитний LSR3 замінює вхідну мітку 8, яку має отриманий пакет, вихідною міткою 76. Потім транзитний LSR3 використовує відповідний вихідний інтерфейс для передачі пакета до іншого транзитного маршрутизатору LSR4, який виконує аналогічну процедуру з пакетом, що надійшли через його вхідний інтерфейс з міткою 76: постачає цей пакет новою міткою 33 і передає його до вихідного граничного маршрутизатора LSR5. В маршрутизаторі LSR5 мітка 33 видаляється і пакет пересилається до одержувача з адресою 212.1.22.34 за допомогою традиційної маршрутизації на мережевому рівні, залишаючи зображений на рис. 5 домен MPLS.

Таким чином, використання міток є основним механізмом перенесення трафіку через мережу MPLS. Мітки вводяться в пакети при їх вході в мережу

MPLS, замінюються новими мітками по мірі передачі пакетів від вузла до вузла і видаляються на виході пакетів з цієї мережі.

З описаного прикладу видно, що механізм заміни міток має ряд переваг перед механізмом маршрутизації по ділянках, що використовується у традиційних IP-маршрутизаторах. Він більш простий і ефективний. Аналіз заголовка пакета виконується тільки один раз – у вхідному LSR1. Заміна міток всередині домену MPLS виконується швидко, оскільки LSR просто розпізнає мітку і замінює її на нову. Вихідний LSR5 визначає, що пакет знаходиться на границі домену, видаляє мітку пакету і пересилає його в домен одержувача вже на основі іншої інформації – заголовку IP-пакету мережевого рівня (рис. 5).

2.3.3. Структура мітки

Мітка являє собою послідовність записів. Кожна запис в стек має довжину 4 октету. Формат такого запису показаний на рис. 6

Запис міток розміщується після заголовка канального рівня, і перед заголовком мережевого рівня (наприклад, між Ethernet - і IP-заголовком). Верх стек записується першим, а дно – останнім. Мережевий заголовок слід відразу за записом стека міток з бітом S=1 . Кожна запис стека міток містить у собі наступні поля.

- Дно стека (S)

Є засобом підтримки ієрархічної структури стека міток MPLS. У заголовку останньої (тобто самої глибокої або нижній) мітки біт S=1, а у всіх інших позначці у стеку біт S=0. Детальніше стек міток розглядається нижче.

- Час життя (TTL)

Це 8-бітове поле служить для представлення значення часу життя пакету. Дане поле є механізмом, що запобігає можливість нескінченної циркуляції пакетів по мережі внаслідок утворення закільцьованих маршрутів. Байт TTL знаходиться в кінці заголовка мітки.

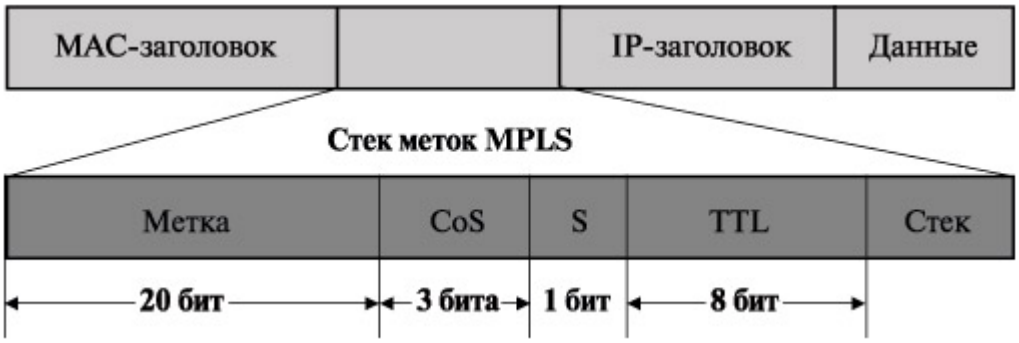


Рис. 6. Формат запису міток стека

- Експериментальне поле (CoS)

Це 3-бітове поле зарезервовано для експериментальних цілей (QoS). В даний час проводиться робота на створення узгодженого стандарту використання цих бітів для підтримки диференційованого обслуговування різнотипного трафіку та визначення класу обслуговування. Спочатку це поле так і називалося – "Клас обслуговування (CoS), і ця назва досі широко поширене. При надання диференційованих послуг MPSL-мережі це поле може вказувати певний клас обслуговування, наприклад аналогічний класів DiffServ.

- Значення мітки

Це 20-бітове поле несе в собі код мітки. Може бути будь-яким числом в діапазоні від 0 до 220 - 1, за винятком резервних значення (0, 1, 2, 3 та ін), визначенням використання яких займається робоча група MPLS у складі комітету IETF.

Коли отримано позначений пакет, аналізується значення мітки нагорі стека. В результаті цього аналізу визначається:

.наступний крок, куди повинен бути переадресований пакет;

.операція, яка повинна бути виконана зі стеком міток до переадресації. Ця операція може бути заміною мітки на вершині стеку, або видаляти записи з стека, або заміщенням верхній позиції в стеку і занесенням туди потім одного або більше нових записів.

На додаток до визначення наступного кроку та операції зі стеком міток можна також отримати дані про інкапсуляції вихідної інформації і, можливо, інші дані, які необхідні для того, щоб коректно переадресовувати пакети.

Існує кілька зарезервованих значень міток.

Значення 0 означає "IPv4 Explicit NULL Label". Це значення мітки є єдино допустимим для дна стека міток. Воно вказує, що стек повинен бути очищений і переадресація пакету повинна ґрунтуватися на IPv4-заголовку.

Значення 1 представляє "Router Alert Label". Це значення мітки є легальним в будь-якому місці стека міток, за винятком дна. Коли отриманий пакет містить таку мітку на вершині стека, він доставляється локального модуля для обробки. Дійсна переадресація пакета визначається міткою в його стеку. Однак якщо пакет переадресовується далі, ще до переадресації в стек повинна бути занесена мітка "Router Alert". Використання цієї мітки схоже з використанням опції "Router Alert" в IP-пакетах. Так як ця мітка не може лежати на дні стека, вона не асоціюється з певним протоколом мережевого рівня.

Значення 2 представляє "IPv6 Explicit NULL Label". Це значення мітки є єдино допустимим для запису на дні стека. Воно вказує, що стек повинен бути очищений, а перенаправлення пакетів мають ґрунтуватися на заголовку IPv6.

Значення 3 представляє "Implicit NULL Label". Це мітка, яку LSR може привласнювати і розсилати, але яка насправді ніколи не використовується при інкапсуляції. Коли LSR заміщує мітку на вершині стека на нову і ця нова мітка є "Implicit NULL", LSR очистить стек, замість того щоб здійснити заміну. Хоча це значення не може з'явитися при інкапсуляції, воно повинно бути специфіковано в протоколі розсилки міток, так що значення може вважатися зарезервованим.

Значення 4-15 зарезервовані.

2.3.4. Стек міток MPLS

Специфікація кодування стека міток MPLS визначена в RFC3032 "MPLS Label Stack Encoding". Даний документ містить детальну інформацію про мітках і про те, як вони використовуються з різними мережевими технологіями, а також визначає ключове для технології MPLS поняття – стек міток. Можливість мати в пакеті більше однієї мітки у вигляді стека дозволяє створювати ієрархію міток, що відкриває дорогу багатьом додаткам.

MPLS може виконати зі стеком наступні операції: розміщувати мітку в стек, видаляти мітку з стека і замінювати мітку. Ці операції можуть використовуватися для злиття та розгалуження інформаційних потоків. Операція приміщення мітки в стек (push operation) додає нову мітку поверх стека, а операція видалення мітки з стека (pop operation) видаляє верхню позначку стека.

Функціональні можливості стека MPLS дозволяють об'єднувати кілька LSP в один. До стеку міток кожного з цих LSP зверху додається загальна мітка, в результаті чого утворюється агрегований тракт MPLS. В точці закінчення такого тракту відбувається його розгалуження на складові його індивідуальні LSP. Так можуть об'єднатися тракти, що мають загальну частину маршруту. Отже, MPLS здатна забезпечувати ієрархічну пересилку, що може стати важливою і затребуваною функціональною можливістю. При її використанні не потрібно переносити глобальну маршрутну інформацію, і це робить мережу MPLS більш стабільною і масштабованої, ніж мережа з традиційною маршрутизацією.

Згідно з розглянутим нижче правилами інкапсуляції міток, за міткою MPLS в пакеті завжди повинен слідувати заголовок мережевого рівня. Так як MPLS починає роботу верхнього рівня стека, цей стек використовується за принципом LIFO "останнім прийшов, першим пішов".

Приклад чотирирівневого стека міток представлений на рис. 7

Заголовок MPLS № 1 був першим заголовком MPLS, поміщених в пакет, потім в нього були поміщені заголовки № 2, № 3 і, нарешті, заголовок № 4. Комутація по мітках завжди використовує верхню позначку стека, і мітки видаляються з пакету так, як це визначено вихідним вузлом для кожного LSP, за яким слід пакет. Розглянутий у попередньому параграфі біт S має значення 1 в нижній мітці стека і 0 – у всіх інших мітках. Це дозволяє прив'язувати префікс до кількох мітках, іншими словами – до стеку міток (Label Stack). Кожна мітка стека має власні значення поля EXP, S-біта і поля TTL.

Рис. 7. Чотирирівневий стек міток

2.3.5. Інкапсуляція міток

При використанні протоколів комутації на рівні ланки даних, таких як ATM і Frame Relay, верхня MPLS -мітка вписується в поле ідентифікаторів цих протоколів. Далі буде показано, як при застосуванні ATM для розміщення MPLS -мітки використовується поле VPI/VCI, а при застосуванні Frame Relay – поле DLCI (Data LinkConnection Identifier). У тих випадках, коли MPLS забезпечує пересилання IP-пакетів мережевого рівня і коли технологія рівня ланки даних не підтримує власне поле міток MPLS -заголовок повинен инкапсулироваться між заголовками рівня ланки даних і мережевого рівня.

Механізм інкапсуляції переносить один чи більше протоколів верхніх рівнів всередині корисної навантаження дейтаграми инкапсулирующего протоколу. По суті, вводиться новий заголовок, який робить з інкапсульованого

заголовка і поля даних нове поле даних. Загальна модель інкапсуляції представлена на рис. 8, де мається на увазі, що інкапсуляція MPLS може бути використана з будь-якою технологією рівня 2. Мітка MPLS може бути поміщена в існуючий формат заголовка рівня 2, як у випадку ATM або FR, або вписана в спеціальний заголовок MPLS, як у випадку Ethernet або PPP. Во всіх випадках будь-які додаткові мітки знаходяться між верхньою міткою стека і IP-заголовком рівня 3.

Показаний на рис 8 заголовок MPLS часто називають shim header ("заголовком — клином"), підкреслюючи в метафоричній формі той факт, що цей заголовок "рівня 2.5" вклинюється в пакет між заголовками рівня даних і мережевого рівня.

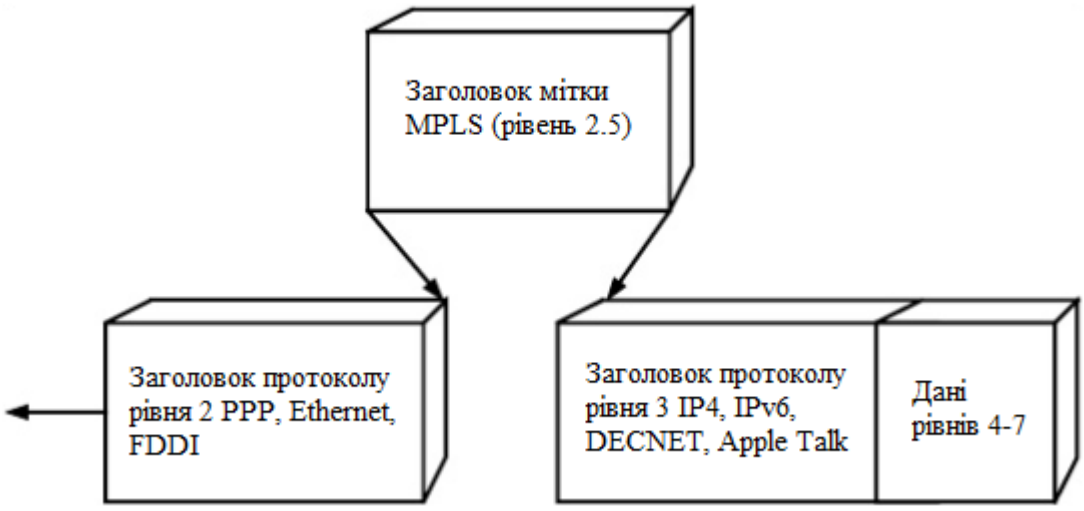


Рис 8. Принцип інкапсуляції заголовку MPLS

Однією з найсильніших сторін технології MPLS (і тому що відображена в його назві) є те, що вона може використовуватися спільно з різними протоколами рівня 2. Серед цих протоколів – ATM, Frame Relay, PPP і Ethernet, FDDI і інші, передбачені документами по MPLS.

Покажемо, як мітка може вписуватися в заголовок рівня ланки даних (VCI/VPI для мережі ATM, DLCI для мережі Frame Relay і т. п.) або "вставити" між заголовками рівня ланки даних і мережевого рівня. З самого початку робоча

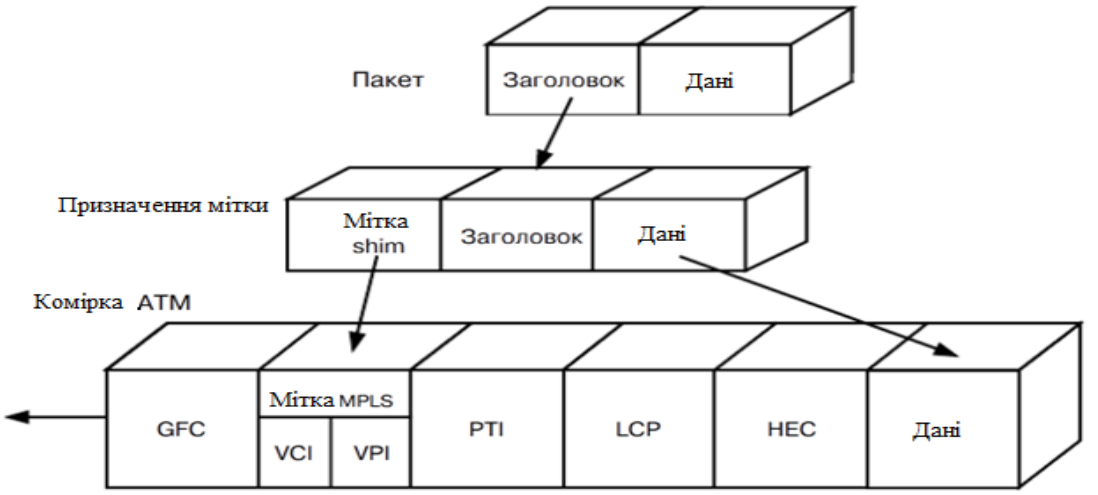
група IETF MPLS вирішила, що у всіх випадках, коли це можливо, MPLS повинна використовувати наявні формати. З цієї причини інформація мітки MPLS може передаватися в пакеті кількома різними методами:

-як частина заголовка другого рівня ATM, коли інформація мітки передається в ідентифікаторах віртуального каналу VCI і віртуального тракту VPI, що показано на рис. 9;

-як частина кадру AAL5 рівня адаптації ATM (ATM Adaptation Layer 5) перед сегментацією і складанням SAR (Segmentation and Reassembly), що виконується в ATM-оточенні у випадку, коли ця інформація містить дані про стеку міток (кілька полів MPLS -міток);

-як частина заголовка другого рівня Frame Relay, коли інформація мітки передається в ідентифікаторах DLCI, що зображено на рис. 10;

-як нова 4-байтове мітка, звана клином або прокладкою (shim), яка вставляється між заголовками другого і третього рівнів, що показано на рис. 9, – у всіх інших випадках.

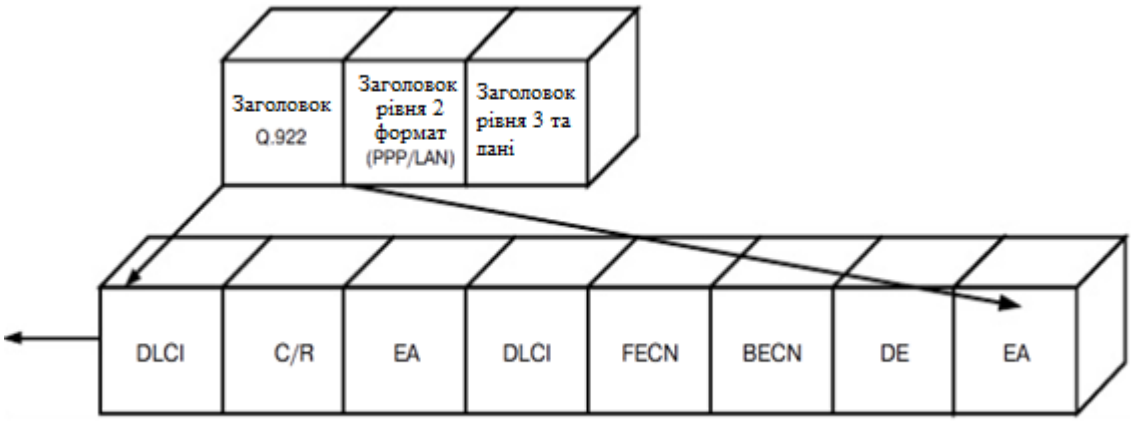


Заголовок ATM (5 байтів):
GFC – поле загального керування потоком (4 біти) для передачі інформації про перезавантаження
VCI – поле ідентифікатора віртуального каналу (16 бітів)
VPI – поле ідентифікатора віртуального тракту (8 бітів)
PTI - поле ідентифікатора типу корисного навантаження (3 біти): дані користувача або трафік техобслуговування
CLP – поле пріоритету комірки (1 біт): низький або високий пріоритет
HEC - поле контролю помилок в заголовку (8 бітів) для виправлення одиничних помилок або виявлення багатьох помилок в заголовку комірки

Рис. 9. MPLS-мітка, що передається в полях VPI/VCI заголовка ATM

Використання MPLS поверх ATM зараз досить поширене, особливо для транспортування в мережах ATM трафіку IP. ATM-комутаторів, які налаштовані для підтримки MPLS (ATM-LSR), виконують протоколи маршрутизації TCP/IP і використовують пересилку даних в ATM фіксованої довжини 53 байти. Всередині цих ATM-LSR верхня мітка MPLS поміщається в поля VCI/VPI заголовку чарунки ATM, а дані про стеку міток MPLS — в полі даних комірок ATM.

MPLS в мережах Frame Relay була розгорнута низкою великих постачальників послуг і до цих пір широко використовується. Подібно ATM, FR-комутатори підтримують MPLS, застосовують протоколи маршрутизації TCP/IP для пересилання даних під управлінням FR. При використанні FR поточна мітка міститься в поле ідентифікатора каналу ланки даних DLCI в заголовку FR. Будь-які додаткові запису в стек міток MPLS переносяться після заголовка FR, але до заголовка мережевого рівня, що міститься в поле даних кадру FR. Стандарт MPLS дозволяє FR використовувати адресу Q. 922 довжиною 2 октету, або 4 октету. Формат представлений на рис. 10



Примітка: Довжина поля DLCI може складати 10, 17 або 23 біти

Рис. 10. Розміщення мітки MPLS в кадрі FR

Принцип, представлений на рис. 8, підходить для каналів типу "точка-точка" (Point-to-Point – PPP) і для локальних мереж Ethernet (всіх типів). Подібним методом можна передати одну MPLS -мітку або стек міток.

Протокол PPP фактично являє собою сімейство споріднених протоколів IETF, що використовується для передачі багатопротокольних дейтаграм з двоточковим каналах зв'язку. PPP визначає метод інкапсуляції дейтаграм різних протоколів мережевого рівня, протоколу управління ланкою даних LCP і набору протоколів керування мережею NCP. Для використання MPLSCP з управлінням комутація по мітках через ланку PPP був визначений спеціальний протокол, який управляє передачею пакетів MPLS по каналу PPP. Цей протокол позначається абревіатурою MPLS CP. Формат показаний на рис. 11

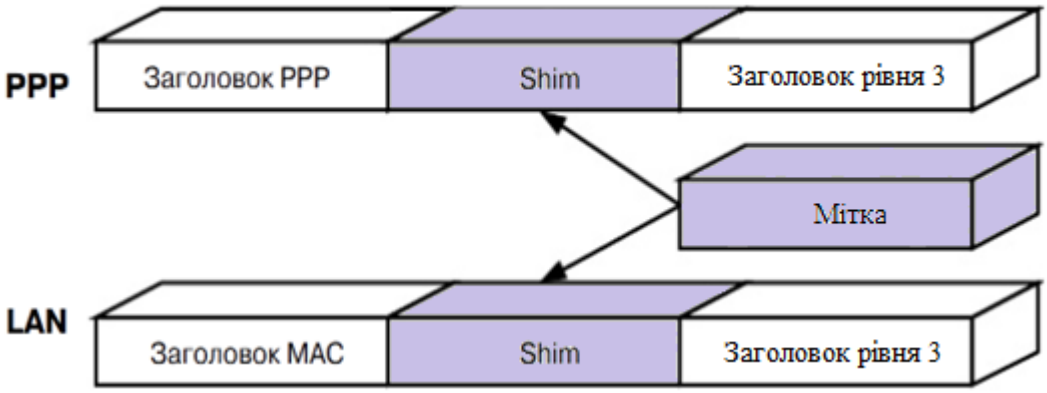


Рис. 11. Формат для введення MPLS-мітки в пакет PPP та в кадр Ethernet

Коли пакети MPLS передаються по Ethernet, в кожному кадрі Ethernet переноситься тільки один з міткою пакет. Мітка міститься між заголовком рівня ланки даних і заголовком мережевого рівня. Використання MPLS в мережах Ethernet, особливо в міських мережах, є ще однією перспективною можливістю MPLS. У стандарт Ethernet вносяться зміни, що дозволяють збільшити швидкість і дальність передачі Ethernet-пакетів. В даний час починають застосовуватися Ethernet інтерфейси на швидкості 10 Гбіт/с, а незабаром з'являться Ethernet інтерфейси і на більших швидкостях.

На жаль, додавання MPLS -мітки або стека міток до 1492-байтовому пакету може привести до необхідності його фрагментації. При передачі пакетів MTU-розміру (Maximum Transmission Unit – максимально можливий розмір

передаваного блоку даних) з MPLS -міткою протокол управління передачею TCP визначає, що в MPLS -мережі потрібно зробити фрагментацію. Однак слід зазначити, що багато Ethernet-канали підтримують передачу 1500-байтових або 1508-байтних пакетів. Більш того, в більшості мереж пакети з мітками зазвичай передаються по ATM - або PPP-каналах, а не за сегментами локальних мереж.

Отже, мітка може бути поміщена в пакет різними способами – вписується в спеціальний заголовок, розміщений між заголовками рівня 2 і рівня 3, або у вільний і доступне поле заголовка одного з цих двох рівнів, якщо, звичайно, таке є. Очевидно, що питання про те, куди слід помістити заголовок, що містить мітку, повинен узгоджуватися між об'єктами, що її використовують.

2.3.6. Таблиці пересилання

Коли пакет MPLS потрапляє в маршрутизатор комутації по мітках LSR, цей маршрутизатор переглядає наявну в нього таблицю інформаційної бази міток LIB (Label Information Base) для того, щоб прийняти рішення про подальшу обробку пакету. Цю інформаційну базу іноді називають також Next Hop Label Forwarding Entry (NHLFE), та відповідно до RFC 3031 у неї входить наступна інформація:

1) операція, яку потрібно зробити зі стеком міток пакета (замінити верхню позначку стека, видалити верхню позначку, помістити поверх стека нову мітку);

2) наступний маршрутизатор в LSP, причому “наступним” може бути той же самий LSR;

3)інкапсуляція, яка використовується при передачі пакета на канальному рівні;

4) спосіб кодування стека міток при передачі пакета;

5) інша інформація, що відноситься до пересилання пакета.

Таблиця пересилання, що містить цю інформацію, яку веде кожен LSR, як, втім, і будь-які інші таблиці, представляє собою послідовність записів. Кожен запис таблиці пересилання LSR складається з вхідної мітки і одного або більше _агато прот, причому кожен _агато пр містить значення вихідної мітки ідентифікатор вихідного інтерфейсу і адресу наступного маршрутизатора в LSP. Приклад простої таблиці пересилання LIB представлений в таблиці 1.

Таблиця 1

Запис в таблиці пересилання LIB

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

Різні подзаписи всередині однієї записи можуть мати однакові або різні значення вихідних міток. Більше однієї подзаписи буває потрібно для підтримки багатоадресної розсилки пакета, коли пакет, який надійшов до одного вхідного інтерфейсу, повинен потім розсилатися через кілька вихідних інтерфейсів. Звернення до таблиці записів проводиться за значенням вхідної мітки, тобто входить до мітці відбувається звернення до к-ї запису в таблиці.

Запис у таблиці може також містити інформацію, яка вказує, які ресурси має можливість використовувати пакет, наприклад, певну вихідну чергу.

LSR може підтримувати або одну загальну таблицю, або окремі таблиці для кожного зі своїх інтерфейсів. У першому варіанті обробка пакета визначається виключно міткою, переноситься в пакеті. У другому варіанті обробка пакета визначається не тільки міткою, але і інтерфейсом, до якої надійшов пакет. LSR може використовувати або перший, або другий, або їх поєднання.

2.3.7. Прив’язка “мітка-FEC”

Кожен запис у таблиці пересилання, яку веде LSR, що містить одну вхідну мітку і одну або більше вихідних міток. У відповідності з цими двома типами міток забезпечується два типу прив'язки міток до FEC:

перший тип – мітка для прив'язки обирається і призначається в LSR локально. Така прив'язка називається локальною;

другий тип – LSR отримує від деякого іншого LSR інформацію про прив'язку мітки, яка відповідає прив'язці, створеної на цьому іншому LSR. Така прив'язка називається віддаленої.

Засоби керування комутацією по мітках використовують для заповнення таблиць пересилання як локальну, так і віддалену прив'язку міток до FEC. Це може робитися у двох варіантах: upstream і downstream. Перший: коли мітки на локальній прив'язці використовуються як вхідні мітки, а мітки з віддаленої прив'язки — як вихідні. Другий варіант – прямо протилежний, тобто мітки з локальної прив'язки використовуються як вихідні мітки, а мітки з віддаленої прив'язки – як вхідні. Розглянемо кожен із цих варіантів.

Перший варіант називається прив'язкою до мітки FEC "знизу" (downstream label binding), тому що в цьому випадку прив'язка переносимої пакетом мітки до того FEC, якому належить цей пакет, створюється нижчестоящим LSR, тобто LSR, розташованим ближче до адресата пакета, ніж LSR, який поміщає мітку в пакет. При прив'язці "знизу" пакети, які переносять певну мітку, передаються в напрямку, протилежному напрямку передачі інформації про прив'язку цієї мітки до FEC.

Другий варіант називається прив'язкою до мітки FEC "зверху" (upstream label binding), тому що в цьому випадку прив'язка переносимої пакетом мітки до того FEC, якому належить цей пакет, створюється тим же LSR, який поміщає мітку в пакет; тобто творець прив'язки розташований "вище" (ближче до відправника пакета), ніж LSR, до якого пересилається цей пакет. При прив'язці

"зверху" пакети, які переносять певну мітку, передаються в тому ж напрямку, що і інформація про прив'язку цієї мітки до FEC.

LSR обслуговує також пул "вільних" міток (тобто міток без прив'язки). При початковій установці LSR пул містить усі мітки, які може використовувати LSR для їх локальної прив'язки до FEC. Саме ємність цього пулу і визначає, в кінцевому рахунку, скільки пар "мітка - FEC" може одночасно підтримувати LSR. Коли маршрутизатор створює нову локальну прив'язку, він бере одну з пулу; коли маршрутизатор знищує раніше створену прив'язку, він повертає мітку, зв'язану з прив'язкою, назад в пул.

Згадаймо, що LSR може вести або одну загальну таблицю пересилання, або кілька таблиць – по одній на кожен інтерфейс. Коли маршрутизатор веде загальну таблицю пересилання, він має один пул міток. Коли LSR веде кілька таблиць, він має окремий пул міток для кожного інтерфейсу.

LSR створює або знищує прив'язку до мітки FEC внаслідок певної події. Така подія може ініціюватися або пакетами даних, які повинні пересилатися маршрутизатором LSR, або керуючої (маршрутної) інформацією, яка повинна оброблятися LSR. Коли створення або знищення прив'язки ініціюється пакетами даних, ця прив'язка називається прив'язкою під впливом даних (data-driven). Коли створення або знищення прив'язки ініціюється керуючою інформацією, ця прив'язка називається прив'язкою під впливом керуючої інформації (control-driven).

Прив'язка під впливом даних передбачає, що LSR підтримує як функції пересилання при комутації по мітках, так і функції пересилання при традиційній маршрутизації. Підтримка функцій пересилання при традиційній маршрутизації необхідна тому, що прив'язка мітки являє собою ефект, супутній традиційної маршрутизації пакета.

Важливою проблемою якості функціонування, що виникає при використанні схем прив'язки під впливом даних (і, меншою мірою, – схем прив'язки під впливом керуючої інформації), є продуктивність. Кожен раз, коли LSR вирішує, що потік повинен комутувати по мітках, йому необхідно обмінюватися інформацією про прив'язку міток з суміжними LSR, і йому може знадобитися внести деякі зміни в прив'язці міток до FEC. Всі ці процедури вимагають передачі трафіку, керуючого роздачею інформації про прив'язку, і, отже, споживають ресурси засобів управління комутацією по мітках. Більш того, ці процедури споживають тим більше ресурсів, засобів управління, чим більше частка потоків, обраних для комутації по мітках. Важко кількісно оцінити, наскільки дорогим є процедура призначення і розподілу міток, але не підлягає сумніву, що продуктивність схем, що працюють під впливом даних, чутлива до цього фактору. Якщо LSR не може призначати і розподіляти мітки зі швидкістю, необхідної алгоритмом виявлення потоків, то комутувати по мітках буде менший відсоток потоків, і від цього буде страждати загальна продуктивність.

2.4. **Висновок**

У складних комп’ютерних мережах доцільним є використання технології MPLS, що базується на використанні міток. Можливості управління трафіком в мережі MPLS реалізовуються за допомогою технології інжинірингу трафіка, основний механізм якого використання односпрямованих тунелів (MPLS TE tunnel).

3. ВІРТУАЛЬНІ ПРИВАТНІ МЕРЕЖІ ТА ТУНЕЛІ

3.1. **Віртуальні приватні мережі VPN**

Термін «віртуальні приватні мережі» (VPN, Virtual Private Networks) виник на початку 1997 р., але не всі згодні з цим твердженням. Базисною технологією, яка використовується у віртуальних приватних мережах, є стек протоколів TCP / IP, який був розроблений у 60-х роках, проте деякі концепції з'явилися ще раніше.

Щоб пояснити, що таке VPN, необхідно описати два поняття: шифрування і віртуальність

Віртуальна приватна мережа - це зашифрований або інкапсульований процес комунікації, який безпечним чином передає дані з однієї точки в іншу; безпека цих даних забезпечена стійкою технологією шифрування, і передані дані проходять через відкриту, незахищену, маршрутизуєму мережу.

У цьому визначенні кілька важливих моментів:

* VPN є зашифрованим або інкапсульованим комунікаційним процесом;

* комунікація між вузлами зашифрована що гарантує безпеку і цілісність даних;

* дані проходять через відкриту, незахищену, маршрутизуєму мережу.

Тому, на відміну від віртуального ланцюга в прикладі з телефонним викликом, дані VPN проходять через колективну лінію і можуть мати багато шляхів до остаточного місця призначення.

VPN можна уявити і як процес відправлення зашифрованих даних з однієї точки в іншу через Інтернет.

VPN можуть також використовуватися на орендованих лініях, на з'єднаннях frame relay / ATM або на службах POTN (Plain Old Telephone Network, Проста стара телефонна мережа), наприклад ISDN (Integrated Service Digital Network, Цифрова мережа з інтегрованими послугами) та xDSL (Digital Subscribe

Line, Цифрова абонентська лінія). Деякі реалізації VPN, такі як в топології ретрансляції кадрів (frame relay), вже надаються деякими провайдерами Інтернету. Хоча це приватна мережа з точки зору провайдера, це все ще відкрита мережа з точки зору споживача. Додаючи технологію VPN до свого сегменту кадру (frame segment), споживачі отримують додаткові переваги.

Розглянемо приклад розміщення послуг VPN.

Корпоративна мережа, яка з'єднується з відкритою мережею для транспортування, - поширене розміщення, що використовується сьогодні в технології VPN. Інтернет застосовується як транспортний носій технології VPN, але хмара з Інтернетом можна замінити хмарою з ATM або з frame relay.

Чудовою властивістю технології VPN є її масштабність. У міру того як провайдери мережевих послуг збільшують смугу пропускання на своїх магістралях, VPN теж можуть рости, щоб користуватися цією смугою. Так як VPN не залежать від платформи і не спираються на певну операційну систему, майже будь-який пристрій в компанії може функціонувати або як клієнт VPN, або як сервер. VPN також нададуть простір для власного зростання, більшість пристроїв VPN зможуть керувати будь-якими службами, розміщеними на них. Вони дозволять за запитом створювати тунелі або наскрізну передачу з шифруванням. З'являється можливість створювати тунелі до інших вузлів, наприклад тунель між корпоративним центральним офісом і основними офісами збуту, а пізніше додаткові тунелі для інших офісів.

При створенні VPN необхідно вирішити, чи потребує ваша організація (компанія) в інкапсуляції. Інкапсуляція - це процес розміщення пакету даних усередині IP-пакету. Якщо ви хочете використовувати протокол IPX для комунікації з іншим вузлом через Інтернет, пакет IPX поміщається всередину пакету IP і відсилається. Можна також інкапсульовати IP пакет всередину іншого IP-пакету. Ця конфігурація додає додатковий шар захисту. Тому при використанні протоколу IPX знадобиться пристрій для інкапсуляції пакета IPX

всередину пакету IP. Деякі пристрої VPN (у тому числі шлюзи) підтримують цю функціональність.

Підводячи підсумки з визначення віртуальної приватної мережі та даного розділу, можна прийти до висновку, що:

VPN (Virtual Private Network - віртуальна приватна мережа) - узагальнена назва технологій, що дозволяють забезпечити одне або кілька мережевих з'єднань (логічну мережу) поверх іншої мережі (наприклад, Інтернет). Незважаючи на те, що комунікації здійснюються по мережах з меншим невідомим рівнем довіри (наприклад, з публічних мережам), рівень довіри до побудованої логічної мережі не залежить від рівня довіри до базових мереж завдяки використанню засобів криптографії (шифрування, аутентифікація, інфраструктури публічних ключів, засобам для захисту від повторів і зміни переданих по логічної мережі повідомлень).

Існує безліч різновидів віртуальних приватних мереж. Їх спектр варіюється від мереж інтернет-провайдерів, які дозволяють керувати обслуговуванням клієнтів безпосередньо на їх площах, до корпоративних VPN, які розгортаються та керуються самими корпораціями. Прийнято виділяти три основних види віртуальних приватних мереж:

VPN з віддаленим доступом (Remote Access VPN);

Багато протокольній ні VPN (Intranet VPN);

Багато протоколь VPN (Extranet VPN).

Принцип роботи VPN з віддаленим доступом простий: користувачі встановлюють з’єднання з місцевою точкою доступу до глобальної мережі (PoP), після чого їх потоки даних тунелюються через Інтернет, що дозволяє, зокрема, уникнути плати за міжміський або міжнародний зв’язок. Потім всі ці потоки концентруються у відповідних вузлах і передаються в корпоративні мережі. Внаслідок використання в якості об’єднуючої магістралі відкритої мережі Інтернет механізми захисту інформації стають життєво важливими елементами такої технології.

Intranet VPN представляє собою найпростіший варіант VPN: корпорації, які потребують організації для своїх філій і відділень доступу до централізованих сховищ інформації, використовують замість виділених ліній дешевий зв'язок з цими сховищами через Інтернет.

Extranet VPN – мережева технологія, яка забезпечує прямий доступ з мережі однієї компанії до мережі іншій компанії, сприяючи тим самим підвищенню надійності зв'язку, яка встановлюється для ділового співробітництва. Мережі Extranet VPN, в цілому, схожі на _агато протокольній__ні віртуальні приватні мережі, з тією лише різницею, що проблема захисту інформації є для них більш гострою. Коли кілька компаній приймають рішення працювати разом і відкривають один для одного свої мережі, вони повинні дбати про те, щоб їхні нові партнери мали доступ тільки до певної інформації. Конфіденційна ж інформація повинна бути надійно захищена від несанкціонованого використання. Саме тому в _агато протокольн мережах більше значення повинне надаватися контролю доступу за допомогою брандмауерів (Firewalls). Важлива і аутентифікація користувачів, покликана гарантувати, що доступ до інформації отримають лише ті, кому він дійсно разрешен. В додаток до типів технологій, що використовуються для реалізації VPN, ці мережі поділяються також за рівнями моделі OSI, в яких вони працюють. Існують дві основні групи – мережі VPN рівня 2 і мережі VPN рівня 3,- хоча деякі фахівці вважають, що покажчики URL з префіксами https:// дозволяють створювати VPN рівня 4. Мережі MPLS-VPN в цій класифікації утворюють новий тип VPN рівня 2.5.

3.1.1. Основи тунелювання

Туннелювання (tunneling), або інкапсуляція (encapsulation), - це спосіб передачі корисної інформації через проміжну мережу. Такою інформацією можуть бути кадри (або пакети) іншого протоколу. При інкапсуляції кадр не передається в сгенерированном вузлом-відправником вигляді, а забезпечується додатковим заголовком, що містить інформацію про маршрут, що дозволяє

інкапсульованим пакетам проходити через проміжну мережу (Internet). На кінці тунелю кадри деінкапсуліруются і передаються одержувачу. Цей процес (що включає инкапсуляцию і передачу пакетів) і є тунелювання. Логічний шлях пересування інкапсульованих пакетів в транзитній мережі називається тунелем.

3.1.2. Протоколи

Протокол VPN визначає, яким чином система VPN взаємодіє з іншими системами в інтернеті, а також рівень захищеності трафіку. Якщо розглянута організація використовує VPN тільки для внутрішнього інформаційного обміну, питання про взаємодію можна залишити без уваги. Однак якщо організація використовує VPN для з'єднання з іншими організаціями, власні протоколи використовувати, швидше за все, не вдасться. У розмові про алгоритм шифрування було згадано, що зовнішні навколишні фактори можуть чинити більший вплив на безпеку системи, ніж алгоритм шифрування. Протокол VPN впливає на загальний рівень безпеки системи. Причиною цьому є той факт, що протокол VPN використовується для обміну ключами шифрування між двома кінцевими вузлами. Якщо цей обмін не захищений, зловмисник може перехопити ключі і потім розшифрувати трафік, звівши нанівець всі переваги VPN.

Для того щоб була можливість створення VPN на базі обладнання і програмного забезпечення від різних виробників необхідний деякий стандартний механізм. Таким механізмом побудови VPN є протокол Internet Protocol Security (IPSec). IPSec описує всі стандартні методи VPN. Цей протокол визначає методи ідентифікації при ініціалізації тунелю, методи шифрування, використовувані кінцевими точками тунелю і механізми обміну та управління ключами шифрування між цими точками. З недоліків цього протоколу можна відзначити те, що він орієнтований на IP. Іншими протоколами побудови VPN є протоколи PPTP (Point-to-Point Tunneling Protocol), розроблений компаніями Ascend Communications і 3Com, L2F (Layer-2 Forwarding) - компанії Cisco Systems і L2TP

(Layer-2 Tunneling Protocol), який об'єднав обидва вищеназваних протоколу. Однак ці протоколи, на відміну від IPSec, не є повнофункціональними (наприклад, PPTP не визначає метод шифрування) Говорячи про IPSec, не можна забувати про протокол IKE (Internet Key Exchange), що дозволяє забезпечити передачу інформації по тунелю, виключаючи втручання ззовні. Цей протокол вирішує завдання безпечного управління та обміну криптографічними ключами між віддаленими пристроями, в той час, як IPSec кодує і підписує пакети. IKE автоматизує процес передачі ключів, використовуючи механізм шифрування відкритим ключем, для встановлення безпечного з'єднання. Крім цього, IKE дозволяє виробляти зміна ключа для вже встановленого з'єднання, що значно підвищує конфіденційність переданої інформації. Інкапсуляція - забезпечує мультиплексування декількох транспортних протоколів по одному каналу; Протокол LCP - PPP задає гнучкий LCP для встановлення, налаштування та перевірки каналу зв'язку. LCP забезпечує узгодження формату інкапсуляції, розміру пакета, параметри установки і розриву з'єднання, а також параметри аутентифікації. В якості протоколів аутентифікації можуть використовуватися PAP, CHAP і ін; Протоколи управління мережею - надають специфічні конфігураційні параметри для відповідних транспортних протоколів. Наприклад, IPCP протокол управління IP. Для формування тунелів VPN використовуються протоколи PPTP, L2TP, IPsec, IP-IP.Протокол PPTP - дозволяє інкапсулювать IP-, IPX-і NetBEUI-трафік в заголовки IP для передачі по IP-мережі, наприклад Internet.

Протокол L2TP - дозволяє шифрувати і передавати IP-трафік з використанням будь-яких протоколів, що підтримують режим "точка-точка" доставки дейтаграм. Наприклад, до них відносяться протокол IP, ретрансляція кадрів і асинхронний режим передачі (ATM). Протокол IPsec - дозволяє шифрувати і інкапсулювать корисну інформацію протоколу IP в заголовки IP для передачі по IP-мереж. Протокол IP-IP - IP-дейтаграма инкапсулируется за допомогою додаткового заголовка IP. Головне призначення IP-IP -

туннелирование багатоадресного трафіку в частинах мережі, що не підтримують багатоадресну маршрутизацію. Для технічної реалізації VPN, крім стандартного мережевого обладнання, знадобиться шлюз VPN, що виконує всі функції з формування тунелів, захисту інформації, контролю трафіку, а нерідко і функції централізованого управління. На сьогоднішній день VPN - це економічне, надійне і загальнодоступне рішення організації віддаленого доступу. Яким би не була відстань, VPN забезпечить з'єднання з будь-якою точкою світу і збереження передачі найважливіших даних.

3.1.3. Переваги VPN

Віртуальні приватні мережі мають декілька переваг над традиційними приватними мережами. Головні з них - економічність, гнучкість і зручність використання.

Економічність. За допомогою VPN-мереж підприємствам вдається хоча б частково обмежити зростання числа модемів, серверів доступу, комутованих ліній та інших технічних засобів, які організації змушені впроваджувати, щоб забезпечити віддаленим користувачам доступ до своїх корпоративних мереж. Крім того, віртуальні приватні мережі дають можливість віддаленим користувачам звертатися до мережевих ресурсів компанії не по дорогих орендованим лініях, а через місцевий телефонний зв'язок. Особливо вигідні віртуальні приватні мережі в тих випадках, коли користувачі видалені на великі відстані і тому орендовані лінії обходяться дуже дорого, а також коли таких користувачів багато, у зв'язку з чим і їм потрібна велика кількість орендованих ліній. Однак ці переваги можуть зійти нанівець, якщо обсяг трафіку в VPN-мережі настільки великий, що система не встигає зашифровувати і розшифровувати пакети даних. Щоб уникнути виникнення таких вузьких місць, підприємство змушене купувати додаткове устаткування. Крім того, через відносну новизни технології VPN і складності використовуваних засобів безпеки системний адміністратор для віртуальної мережі обходиться дорожче, ніж для традиційної.

Дослідницька компанія Forrester Research опублікувала наступні дані, що характеризують перевага застосування VPN поверх Internet (з розрахунку 1000 користувачів) порівняно зі створенням центру віддаленого доступу (Remote Access Service).

3.1.4. Компоненти MPLS VPN

Перш за все, мережа MPLS VPN ділиться на дві області: мережі IP клієнтів і внутрішня (магістральна) мережа MPLS провайдера, яка необхідна для об'єднання мереж клієнтів

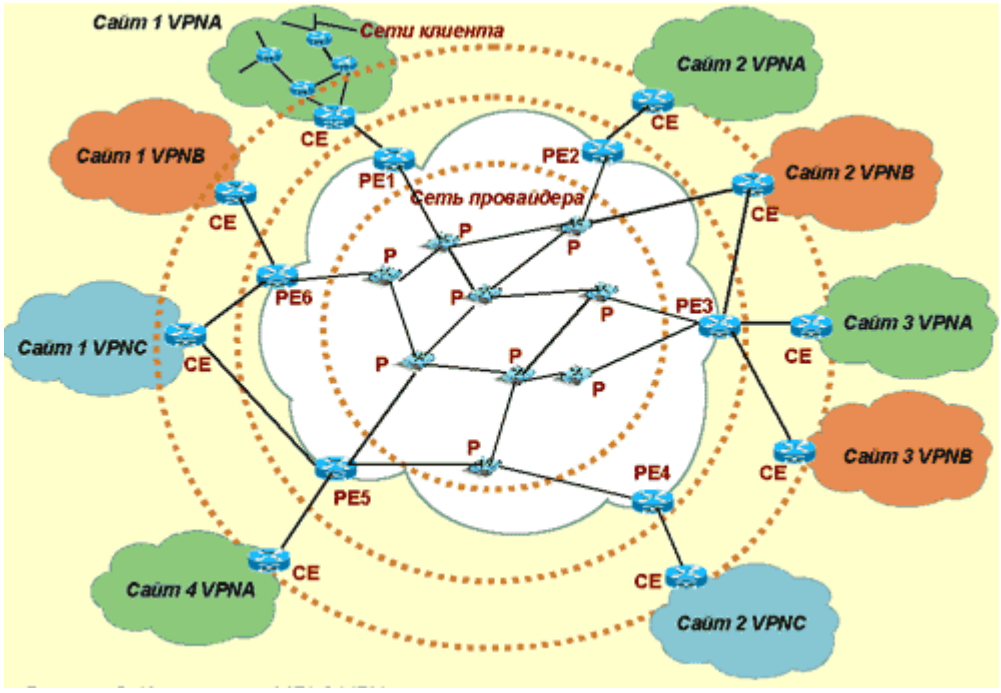


Рис.`12. Структура розробленої мережі

У загальному випадку у кожного клієнта може бути кілька територіально відокремлених мереж IP, кожна з яких у свою чергу може включати декілька підмереж, пов'язаних маршрутизаторами. Такі територіально ізольовані мережеві «острівці» корпоративної мережі прийнято називати сайтами. Належать одному клієнту сайти обмінюються пакетами IP через мережу провайдера і утворюють віртуальну приватну мережу цього клієнта. Наприклад, про корпоративної мережі, в якій мережу центрального відділення зв'язується з трьома віддаленими філіями, можна сказати, що вона складається з чотирьох

сайтів. Для обміну маршрутної інформацією в межах сайту вузли користуються одним з внутрішніх протоколів маршрутизації (Interior Gateway Protocol, IGP), область дії якого обмежена автономною системою: RIP, OSPF або IS-IS. Маршрутизатор, за допомогою якого сайт клієнта підключається до магістралі провайдера, називається прикордонним маршрутизатором клієнта (Customer Edge router, CE). Будучи компонентом мережі клієнта, CE нічого не знає про існування VPN. Він може бути з'єднаний з магістральною мережею провайдера кількома каналами.

Магістральна мережа провайдера є мережею MPLS, де пакети IP просуваються на основі не IP-адрес, а локальних міток (більш докладно про технології цього типу можна прочитати в статті Н. Оліфер «Перехресні стежки через мережу» в даному номері). Мережа MPLS складається з маршрутизаторів з комутацією міток (Label Switch Router, LSR), які направляють трафік за попередньо прокладених шляхах з комутацією міток (Label Switching Path, LSP) у відповідності зі значеннями тегів. Пристрій LSR - це своєрідний гібрид маршрутизатора IP і комутатора, при цьому від маршрутизатора IP береться здатність визначати топологію мережі за допомогою протоколів маршрутизації і вибирати раціональні шляху проходження трафіку, а від комутатора - техніка просування пакетів з використанням міток і локальних таблиць комутації. Пристрої LSR для стислості часто називають просто маршрутизаторами, і в цьому є свій резон - вони з таким же успіхом здатні просувати пакети на основі IP-адреси, якщо підтримка MPLS відключена.

У мережі провайдера серед пристроїв LSR виділяють прикордонні маршрутизатори (Provider Edge router, PE), до яких через маршрутизатори CE підключаються сайти клієнтів і внутрішні маршрутизатори магістральної мережі провайдера (Provider router, P). Маршрутизатор CE і PE зазвичай пов'язані безпосередньо фізичною каналом, на якому працює будь-якої протокол канального рівня - наприклад, PPP, FR, ATM або Ethernet. Спілкування між CE і PE йде на основі стандартних протоколів стека TCP / IP, підтримка MPLS

потрібна тільки для внутрішніх інтерфейсів PE (і всіх інтерфейсів P). Іноді корисно розрізняти щодо направлення просування трафіку вхідний PE і вихідний (віддалений) PE.

У магістральної мережі провайдера тільки прикордонні маршрутизатори PE повинні бути налаштовані для підтримки віртуальних приватних мереж, тому тільки вони «знають» про існуючі VPN. Якщо розглядати мережу з позицій VPN, то маршрутизатори провайдера P безпосередньо не взаємодіють з маршрутизаторами замовника CE, а просто розташовуються уздовж тунелю між вхідним і вихідним маршрутизаторами PE.

Маршрутизатор PE є функціонально більш складними, ніж P. На них покладаються головні завдання з підтримки VPN, а саме розмежування маршрутів і даних, які від різних клієнтів. Маршрутизатор PE служать також кінцевими точками шляхів LSP між сайтами замовників, і саме PE призначає мітку пакету IP для його транзиту через внутрішню мережу маршрутизаторів P.

Шляхи LSP можуть бути прокладені двома способами: або із застосуванням технології прискореної маршрутизації (IGP) за допомогою протоколів LDP, або на основі технології Traffic Engineering за допомогою протоколів RSVP або CR-LDP. Прокладка LSP означає створення таблиць комутації міток на всіх маршрутизаторах PE і P, що утворюють даний LSP

У сукупності ці таблиці задають безліч шляхів для різних видів трафіку клієнтів. У VPN застосовується різна топологія зв'язків: повнозв'язна, «зірка» (часто звана в англомовній літературі hub-and-spoke) або чарункова.

3.1.5. Маршрутизація MPLS-VPN

PE-маршрутизатори підтримують для кожного підключеного сайту одну асоційовану з ним таблицю маршрутизації. Розглянемо мережу, в якій існують три PE-маршрутизатора – PE1, PE2 і PE3. Кожен з них з’єднується з одним із CE-маршрутизаторів – CE1, CE2 і CE3, відповідно. При цьому CE1, CE2 і CE3 належать сайтам, що входять в одну VPN. У такому разі PE1 використовує протокол MP-BGP, щоб передати PE2 і PE3 відомості про маршрути, які він

отримав від CE1. У свою чергу, PE2 і PE3 вносять дані про ці маршрути у свої таблиці маршрутизації, асоційовані з сайтами, в яких знаходяться CE2 і CE3. Якщо сайт належить кільком VPN, то відповідна йому таблиця маршрутизації в PE може містити дані про маршрути всіх цих VPN.

Якщо PE-маршрутизатор отримає від сайту пакет з адресою, котрого немає в асоційованої таблиці маршрутизації, то або він відкине такий пакет, або, якщо оператор надає послуги доступу в Internet через цю VPN, відбудеться звертання до таблиці маршрутизації Internet.

Щоб забезпечувалася ізоляція однієї VPN від іншої, важливо щоб ні один з маршрутизаторів, з яких складається магістральна мережа MPLS (Backbone Router), не приймав пакети з мітками від маршрутизаторів, що не належать до цієї мережі, за винятком випадку, коли верхня мітка стека вже була присвоєна маршрутизатором, що входять в магістральну мережу MPLS, і притому виявляється, що використання цієї мітки призведе до виходу пакета з мережі до того, як будуть опрацьовані інші мітки стека і виконано аналіз IP-заголовка.

Асоційовані таблиці маршрутизації в PE використовуються тільки для пакетів, які отримані від сайтів, безпосередньо з'єднаних з PE, і, як результат, може існувати кілька різних маршрутів до однієї системи, причому маршрут буде визначатися сайтом, з якого пакет потрапив в магістральну мережу.

В деяких випадках сайт клієнта може бути розділений на кілька віртуальних сайтів, наприклад, з використанням VLAN. Такі віртуальні сайти можуть входити в різні VPN, і PE повинен підтримувати таблиці маршрутизації для кожного віртуального сайту.

PE-маршрутизатори використовують протокол BGP для передачі один одному маршрутної інформації. Для кожного адресного префікса BGP-спікер може визначити та оголосити тільки один маршрут, але будь-яка VPN може мати власний адресний простір, одна і та ж адреса може використовуватися в різних VPN. Для того щоб усунути це протиріччя, було специфіковано нове сімейство адрес VPN-Ipv4 Address Family.

На рис представлено кодування Route Distinguisher.

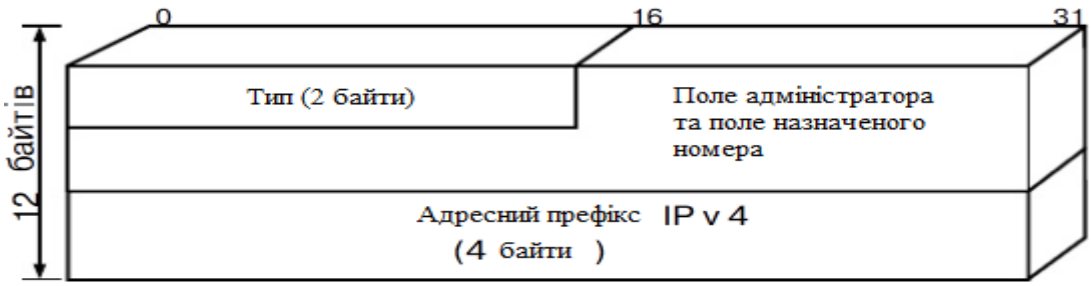


Рис. 13. Кодування Route Distinguisher

Адреса VPN-Ipv4 має довжину 12 байтів, перші вісім з яких займає префікс, званий роздільником маршрутів RD (Route Distinguisher), а інші 4 байти містять Ipv4-адреси (рис.13). Навіть якщо в двох VPN будуть збігаються Ipv4-адреси, PE-маршрутизатор перетворює їх в унікальні адреси VPN-Ipv4. Таким чином вирішується завдання визначення різних маршрутів до пристроїв, які мають один і той же IP-адрес, але належать різним VPN.

Сам RD не є інформативним і служить лише для створення декількох окремих маршрутів загального адресного префікса Ipv4. Він може бути використаний також для визначення декількох різних маршрутів до одного і того ж мережевого пристрою шляхом створення двох різних адрес VPN-Ipv4, що мають загальну Ipv4-частина [3].

RD мають структуру, що дозволяє кожному провайдеру створювати і модифікувати власний “номерний простір”, не конфліктуючи при цьому з RD, призначеними іншими провайдерами. RD складається з 2-байтового поля типу, поля адміністратора (Administrator) і поля призначеного номери (Assigned Number). При цьому значення поля типу визначає довжину обох

наступних полів, а також семантику поля адміністратора.

Структура розділювача маршрутів повністю ігнорується протоколом BGP, коли він порівнює два таких адресних префікса. Вона має сенс тільки для провайдера послуг. Якщо ж поля адміністратора і призначеного номери заповнені нулями, то адреса має те ж значення, що і звичайний Ipv4-адрес.

Будь-яка асоційована таблиця маршрутизації для будь-якого заданого Ipv4-префіксу буде мати дані тільки про одному маршруті VPN-Ipv4. Коли адресою призначення ставиться у відповідність маршрут VPN-Ipv4, то співвідноситься лише Ipv4-частина. PE-маршрутизатор повинен асоціювати маршрути, які ведуть до певного CE, з певним RD. При цьому PE може бути налаштований так, щоб асоціювати всі маршрути, що ведуть до одного CE, з одним RD або з різними RD.

4. КОМП'ЮТЕРНА МЕРЕЖА НА ОСНОВІ ТЕХНОЛОГІЇ MPLS

4.1. **Розробка мережі**

Для того щоб налагодити та протестувати мережу VPN MPLS необхідно виконати наступні дії:

1)Сконфігурувати інтерфейси мережі і протокол IGP;

Для того щоб сконфігурувати інтерфейси мережі і IGP, необхідно виконати наступні дії.

Етап 1. Включити службу CEF на PE-маршрутизаторі в режимі глобального конфігурування. CEF-комутація є суттєвою частиною функціонування MPLS-комутації.

Результат:

Router(config) #ip cef

Етап 2. Налаштувати IP-адреса петлевого інтерфейсу для використання його в якості ідентифікатора в процесі IGP-маршрутизації:

Router(config) #loopback n

Router(config-interface) #ip-адреса, IP-адреса, маска

Етап 3. Сконфігурувати протокол IGP. В даному прикладі використано маршрутизації OSPF, переводить командний рядок в режим конфігурування маршрутизатора.

Результат:

Router(config)#маршрутизатор ospf ospf-процесу*id;

Етап 4. Задати інтерфейс, на якому буде використовуватися маршрутизації OSPF, і вказати ідентифікатор (ID) області для даного інтерфейсу:

Router(config-router)#мережевий адресу символи-маска зона-id

Етап 5. Сконфігурувати інтерфейси, приєднані до PE- маршрутизаторам з даними IP-адресою.

Результат:

Router(config)#інтерфейс послідовний роз'єм/адаптер/порт Router(config-interface)#ip-адреса, IP-адреса, маска

Етап 6. Включити на заданому інтерфейсі теговую комутацію (Tag Switching):

Router(config-interface)#tag-switching IP

2)Вказати VPN-мережі;

Технологія MPLS підтримує велику кількість VPN-мереж для різних користувачів і має виключно високим ступенем розширюваності. Кожен користувач VPN-мережі логічно пов'язаний з комплексом маршрутизації і пересилання (VRF). Для того щоб визначити VPN-комплекс маршрутизації на PE-маршрутизаторі, необхідно виконати наступні дії:

Етап 1. Задати різні VPN-комплекси маршрутизації і пересилання шляхом призначення VRF-імен і увійти в режим конфігурування VRF: Router(config)#ip vrf vrf-name,

У цій команді vrf-name – ім'я, призначене комплексу VRF. Воно використовується для ідентифікації користувача служби VPN і повинно бути унікальним. Ім'я vrf-name чутливе до регістру. Все CE-маршрутизатори користувача, приєднані до PE-маршрутизатора, повинні мати певні подібним чином імена.

Етап 2. Створити таблиці маршрутизації і пересилання для мереж VPN з використанням ознаки маршрутів (Route Distinguisher – RD). Ознака RD додається в подрежиме VRF. Стандартне значення RD відсутня. Ознака RD повинен бути налаштований так, щоб стало можливим функціонування VRF-комплексу. Ознака RD додає 64-бітове значення до 32-бітовому префікса IP версії 4, в результаті чого створюється 96-бітовий VPN-префікс протоколу IP. Служба RD створює таблиці маршрутизації і пересилання і задає для VPN-мережі значення параметра RD. Ознаки маршрутів RD вставляються перед початком префіксів протоколу IP

четвертої версії, перетворюючи їх у глобально унікальні VPN-префікси протоколу. Така структура дозволяє користувачам VPN-мереж використовувати ту ж саму приватну схему адресації IP:

Router(config-vrf)#rd route-distinguisher

Етап 3. Імпортувати з розширеного VPN-спільноти або експортувати йому інформацію про маршрутизації. Після цього потрібно створити для комплексу VRF розширене співтовариство адресатів маршруту з використанням команди route-target підрежимі VRF. Цей адресат маршруту задає розширене співтовариство VPN-адресатів маршруту. Подібно ознакою маршруту розширене співтовариство складається з номера автономної системи і довільного кімнати або з IP-адреси і довільного номери.

Результат:

Router(config-vrf)#route-target {import | export | both } route-target-ext-community

Етап 4. Виконати логічне зв’язування VRF-комплексу з інтерфейсом. Даний етап дуже важливий, оскільки служба MPLS логічно пов’язує фізичний інтерфейс з комплексом VRF.

Результат:

Router(config-if)#ip vrf forwarding vrf-name

Логічне зв’язування інтерфейсу з комплексом VRF призводить до видалення IP-адреси даного інтерфейсу. Після того як інтерфейсу буде призначений комплекс VRF, IP-адреса має бути налаштований повторно.

3)Налаштувати сеанси маршрутизації PE-PE;

Для того щоб сконфігурувати сеанси маршрутизації PE-PE многопротокольного IBGP в мережі провайдера, на PE-маршрутизаторах необхідно виконати наступні дії.

Етап 1. Налаштувати процес маршрутизації IBGP з передачею номери автономної системи іншим PE-маршрутизаторам IBGP: Router(config)#маршрутизатор bgp автономної системи

Етап 2.Вимкнути одноадресні анонси префіксів протоколу IP версії 4:

Маршрутизатор{config-router)#немає bgp ipv4 за замовчуванням-unicast

Етап 3. Задати IP-адреса сусіднього PE-маршрутизатора або паритетну групу пристроїв протоколу IBGP, ідентифікуючи її тим самим для автономної локальної системи:

Router(config-router)#сусід {ip-адреса | peer-групи-ім'я} лист.-як число

Етап 4. Включити анонси адрес протоколу IP версії 4 сусіднім пристроям IBGP:

Маршрутизатор (conf ig-маршрутизатор) #сусід ip-адреса включити

4)Налаштувати сеанси маршрутизації PE-CE;

PE-маршрутизатор необхідно налаштувати таким чином, щоб вся інформація про маршрутизації, отримана від інтерфейсу користувача, могла бути логічно пов'язана з конкретним комплексом VRF. Необхідного результату можна досягти шляхом використання стандартних процесів протоколів маршрутизації, відомих як контексти маршрутизації. Протокол RIP версії 2 може бути використаний в якості протоколу маршрутизації між пристроями PE і CE. Маршрутна інформація, отримана в PE-маршрутизатором по протоколу RIPv2 (версії 2) від CE-маршрутизатора, поміщається в комплекс VRF, логічно пов'язаний з фізичним інтерфейсом, під'єднаним до CE-маршрутизатора. Після цього інформація VRF передається по сеансам IBGP PE-маршрутизаторам того ж рівня. При звичайній маршрутизації за допомогою протоколу RIP першої і другої версій команди, що починаються з ключового слова в мережі, які задають

використовують його інтерфейси, вводяться в _агато про конфігурування протоколу маршрутизації router rip. Такі дії призводять до того, що RIP-маршрути передаються в глобальні табличні маршрутизації PE-маршрутизаторів. Однак потрібно, щоб RIP-маршрути підтримувалися тільки усередині замкнутої VRF-групи VPN-мережі користувача. Для цього мережні команди вводяться в _агато про адресу сім'ї. Аналогічним чином в _агато про адресу сім'ї повинно бути конфігуровано перерозподіл IBGP-маршрутів, щоб VPN-маршрути, отримані від сеансу IBGP, були оголошені CE-маршрутизатора за допомогою RIP-процесу. Для того щоб налаштувати сеанси RIP-маршрутизації від PE до РЄ, на PE-маршрутизаторі необхідно виконати наступні дії.

Етап 1. Включити протокол RIP версії 2:

Router(config)#router rip

Router(config-router) #version 2

Етап 2. Задати параметри протоколу RIP для сеансів маршрутизації від пристрою PE до пристрою CE _агато про адресу сім'ї всередині головного процесу конфігурування RIP:

Router(config-router)#адреса сім'ї ipv4 [unicast] vrf vrf-ім'я

Етап 3. Зв'язати мережу з процесом маршрутизації RIP в _агато про адреса сім'ї:

Router(config-router-af) #префікс мережі

Етап 4. Перерозподілити IBGP-маршрути в колекції RIP-адрес для того, щоб оголосити їх CE-маршрутизаторам:

Router(config-router-af)#поширювати bgp asn показника показника

5)Сконфігурувати P-маршрутизатори;

Базові маршрутизатори провайдера (постачальника основні маршрутизатори – P-маршрутизатори) являють собою LSR-пристрої, які беруть участь у роботі протоколу маршрутизації IGP, такого, наприклад, як OSPF або IS-IS. Однак вони не беруть участі в _агато протокольній_

процесі IBGP, як це роблять PE-маршрутизатори, тому вони мають більш просту конфігурацію. P-маршрутизатори не є термінальними пристроями каналів користувача від CE-маршрутизаторів. Нижче наводиться поетапний опис процесу конфігурування P-маршрутизатора, на якому функціонує протокол OSPF.

Етап 1. Включити комутацію CEF на PE-маршрутизаторі в режимі глобального конфігурування. CEF-комутація є істотним елементом функціонування технології MPLS.

Результат: Router(config)#ip cef

Етап 2. Налаштувати IP-адреса петлевого інтерфейсу для використання його в якості ідентифікатора в процесі IGP-маршрутизації:

Router(config)#loopback n

Router(config-interface)#ip-адреса, IP-адреса, маска

Етап 3. Задати конфігурацію використовуваного протоколу IGP. У даному прикладі використовується маршрутизація протоколу OSPF; введення команди відбувається в режимі конфігурування маршрутизатора.

Результат:

Router(config)#маршрутизатор ospf ospf-id-процесу

Етап 4. Задати інтерфейс, на якому буде функціонувати OSPF, і ідентифікатор області для цього інтерфейсу:

Router(config-router)#мережевий адресу символи-маска зона-id

Етап 5. Сконфігурувати інтерфейси, приєднані до PE-маршрутизаторам з даними IP-адресою. У прикладі налаштований інтерфейс DS3. Результат:

Router(config)#інтерфейс послідовний роз'єм/адаптер/порт
Router(config-interface)#ip-адреса, IP-адреса, маска

Етап 6. Включити тегову комутацію (Tag Switching) для інтерфейсу:
Router(config-interface)#tag-switching IP

6)Сконфігурувати CE-маршрутизатори;

CE-маршрутизатори можуть бути налаштовані з використанням однієї з чотирьох опцій:

• статична маршрутизація;

• маршрутизація за протоколом RIP версії 2;

• маршрутизація за протоколом BGP4;

• маршрутизація за протоколом OSPF.

PE-маршрутизатор повинен бути налаштований з використанням того ж самого протоколу маршрутизації, який був обраний для CE-маршрутизатора. CE-маршрутизатори можуть належати користувачеві або провайдера. Як правило, якщо провайдер пропонує VPN-служби керованого протоколу IP (Managed IP), то CE-маршрутизатор належить провайдеру і підтримується ним. Користувачам надається докладна інформація про IP-структурі та відповідна документація для нумерації IP-пристроїв користувача та внутрішньої маршрутизації. Більшість провайдерів воліють самостійно управляти CE-маршрутизаторами, особливо якщо структура їх VPN-мереж MPLS досить складна. Усунення помилок і несправностей в такій ситуації стає скрутним, якщо інженери провайдера не мають повного доступу до CE-маршрутизатора.

Для того щоб настроїти використання протоколу RIP версії 2 для сеансів маршрутизації CE-PE, на CE-маршрутизаторі необхідно виконати наступні дії.

Етап 1. Сконфігурувати використання протоколу RIP версії 2:
Router(config)#router rip

Router(config-router)#version 2

Етап 2. У режимі конфігурування маршрутизатора зв’язати мережу з процесом RIP-маршрутизації:
Router(config-router)#network prefix

7)Налаштувати QoS.

Для налаштування QoS на вхідних PE-маршрутизаторах використовується модульний інтерфейс CLI функції якості обслуговування. Він дозволяє користувачам задавати клас потоку даних незалежно від стратегії QoS.

4.2. **Термінологія**

Канали MPLS можна назвати VPN ". Це так. Але термін VPN тут використовується дещо в іншому значенні. Класична технологія VPN забезпечує передачу інформації по зашифрованим тунелях поверх протоколу третього (мережного) рівня. Шифрування робить неможливим читання сторонніми адреси та вмісту переданого пакета. Зашифрована інформація передається по мережі і розшифровується вузлом-одержувачем.

MPLS VPN - це теж приватні віртуальні канали, подібно IPsec або PPTP (Point-to-Point Tunneling Protocol) VPN, але на цьому вся їх схожість і закінчується. У MPLS VPN немає ніякого шифрування. Пакети "ховаються" від сторонніх очей, оскільки передаються за маршрутом міток MPLS. Трафік з певними мітками читають тільки маршрутизатори LSR (Label Switch Routers), що знаходяться на маркірованому маршруті. Звичайні способи IP-маршрутизації в мережі MPLS не застосовуються - трафік передається тільки уздовж траєкторій тегів. Подібний рівень безпеки забезпечується і в мережах ATM і Frame Relay, де інформація "подорожує" по віртуальних каналах теж в незашифрованому вигляді. Але, власне кажучи, ніхто не забороняє вам додатково шифрувати пакети MPLS

4.3. **Безпека в мережах MPLS-VPN**

Функціональність MPLS-VPN підтримує рівень безпеки, еквівалентний безпеки оверлейних віртуальних каналів в мережах Frame Relay і ATM. Безпека

в мережах MPLS-VPN підтримується за допомогою поєднання протоколу BGP і системи дозволу IP-адрес.

BGP-протокол відповідає за поширення інформації про маршрути. Він визначає, хто і з ким може зв'язуватися з допомогою багатопротокольних розширень і атрибутів community. Членство в VPN залежить від логічних портів, які об'єднуються в мережу VPN і яким BGP присвоює унікальний параметр Route Distinguisher (RD). Параметри RD невідомі кінцевим користувачам, і тому вони не можуть отримати доступ до цієї мережі через інший порт і перехопити чужий потік даних. До складу VPN входять тільки певні призначені порти. У мережі VPN з функціями MPLS протокол BGP поширює таблиці FIB (Forwarding Information Base) з інформацією про VPN тільки учасникам даної VPN, забезпечуючи таким чином безпеку передачі даних за допомогою логічного поділу трафіку.

Саме провайдер, а не замовник присвоює порти певної VPN під час її формування. У мережі провайдера кожен пакет асоційований з RD, і тому спроби перехоплення пакету або потоку трафіку не можуть привести до прориву хакера в VPN. Користувачі можуть працювати в мережі інтранет або екстранет, тільки якщо вони пов'язані з потрібним фізичним або логічним портом і мають потрібний параметр RD. Ця схема надає мережам Cisco MPLS-VPN дуже високий рівень захищеності.

В опорній мережі інформація про маршрути передається за допомогою стандартного протоколу Interior Gateway Protocol (IGP), такого як OSPP або IS-IS. Прикордонні пристрої PE в мережі провайдера встановлюють між собою зв'язки-шляху, використовуючи LDP для призначення тегів. Призначення міток для зовнішніх (для користувача) маршрутів поширюється між PE-Маршрутизатор не через LDP, а через багатопротокольна розширення BGP. Атрибут Community BGP обмежує рамки інформації про доступність мереж і дозволяє підтримувати дуже великі мережі, не перевантажуючи їх інформацією про зміни маршрутної інформації. BGP не оновлюється інформацію на всіх

периферійних пристроях PE, що знаходяться в провайдерської мережі, а приводить у відповідність таблиці PIB тільки тих PE, які належать до конкретної VPN.

Якщо віртуальні канали створюються при оверлейної моделі, вихідний інтерфейс будь-якого індивідуального пакету даних є функцією тільки входить інтерфейсу. Це означає, що IP-адреса пакета не визначає маршруту його передачі по магістральній мережі. Це дозволяє запобігти попаданню несанкціонованого трафіку в мережу VPN і передачу несанкціонованого трафіку з неї. У мережах MPLS-VPN пакет, що надходить в магістраль, в першу чергу асоціюється з конкретною мережею VPN на підставі того, за якого інтерфейсу (подин-терфейс) пакет вступив на PE-маршрутизатор. Потім IP-адреса пакета звіряється з таблицею передачі (forwarding table) даної VPN. Зазначені в таблиці маршрути відносяться тільки до VPN прийнятого пакета. Таким чином, вхідний інтерфейс визначає набір можливих вихідних інтерфейсів. Ця процедура також запобігає як попадання несанкціонованого трафіку в мережу VPN, так і передачу несанкціонованого трафіку з неї.

4.4. **Висновок**

Розроблена комп'ютерна мережа на основі технологія MPLS для організації єдиного протоколу передачі даних як для додатків з комутацією каналів, так і додатків з комутацією пакетів (маються на увазі програми з дейтаграмному передачею пакетів). Вона може бути використана для передачі різного виду трафіку, включаючи IP-пакети, осередки ATM, фрейми SONET / SDH, і кадри Ethernet.

ВИСНОВКИ

В роботі проаналізовані характеристики технології MPLS, особливості архітектури комп’ютерної мережі на основі технології MPLS, якість обслуговування в комп’ютерній мережі на основі технології MPLS, віртуальні приватні мережі VPN, віртуальні приватні VPN мережі на основі технології MPLS.

Показано, що технологія MPLS поєднує в собі можливості управління трафіком, властиві технологіям канального рівня, і масштабованість і гнучкість протоколів, характерні для мережевого рівня. MPLS з'єднала в собі надійність ATM, зручні і потужні засоби доставки і забезпечення гарантованої якості обслуговування IP-мереж, така інтеграція мереж дозволяє отримати додаткову вигоду від спільного використання IP та ATM.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Гольдштейн А. Б., Гольдштейн Б. С. Технология и протоколы MPLS СПб. : БХВ — 2005. — 304 с . : ил.
2. Олвейн, Вивек. Структура и реализация современной технологии MPLS. : Пер. с англ. – М. : Издательский дом «Вильямс», 2004. – 480 с.
3. RFC 3468. The Multiprotocol Label Switching (MPLS) Working Group decision on MPLS signaling protocols. L. Andersson, G. Swallow. February 2003.
4. RFC 3031. Multiprotocol Label Switching Architecture. E. Rosen, A. Viswanathan, R. Callon. January 2001. 61 c.
5. RFC 3035. MPLS using LDP and ATM VC Switching. B. Davie, J. Lawrence, K. McCloghrie, E. Rosen, G. Swallow, Y. Rekhter, P. Doolan. January 2001. 20 c.
6. Armitage Grenville. MPLS: the magic behind the myths / Armitage Grenville // IEEE Communications Magazine, , January 2000. - vol. 38, no. 1. – ст. 54 – 63.