УДК 621.391

АНАЛІЗ ПРИНЦИПІВ ПОБУДОВИ MPLS L3 VPN

Литовченко К.А., Романов О.І.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського
E-mail: konstantinlitovchenko02@gmail.com; a_i_romanov@ukr.net

MPLS L3 VPN construction principles analysis

This article explores building a VPN network that runs on the third layer of the OSI model, based on the transmission protocol using MPLS tags. Description of the MPLS protocol. The overall infrastructure of a VPN system that benefits from such a system based on MPLS tags compared to using IPv4. More and more telecom representatives are moving to MPLS L3 VPN based jobs. The solution can be justified by a well-designed network architecture, high quality of service (QoS) and the degree of security of such a system.

У даній статті досліджується побудова VPN мережі, яка працює на третьому рівні моделі OSI, на базі протоколу передачі за допомогою міток MPLS. Опис роботи протоколу MPLS. Загальна інфраструктура системи VPN, виграш такої системи побудованої на основі міток протоколу IPMPLS у порівняні з використанням протоколу IPv4. Все більше представників телекомунікаційної сфери переходять на роботу, яка основана на MPLS L3 VPN. Рішення можна обґрунтувати добре продуманою архітектурою мережі, високою якістю послуг (QoS) та ступінню захищеності такої системи.

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

VPN на базі MPLS 3 рівня використовує однорангову модель, котра базується на протоколі граничного шлюза (BGP) для передачі інформації. Ця масштабована однорангова модель дозволяє корпоративним абонентам розповсюджувати дані про маршрутизації інших постачальників послуг, що приводить до значної економії ресурсів та зниженню складності операцій. Також система реалізована на протоколі MPLS, не потребує налаштувань всіх BGP на кожному маршрутизаторі, а лише на граничних роутерах, підключених до інших клієнтів або провайдерів, на відміну від IPv4. В VPN на базі IP використовується екземпляр віртуальної маршрутизації/ пересилання наступного покоління (VRF), званий Easy Virtual Network (EVN). Це спрощує віртуалізацію мережі рівня 3 і дозволяє клієнтам забезпечити поділ трафіку й ізоляцію шляху в загальній мережі інфраструктури, усуваючи необхідність розгортання MPLS в мережі підприємства. EVN повністю інтегрований з традиційним MPLS-VPN або MPLS VPNomGRE.[1]

MPLS дозволяє створювати віртуальні приватні мережі Layer 3, не вдаючись дотунелюванні (GRE) та шифрування (IPsec). MPLS VPN мережу ділить на дві області: IP мережі клієнтів і магістраль провайдера. Класична конструкція MPLS L3 VPN складається з наступних компонентів: граничні маршрутизатори провайдера PE, звернені до клієнтського обладнання CE, з'єднані між собою P маршрутизаторами в MPLS домені. В принципі, P маршрутизаторів може і не бути, необхідно щоб забезпечувалася зв'язність між PE.

MPLS L3 VPN інфраструктура (рис.1) передбачає забезпечення ізоляції розподілених клієнтських IP мереж в рамках VPN. Тобто забезпечується тільки обмін пакетами між IP мережами однієї VPN.

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

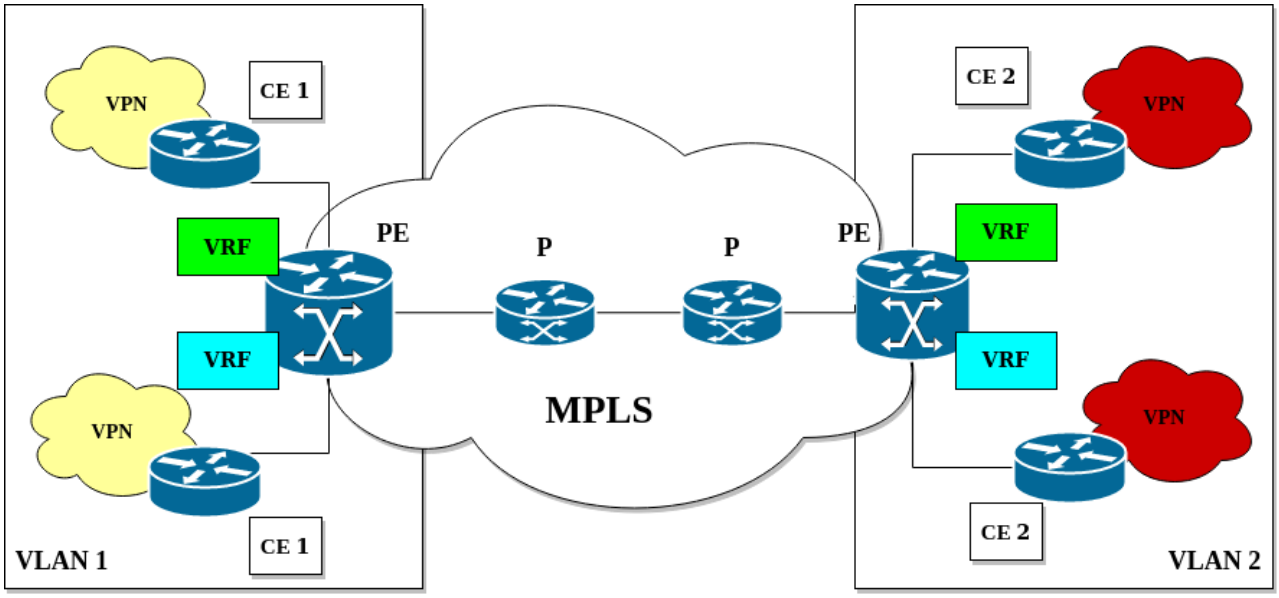

Рис. 1. Схема передачі VRF повідомлення між VLAN 1 та VLAN 2
за допомогою протокола MPLS.

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

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

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

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

які входить даний сайт, IPv4 маршрути (префікси) перетворюються в VPN-IPv4 маршрути і поміщаються в MP-BGP. MP-BGP згідно з політикою імпорту/експорту пов'язує між собою всі PE маршрутизатори (їх VRF). У підсумку в VRF різних PE, але належать одній VPN, потрапляють всі маршрути з даної VPN. Причому в записах VRF Next-Hopі є PE, який ніби пов'язаний між собою (віртуально за допомогою MPLS) [2].

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

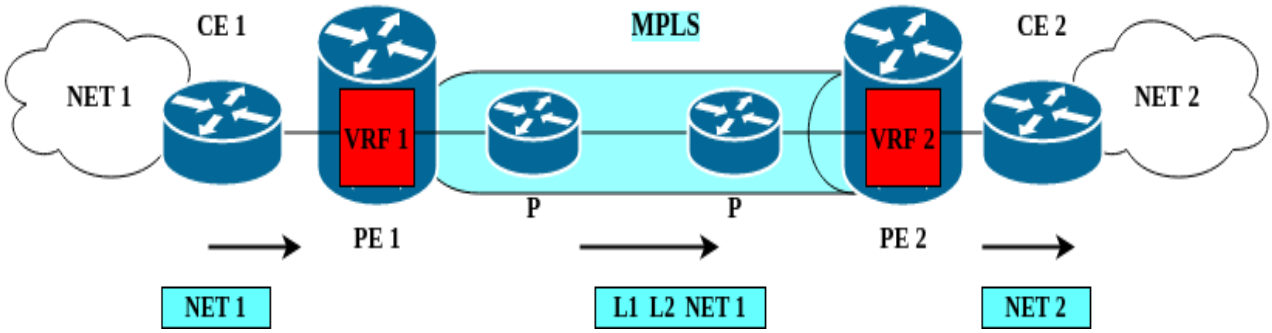

Рис. 2. Схема передачі MPLS пакетів по L3 VPN.

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

Отже, було продемонстровано роботу протоколу MPLS в мережі VPN L3. Збільшується швидкість передачі даних за рахунок пропуску налаштувань всіх BGP на кожному маршрутизаторі, MPLS забезпечує повне розмежування адрес та передачі даних. Дана мережа є достатньо захищеною від зовнішніх загроз, проте її можна покращити вдаючись до тенулювання (GRE) та шифрування.

Література

1. Layer 3 VPNs [Електронний ресурс] – Режим доступу до ресурсу: https://www.cisco.com/c/en/us/products/ios-nx-os-software/layer-3-vpns-l3vpn/index.html
2. Базовые сервисы технологии MPLS [Електронний ресурс] — Режим доступу до ресурсу: https://nag.ru/articles/reviews/15448/bazovyie-servisyi-tehnologii-mpls.html