ТЕХНОЛОГИЯ MPLS L3VPN

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Скрипелёва А.А.

Саломатин С.Б. – к.т.н.,доцент

На сегодняшний день большинство организаций и предприятий имеют территориально распределенную структуру, вследствие чего возникает необходимость объединения локальных вычислительных сетей территориально распределенных филиалов в одну корпоративную сеть. Кроме того, существуют проблемы защиты информации, аутентификации и авторизации пользователей, предоставления доступа к ресурсам, обеспечение независимости адресных пространств. Эти задачи в настоящее время помогает решить технология виртуальных частных сетей VPN (Virtual Privat Network).

Под термином VPN понимают круг технологий, обеспечивающих безопасную и качественную связь в пределах контролируемой группы пользователей по открытой глобальной сети. Цель создания VPN сводится к максимальной степени обособления потоков данных одного предприятия от потоков данных всех других пользователей сети.

MPLS (Multiprotocol Label Switching) — механизм передачи данных, который эмулирует различные свойства сетей с коммутацией каналов поверх сетей с коммутацией пакетов. MPLS работает на уровне, который можно было бы расположить между вторым (канальным) и третьим (сетевым) уровнями модели OSI. Основным преимуществом MPLS считается ускорение скорости продвижения пакетов в ядре сети. MPLS позволяет создавать Layer 3 VPN, не прибегая к туннелированию и шифрованию.

Построение MPLS L3VPN преследует следующие задачи: обеспечение защиты соединения, требуемого качества обслуживания и расширяемость инфраструктуры.

Для решения поставленных задач представлено три компонента MPLS L3VPN:

1. Компонент для разделения маршрутизируемых данных пользователей: VRF (Virtual Routing and Forwarding).
2. Компонент для обмена маршрутизируемыми данными пользователей: MP-BGP (Multiprotocol BGP).
3. Компонент для гибкого управления маршрутизируемыми данными: TE.

Traffic Engineering (TE) — это возможность управления направлением прохождения трафика с целью выполнения определенных условий (резервирование каналов, распределение загрузки сети, балансировка и предотвращение перегрузок).

Основной механизм TE в MPLS — использование однонаправленных туннелей (MPLS TE tunnel) для задания пути прохождения определенного трафика.

На рисунке 1 показан путь передачи пакетов MPLS L3VPN, создаваемой провайдером.

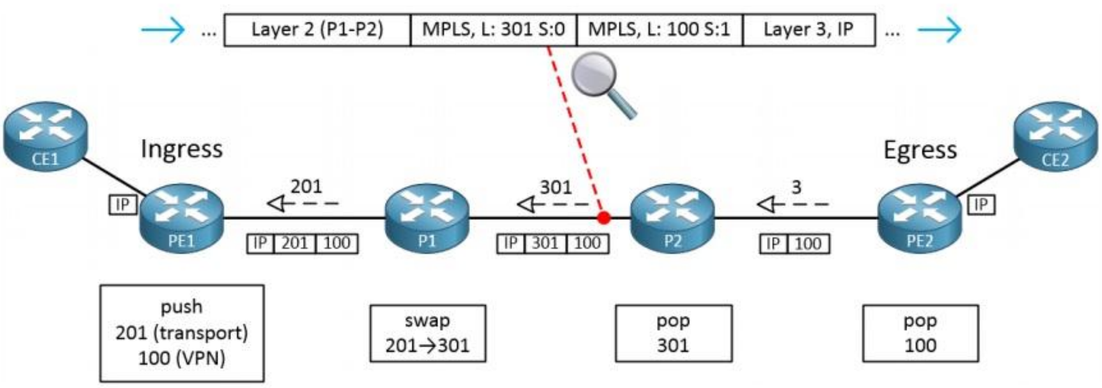

Рис. 1 - Путь передачи пакетов MPLS L3VPN

В состав опорной части сети (core network) входят P-маршрутизаторы (латинская буква «P» обозначает провайдера). В терминологии MPLS эти P-маршрутизаторы называются коммутирующими по меткам маршрутизаторами (Label Switch Routers — LSR). Передача осуществляется с помощью свопинга меток, а управление — с помощью протокола распределения меток (Label Distribution Protocol). Эти маршрутизаторы не осведомлены о существовании виртуальных частных сетей (VPN) и не участвуют в BGP-обмене, который происходит на PE-маршрутизаторах.

PE-маршрутизаторы (периферийную часть сети провайдера) должны присваивать пакету начальную метку при его поступлении в опорную сеть MPLS (MPLS core) и удалять эту метку в момент, когда пакет покидает сеть.

CE-маршрутизаторы (периферия сети заказчика) подключаются к PE-маршрутизаторам и не требуют специальной модификации для поддержки MPLS-VPN.

PE-маршрутизаторы связываются друг с другом по многопротокольному BGP для обмена информацией о подключенных VPN.

Каждое устройство MPLS PE поддерживает по одной таблице VRF (таблица маршрутизации и передачи VPN). MPLS-устройство идентифицирует маршруты, относящиеся к определенной сети VPN с помощью «различителя маршрутов» (Route Distinguisher — RD), который присваивается всем маршрутам соответствующего CE. Эти «различители» (RD) имеют значение только для PE-устройств, так как P-маршрутизаторы коммутируют ячейки или пакеты на основании информации, заключенной в метках.

Магистральная адресация, которая используется для подключения P-маршрутизаторов, полностью отделена от адресации, используемой для подключения CE-маршрутизаторов. Эти две схемы маршрутизации никак не взаимодействуют между собой. PE-маршрутизаторы сохраняют адреса опорной сети в глобальной таблице маршрутизации, которая хранится отдельно от таблиц VRF, где находятся данные обо всех маршрутах каждой VPN, к которой подключены сайты CE. Каждая таблица VRF имеет так называемую «политику импорта» (import policy), которая определяет, какие обновления PE следует принять, и «политику экспорта» (export policy), определяющую, какие маршруты следует объявлять.

Когда PE-устройство присваивает метку на границе сети MPLS, эта метка точно определяет весь маршрут, по которому будет передаваться данный пакет в этой сети. Это происходит потому, что LDP уже определил, какая входящая метка будет заменяться на соответствующую исходящую метку на каждом P-маршрутизаторе с тем, чтобы пакет был доставлен в конечный пункт назначения. Поэтому MPLS представляет собой форму маршрутизации от источника, так как только на периферии принимается решение о маршруте.

Каждый пограничный маршрутизатор заказчика должен инжектировать свои маршруты в соответствующие таблицы VRF, определенные в MPLS-сети для данной VPN. Эта задача выполняется пограничными маршрутизаторами заказчика, настроенными на передачу информации о маршрутах, необходимых другим сайтам своей же VPN. Для этой передачи может использоваться статическая маршрутизация, а также маршрутизация BGP.

Применение технологии MPLS дает возможность маршрутизируемым магистралям провайдера поддерживать VPN-сети и обеспечивает прозрачность механизмов 3-го уровня даже через инфраструктуры 2-го уровня. Такой подход позволяет создавать закрытые пользовательские группы и связанные с ними службы.

Список использованных источников:

1. Cisco Systems, Построение виртуальных частных сетей (VPN) на базе технологии MPLS
2. Бехингер М. Безопасность MPLS VPN. – Индианаполис: Cisco Press, 2005. – 312с.
3. Гейн Л. Основы MPLS. – Индианаполис: Cisco Press, 2007. – 651 с.