УДК 621.3

ТУННЕЛИРОВАНИЕ И ВИРТУАЛЬНЫЕ ЧАСТНЫЕ СЕТИ НА ОСНОВЕ MPLS

Гаттуров В.К., Цыпанов В.А.
Институт телекоммуникационных систем
E-mail: v.tsipanov@hotmail.com

Tunneling and VPNs based on MPLS

This article deals with the architectural VPN solutions in packet-switched networks. It is demonstrated that almost all solutions except MPLS-VPN are insufficient for traffic multiplexing, good QoS and data encapsulation. Also in article compares the tunneling principle for these solutions.

Наиболее универсальным способом построения VPN является использование технологии инкапсуляции, или туннелирования. В общем случае туннелирование применяется для того, чтобы передавать пакеты одной сети (первичной) по каналам связи другой (вторичной), протоколы которых не совместимы. Для этого пакеты первичной сети (данные и протоколы) инкапсулируется в пакеты вторичной сети, и становятся видны как данные. Таким образом, пакет продвигается маршрутизаторами ядра сети только на основании внешнего заголовка, без инспекции содержимого оригинального пакета. Далее приводится краткое описание наиболее распространенных решения по туннелированию при создании виртуальных частных сетей.

Протокол PPTP. Протокол PPTP (Point-to-Point Tunneling Protocol) позволяет инкапсулировать (упаковывать или скрыть от использования) пакеты PPP в пакеты протокола Internet Protocol (IP) и передавать их по сетям IP (в том числе и Интернет).

Протокол PPTP обеспечивает безопасную передачу данных от удаленного клиента к отдельному серверу предприятия путем создания в сети TCP/IP частной виртуальной сети. Протокол PPTP может также использоваться для организации туннеля между двумя локальными сетями.

Протокол L2TP. Протокол L2TP (Layer 2 Tunneling Protocol) - протокол туннелирования канального уровня, который позволяет организовывать VPN с заданными приоритетами доступа, однако не содержит в себе средств для защиты данных и механизмов аутентификации.

Протокол L2TP использует сообщения двух типов: управляющие и информационные сообщения. Управляющие сообщения используются для установления, поддержания и ликвидации туннелей и вызовов. Для обеспечения доставки ими используется надежный управляющий канал протокола L2TP. Информационные сообщения используются для инкапсуляции кадров PPP, передаваемых по туннелю. При потере пакета он не передается повторно.

Протокол IPSec. Другой очень популярный протокол для построения VPN - IPSec в режиме туннелирования. Напомним, что туннельный режим устанавливается для шлюзов и является, по существу, IP-туннелем с аутентификацией и шифрованием. Им предусматриваются два набора IP-заголовков: внешний и внутренний. Первый содержит IP-адрес VPN-шлюза, тогда как второй - IP-адрес конечной системы.

Протокол IPSec может быть полезен для любой VPN даже без его туннельных свойств: какой бы тип VPN ни применялся, если нужно спрятать информацию от чужих глаз, то можно воспользоваться транспортным режимом IPSec поверх основного транспорта.

MPLS VPN. Технология MPLS позволяет пересылать данные с помощью меток, прикрепляемых к каждому пакету. Внутренние узлы ядра сети, поддерживающие MPLS, не нуждаются в анализе содержимого каждого пакета. Так, не рассматривается IP-адрес получателя, что дает возможность MPLS предоставить эффективный механизм инкапсуляции для частного трафика, передаваемого по магистрали оператора. Имея это в виду, сформированные протоколом распределения меток (Label Distribution Protocol, LDP) маршруты продвижения пакетов от отправителей к получателям (Label Switched Path, LSP) нередко рассматривают как туннели через всю сеть MPLS или через ее магистральную часть.

Основой любого решения является использование LSP-туннеля для продвижения данных между фронтальными маршрутизаторами поставщика услуг, которыми ограничивается определенная VPN. Присваивая метки соответствующим пакетам, LER и LSR надежно отделяют VPN-потоки от остальных данных, передающихся по магистрали. Это разделение представляет собой ключевой механизм, посредством которого MPLS может поддерживать следующие характеристики VPN-туннелирования:

- инкапсуляция данных независимо от применяемых протоколов, поскольку пакеты передаваемые по туннелю непрозрачны для промежуточных маршрутизаторов, формирующих магистраль;
- мультиплексирование трафика различных VPN, передаваемого по разделяемой магистрали, посредством использования отдельных LSP-туннелей для каждого источника данных;
- аутентификацию конечных точек LSP-туннелей с помощью протоколов распределения меток (LDP);
- обеспечение необходимого уровня QoS путем резервирования сетевых ресурсов для LSP-туннеля. MPLS поддерживает как IntServ, так и DiffServ;
- надежную коммутацию и автоматическое перенаправление LSP-туннеля за счет исключения неисправного канала или маршрутизатора без вмешательства администратора.

Сравнительный анализ туннелей MPLS и обычных туннелей. Туннели MPLS позволяют передавать данные любого протокола вышестоящего уровня (например IP, IPX, кадры Frame Relay, ячейки ATM), так как содержимое пакетов вдоль всего пути следования пакета остается неизменным, меняются только метки. В отличие от них, туннели IPSec поддерживают передачу данных только протокола IP, а протоколы PPTP и L2TP позволяют обмениваться данными по протоколам IP, IPX или Net BEUI. Безопасность передачи данных в MPLS обеспечивается за счёт определённой сетевой политики, запрещающей принимать пакеты, снабжённые метками, и маршрутную информацию VPN-IP от непроверенных источников. Она может быть повышена использованием стандартных средств аутентификации и/или шифрования (например шифрование IPSec). Для безопасной передачи данных в протокол IP Security включены определенные процедуры шифрования IP-пакетов, аутентификации, обеспечения защиты и целостности данных при транспортировке, вследствие чего туннели IPSec обеспечивают надежную доставку информационного трафика.

Протокол L2TP поддерживает процедуры аутентификации и туннелирования информационного потока, а PPTP помимо данных функций снабжен и функциями шифрования. Применение меток MPLS позволяет реализовать ускоренное продвижение пакетов по сети провайдера. Транспорт MPLS не считывает заголовки транспортируемых пакетов, поэтому используемая в этих пакетах адресация может носить частный характер. Содержимое пакетов не считывается и при передаче IP-пакетов по протоколам IPSec, PPTP и L2TP. Однако, в отличие от MPLS, традиционные протоколы туннелирования для транспортировки IP-пакетов используют традиционную IP-маршрутизацию. При выборе пути следования пакета в MPLS учитываются различные параметры, оказывающие влияние на выбор маршрута. Совместная работа технологии многопротокольной коммутации и механизмов Traffic Engineering позволяет для каждого туннеля LSP предоставить требуемый уровень качества обслуживания за счет процедуры резервирования ресурсов на каждом маршрутизаторе вдоль пути следования пакета. Помимо этого, появляется возможность отслеживать действительный маршрут, проходящий через сформированный туннель, возможность диагностики и административного контроля туннелей LSP. Различные туннели, в соответствии с необходимым уровнем QoS между двумя точками поддерживает и протокол L2TP.

Технология VPN IPSec не поддерживает параметров качества обслуживания установленного соединения, а протокол PPTP поддерживает единственный туннель между двумя точками. Нельзя не отметить и тот факт, что весь трафик при использовании традиционных IP-туннелей следует до адресата вдоль одного и того и того же пути. Технология MPLS позволяет контролировать потоки, передаваемые по множеству всех имеющихся путей до адресата.

В качестве вывода покажем, какие возможности предоставляют туннели в MPLS:

1. Возможность формирования LSP-туннелей с или без требований QoS.
2. Возможность динамически изменять маршруты сформированных LSP туннелей.
3. Возможность отслеживать действительный маршрут, проходящий через сформированный LSP туннель.
4. Возможность идентифицировать и диагностировать LSP туннели.
5. Возможность устанавливать сформированный LSP туннель под административный контроль.
6. Возможность осуществлять посылку запросов выделения меток, их рассылку и объединение.

И как следствие MPLS-VPN предлагает улучшенную производительность по сравнению с IP-VPN, потому что, у вас есть возможность разделить ваши данные на различные категории, такие как реальное время трафика, приоритет трафика, низкий приоритет трафика и так далее. Ваш оператор мобильной связи будет поддерживать эти приоритеты по всей своей сети, обеспечивая качество обслуживания в любом конце. Также MPLS поддерживает высокий уровень безопасности, так как трафик сегментирован от других пользователей на сети оператора.

Литература

1. Семенов Ю.А. «Телекоммуникационные технологии». – «Москва», 2014. – 600с.
2. А.Б. Гольдштейн, Б.С. Гольдштейн «Технология и протоколы MPLS». – «БХВ – Санкт-Петербург», 2005. – 306с.
3. Вивек Олвейн «Структура и реализация современной технологии MPLS», «Москва», 2010 г. – 606с.