Санкт-Петербургский государственный университет
телекоммуникаций им. проф. М.А. Бонч-Бруевича

Кафедра СК и РИ

ДИПЛОМНАЯ РАБОТА

«Анализ и сравнение подходов к предоставлению широкополосных услуг на базе технологии MPLS»

Студентка
5 курс, гр. СК-04 **М.А. Маколкина**

Руководитель
Н.с. ЛОНИИС **к.т.н. А.Б. Гольдштейн**

Санкт-Петербург
2005

Реферат

Работа посвящена сравнению подходов к предоставлению широкополосных услуг, реализуемых на основе технологии MPLS.

Пояснительная записка состоит из 95 страниц, 18 рисунков.

Перечень ключевых слов: технология MPLS, VPN-MPLS, VPLS.

Дипломная работа посвящена анализу и сравнению существующих на момент написания работы подходов построения виртуальных частных сетей на базе MPLS. Работа содержит описание работы сети MPLS, а также описание работы виртуальных частных сетей, построенных на технологиях VPN-MPLS и VPLS. В работе разрабатываются критерии сравнения рассматриваемых технологий. Производится сравнение и анализ по разработанным критериям VPN-MPLS и VPLS. Как результат сравнения рассматриваются варианты применения изучаемых подходов, которые имеют практическое значение.

Основными практическими результатами работы является исследование технологий VPN-MPLS и VPLS. Разработка критериев сравнения и анализ технологий.

Содержание

Введение

Современное общество характеризуется проникновением бизнеса во все области человеческой жизни. При этом в деловом мире можно наблюдать две неоспоримые тенденции – к укрупнению бизнеса и к всё большей роли, которую в нём играют современные системы коммуникации. Действительно, управление большой компанией может быть успешным только в случае согласованности действий её структурных подразделений. Кроме того надо помнить, что глобальная сеть Интернет давно уже перестала быть только сетью передачи данных и даже её ценность, в качестве кладезя информации, с точки зрения делового сообщества, также отходит на задний план. Интернет сегодня – это одновременно и активный потребительский рынок, и товарная и валютная биржа: ежедневно в сети совершаются сделки на астрономические суммы.

Но современные услуги связи необходимы не только деловым заказчикам, связь всё чаще используется рядовыми пользователями: она становится доступом к популярным развлечениям, элементом престижа, средством заработка и т.д.

По мере развития и усложнения услуг связи, они обычно становятся более требовательны к ресурсам сети связи, на базе которой они предоставляются. Вследствие этого термин «современные услуги связи» часто неразделим с понятием «широкополосные услуги связи». Востребованность таких услуг привела к революционному изменению современных телекоммуникационных сетей и задачей любого оператора и провайдера услуг становится нахождение оптимального способа их предоставления с наибольшей выгодой для себя и с наилучшим качеством для заказчика.

Одной из технологий, способствовавших упомянутой революции является технология MPLS. Несмотря на свой достаточно молодой возраст, она стала уже очень популярной и ей даже пророчат место технологии

передачи данных в т.н. сетях следующего поколения NGN. Успех технологии MPLS вызван тем, что она позволяет эффективно управлять сетями, построенными на базе наиболее значимого и распространённого протокола – IP. Эта технология сейчас внедряется в сетях многих российских компаний, а в высокоразвитых странах начинает доминировать в сетях передачи данных. Именно это послужило побудительным моментом выбора темы дипломной работы – рассмотреть возможность предоставления широкополосных услуг связи именно на базе технологии MPLS.

Предоставление широкополосных услуг можно условно подразделить на две отдельных задачи: организация широкополосного доступа и организация такой инфраструктуры опорной сети оператора, что позволит осуществлять трансляцию широкополосного трафика в сеть доступа. MPLS – технология магистральных сетей, поэтому приводимые в настоящей работе исследования будут посвящены только второй из указанных задач.

Основной сетевой структурой для предоставления широкополосных услуг в магистральной сети давно стали разнообразные виртуальные сети, позволяющие разделить пользователей узкополосных и широкополосных услуг, управлять качеством при предоставлении широкополосных услуг и оптимизировать использование ресурсов сети.

В рамках технологии MPLS на текущий момент существует три возможных варианта организации виртуальных сетей: это BGP-MPLS VPN, VR VPN и VPLS. Первые два подхода относятся к классу VPN, организуемых на третьем уровне модели OSI, а последний – к классу VPN, организуемых на втором уровне. Низкая распространённость и прогнозируемое отсутствие перспектив у подхода VR VPN позволяет ограничить исследование только двумя подходами.

В дипломной работе будет рассмотрена ситуация на рынке широкополосных услуг и дана её краткая характеристика. Также будут проанализированы сетевые технологии, которые могут быть использованы оператором для предоставления широкополосных услуг и наибольшее

внимание будет, разумеется, уделено технологии MPLS. Затем будут исследованы и проанализированы оба указанных подхода к предоставлению широкополосных услуг, и после будут выработаны критерии, по которым можно будет произвести сравнительный анализ BGP-MPLS VPN и VPLS и дать оценку применимости того или иного подхода в каждом конкретном случае. Таким образом, исследование должно, с возможной в рамках дипломной работы глубиной, осветить проблему выбора провайдером сетевой технологии для предоставления широкополосных услуг различным клиентам.

1. Широкополосные услуги

1.1. Существующий рынок широкополосных услуг

В течение долгого времени основной услугой, которую предлагали операторы, была телефония**.** Также предоставлялись услуги по передачи данных и видеоизображений, но гораздо в меньшей степени. В последнее время ситуация изменилась и трафик передачи данных превысил речевой. Это послужило толчком к началу новой эры в телекоммуникациях – эры интегрированных решений и конвергенции видов связи.

Современный этап развития мировой цивилизации характеризуется переходом от индустриального к информационному обществу, предлагающему новые формы социальной и экономической деятельности, базирующиеся на массовом использовании информационных и телекоммуникационных технологий. Сегодня клиентов уже не удовлетворяет имеющиеся услуги по передачи речи, данных, видео. Для сохранения конкурентоспособности и получения дополнительных доходов оператору необходимо расширять спектр услуг за счет введения новых. Уровень развития сетевых технологий позволяет операторам предлагать по-настоящему привлекательные в маркетинговом плане широкополосные услуги. Что касается состава широкополосных услуг, то как отмечают зарубежные специалисты, в нем объединяются три составляющие: высокоскоростной Интернет (двусторонний, разумеется), мультисервисные сети ПД с большим охватом (WAN) и интерактивное видео. Далее более подробно будут рассмотрены эти три составляющие широкополосной связи, а также другие услуги, являющиеся продолжением этих трех.

Сегодня сложно представить современную компанию, не использующую телекоммуникации. Одной из важнейших составляющих телекоммуникационного обеспечения любой компании - от малой до большой - является широкополосный доступ в сеть Интернет. «Высокоскоростной доступ в Интернет» на сегодняшний день одна из

наиболее востребованных услуг. Ведущие компании предоставляет услугу постоянного подключения к сети Интернет по выделенной линии (по беспроводной линии или на базе технологий xDSL), или полупостоянного подключения через коммутируемые сети (Frame Relay, IP, ATM), по сегменту локальной сети Ethernet.

Все больший интерес вызывает услуга «Дистанционное обучение», которая выросла из услуги «Высокоскоростного доступа в Интернет», и в основе которой лежит замечательная идея устранить барьеры расстояний и дефицита времени для всех, кто хотел бы получить образование или повысить свою квалификацию. Услуга «Дистанционного обучения» предусматривает организацию широковещательных мультимедийных сессий, разнородных конференций (речевых, видео, данных), а также возможность ведения интерактивного диалога с обучающим сервером через Public Internet.

«Video on demand» (Vod) – Видео по запросу – это услуга, позволяющая просматривать и заказывать видео, не выходя из дома. В основном эта услуга использует принципы «pay-per-view». Пользователи, как правило, имеют специальное устройство, называемое set-top-box, подключаемое к телевизору, которое и реализует услугу со стороны заказчика. Пользователям предлагается меню, при помощи которого они удаленно выбирают и заказывают программу. Стоимость услуги перечисляется на счет. Видео и аудио составляющие (данные) сжимаются и посылаются по линии заказчику услуги, где Set-top-box их декодирует. Услуга может предоставляться как в широковещательном режиме, так и в режиме уникастного вещания на индивидуальное приемное устройство set-top-box. Заказчику услуги VoD обычно требуется по меньшей мере в 10 раз большая полоса пропускания в сети IP, чем заказчику услуги передачи данных или голосовых услуг.

«Pay-per-view» - название, которое получила система, позволяющая телевизионным зрителям звонить и заказывать программы, которые они хотели бы посмотреть по телевизору и оплачивать частное вещание

программ у себя дома позже. Программы показываются в определенное время всем заказавшим эту программу, в отличие от услуги «Видео по запросу», где каждый заказчик выбирает программу и смотрит её в выбранное им самим время и как правило программа передается только для него одного.

Различие между услугой «Видео по запросу» и «Pay-per-view» состоит в том, что пользователь может приостановить, перемотать, ускорить какой-то отрывок или остановить передачу данных в момент просмотра и выбрать просмотр с начальной точки, заказав услугу VoD.

Сильный толчок для развития «HDTV» – телевидение высокой точности получило с приходом широкоэкранного кино. Очевидно, что использование подобного экрана, занимающего большое поле зрения (особенно периферийного), значительно увеличивает чувство «присутствия на месте события». HDTV предполагает широкую полосу телевизионного сигнала и позволяет использовать разрешение большее, чем традиционные форматы.

«Мультивещание видео». Услуга мультивещания видеопотоков обеспечивает передачу качественного видео для пользователей телевизоров и персональных компьютеров. Пользователи могут просматривать видеопоток, возможно, прямо в web-странице, и одновременно обращаться к другим услугам, на которые они подписаны. Провайдеры услуг могут спроектировать web-страницы для управления внешним интерфейсом и организацией услуги. Например, они могут связать дополнительную текстовую и графическую информацию с видеопотоками и отображать их на той же web-странице, на которой отображается видео. Другим примером может быть предоставление пользователю статистики по игроку и команде в процессе просмотра спортивного состязания.

«Потоки с web-камер». С их помощью мобильные пользователи могут визуально наблюдать за удаленными объектами. Данную услугу могут взять на вооружение и охранные агентства, предлагая дополнительные

возможности по обеспечению безопасности жилищ с использованием визуального мониторинга посредством web-камер (WebCam).

«Услуги с самостоятельным управлением». Клиентские интерфейсы на основе WEB позволяют предоставить пользователям непосредственный контроль над управлением и предоставлением услуг. Например, клиент, которому срочно потребовались средства видео-конференций, может немедленно получить доступ и заплатить за требуемую пропускную способность. Самостоятельное управление услугами может оказаться выгодным для провайдера услуг за счет:

• повышения степени удовлетворения конечных пользователей благодаря более высокому качеству обслуживания;

• сокращения объема усилий, предпринимаемых со стороны провайдера для предоставления и обеспечения услуги;

• возможности покупки услуг под влиянием сиюминутного желания;

• увеличения потока денежных средств за счет немедленного «онлайнового» выставления счетов / оплаты услуг.

«Видеотелефония» является услугой аудиовизуальной связи в режиме реального времени, которая позволяет осуществлять симметричную передачу голоса и цветных динамических изображений между двумя и более точками. Особенно актуальной эта услуга является для организаций, имеющих географически удаленные подразделения. При использовании услуги «Видеотелефонии» сотрудникам удаленных филиалов не приходится периодически выезжать в командировки для проведения деловых встреч, что экономически выгодно для компаний.

Другая услуга, весьма похожая на услугу «Видеотелефонии», также являющаяся эффективным инструментом оптимизации бизнес-процессов управления территориально распределенной компанией – «Видеоконференц-связь». Приложения для видеоконференций позволяют осуществлять обмен видео- и аудиоинформацией с одновременным показом графиков и таблиц, снабженых средствами совместного редактирования документов и передачи

файлов. Основная задача, которую решает видеоконференц-связь для территориально распределенных компаний - это существенное сокращение временных и финансовых затрат на организацию и проведение расширенных выездных совещаний оперативного характера с участием руководителей структурных подразделений.

IP-телефония – в узком смысле этого термина, это услуга передачи речевой информации по сетям передачи данных, базирующихся на сетевом протоколе IP. За счёт более эффективного использования полосы пропускания каналов, обеспечиваемого технологией коммутации пакетов и применением современных методов кодирования речи, IP-телефония позволяет сделать услугу передачи речи более экономичной, по сравнению с традиционными сетями с коммутацией каналов. Также преимуществом использования IP-телефонии является возможность предоставления телефонных услуг и услуг передачи данных с использованием единой сетевой инфраструктуры, что снижает капитальные и эксплуатационные расходы оператора.

Технологические подходы к предоставлению IP-телефонии с самого начала учитывали, что хотя формально услуга будет называться IP-телефонией, но сам её смысл будет расширен и она будет, по сути, услугой мультисервисной связи. Это нашло своё отражение уже в первой открытой технологии IP-телефонии, описанной в рекомендации H.323 комитета ITU-T. Более совершенные технологии, такие как, SIP и H.248/MEGACO ещё больше расширили понятие о мультисервисности. Поэтому хотя саму услугу передачи речи по сетям IP можно отнести скорее к узкополосным услугам, но возможности реализующих её технологий по передаче мультимедийной информации и организации мультимедийных сессий автоматически переводят её в ранг широкополосных услуг пользователя. Также IP-телефонию можно отнести к широкополосным услугам, если она предоставляется не одному конкретному пользователю, а группе

пользователей (например, IP PBX), для которых организуется общий широкополосный канал.

«Телемедицина» - обмен медицинской информацией, в том числе и данными, полученными от медицинского оборудования с использованием средств электронных коммуникаций. Использование компьютерной техники и различных телекоммуникационных технологий в медицинских целях привело к возникновению термина "телемедицина". Одним из главных достоинств телемедицины является возможность приблизить высококвалифицированную и специализированную помощь специалистов ведущих медицинских центров в отдаленные районы и существенно сэкономить затраты пациентов. Кроме того, очень важным "побочным" эффектом от использования телемедицины является обучение врачей отдаленных районов в процессе регулярного консультирования. В настоящее время под собственно телемедициной понимается проведение телеконсультаций или консультаций на расстоянии, например, когда пациент находится в одном городе/поселке (а иногда даже стране), а врач-консультант в другом.

«Услуга nPVR» (network based Personal Video Recorder) позволяет организовать на сервере провайдера виртуальный персональный видеомагнитофон с вещанием по принципу VoD и стандартными функциями управления. Виртуальный видеомагнитофон позволяет организовывать видеоматериалы в памяти сервера как виртуальные "видеокассеты". Естественно, любая виртуальная видеокассета может быть "установлена" на один или несколько виртуальных видеомагнитофонов. Внутри каждой видеокассеты обеспечивается произвольный доступ к любому временному фрагменту. Используется для организации интеллектуальных систем безопасности и обучения.

Услуга «IP-VPN» предназначена для клиентов, которым требуется объединение локальных компьютерных сетей удаленных офисов в единую сеть. Характерным свойством большинства корпоративных сетей на

сегодняшний день является их территориально распределенная структура, вследствие чего, возникает задача объединения территориально распределенных филиалов предприятия и компьютеров удаленных сотрудников в одну сеть. Таким образом корпоративный клиент получает высокоэффективную мультисервисную транспортную сеть для передачи информации любого типа (данные, голос, видео) с хорошим качеством услуг.

Новая услуга, которая рассматривается в качестве следующего этапа эволюции VPN, - это VPLS (Virtual Private LAN Services) или VPN уровня 2. Услуги виртуальных локальных частных сетей дают возможность объединить распределенные локальные сети в единую сеть. При этом сеть оператора связи абсолютно «прозрачна» и не видна для сети заказчика, что позволяет строить ее так, как будто операторской сети не существует. В результате заказчик получает полный контроль над собственной сетью и её функционированием.

Очевидно, что многие из вышеперечисленных услуг интегрированы друг с другом, т.е. существует корреляция между услугами. Действительно можно долго перечислять различные широкополосные услуги, предоставляемые операторами, на самом же деле деление на услуги весьма условно, это всего лишь грамотное маркетинговое решение. С точки зрения транспортных сетей предоставление большинства услуг сводится к передачи данных с гарантированной доставкой в разных режимах вещания. Таким образом, для сети оператора все многообразие услуг представляется очень схожим.

1.2. Способы предоставления широкополосных услуг

Ведущие операторы для предоставления широкополосных услуг используют уже давно известные и активно применяющиеся технологии, такие как Ethernet, Frame Relay, ATM. Рассмотрим эти технологии, а именно их особенности, позволяющие предоставлять широкополосные услуги.

ATM – это технология коммутации ячеек и мультиплексирования, в которой объединены преимущества коммутации каналов (гарантированная

пропускная способность и постоянная задержка передачи сигнала) и пакетов (гибкость и эффективность для пульсирующего потока данных). ATM обеспечивает масштабирование полосы пропускания от нескольких мегабит до многих гигабит в секунду. Из-за асинхронного режима передачи ATM эффективнее, чем синхронные технологии, такие как TDM, т.к. в ATM временные интервалы предоставляются по требованию с идентификацией источника передачи, т.е. происходит управление полосой пропускания. ATM передает данные в пакетах фиксированной длины, что особенно хорошо подходит для передачи речевого и видео трафика, поскольку эти виды трафика не допускают задержек вследствие ожидания загрузки большого пакета данных. Сети ATM ориентированы на соединение, т.е. каждой передаче данных предшествует установка виртуального канала. Существует два типа соединений ATM: виртуальные каналы, которые могут объединяются в виртуальные маршруты, которые, в свою очередь, проходят по каналу передачи. Главные преимущества этой технологии – её зрелость, надежность и наличие развитых средств эксплуатационного управления сетью. В ней имеются непревзойденные по своей эффективности механизмы управления качеством обслуживания и контроля использования сетевых ресурсов. Однако ограниченная распространенность и высокая стоимость оборудования не позволяют считать ATM лучшим выбором для предоставления широкополосных услуг.

Frame Relay – это сетевой протокол, который работает на двух нижних уровнях эталонной модели OSI. Он является представителем технологии коммутируемых пакетов, которая позволяет конечным станциям динамически распределять ресурсы, т.е. среду передачи и доступную полосу пропускания. Сети Frame Relay передают данные, используя два типа соединения: коммутируемые виртуальные каналы и постоянные виртуальные каналы. Несколько виртуальных каналов можно объединить в один физический для передачи данных по сети. Это свойство часто позволяет упростить сеть и сократить количество оборудования. Frame Relay позволяет

снизить нагрузку на сеть благодаря простым механизмам оповещения о заторах, используемым вместо явного управления потоком каждого виртуального канала. В 1990 году были разработаны некоторые дополнения к Frame Relay, что позволило расширить несколько функций, предназначенных для управления сложными объединенными сетями. Основными из них являются: глобальная адресация, сообщение о состоянии виртуального канала, многоадресные рассылки, которая позволяет создавать групповые адреса и экономить полосу пропускания. В сетях FR используется обычный механизм проверки ошибок (циклическая проверка четности с избыточностью). За счет проверки ошибок, а не их исправления, нагрузка на сеть сокращается. Однако сети Frame Relay имеют ограниченные возможности дальнейшего развития.

Термином **Ethernet** обозначают семейство продуктов локальных сетей, описываемых стандартом IEEE 802.3, который определяет протокол CSMA/CD (множественный доступ с контролем несущей и обнаружением коллизий). Технология Ethernet не предусматривает организацию виртуальных каналов. Технология Ethernet является наиболее распространенной технологией локальных сетей. На сегодняшний день часто широкополосные услуги реализуются непосредственно в локальной сети. Т.к. локальные сети имеют достаточно простую структуру, то нет необходимости в поддержании специальных механизмов управления полосой пропускания, управления отказами, управления способом кодирования, обеспечения QoS и т.д. Тем не менее протокол Ethernet обладает следующими свойствами: простота, легкость реализации, управления и обслуживания; дешевизна сетей; значительная топологическая гибкость при установке сетей; гарантия успешного взаимодействия между продуктами совместимых стандартов независимо от производителя. Также технология Ethernet используется для организации каналов передачи данных на отдельных звеньях сети доступа.

Несомненно, что возрастающий спрос клиентов на предлагаемые широкополосные услуги повлек за собой появление различных технологий, предлагающих данные виды сервиса. В связи с протеканием процесса конвергенции эти решения должны соответствовать уровню требований, предъявляемых конвергентными сетями. Это должны быть надежные, безопасные сети, отвечающие требованиям по качеству обслуживания при передаче разнотипного трафика. К сожалению, существующие технологии не решают проблем, возникших с началом предоставления широкополосных услуг, и не всегда удовлетворяют требованиям заказчика. Среди вновь появляющихся технологий хотелось бы выделить технологию многопротокольной коммутации по меткам MPLS. Эта технология обладает большой гибкостью в предоставлении новых услуг, масштабируемостью и рядом других достоинств. На базе MPLS активно разрабатываются и внедряются такие подходы к предоставлению широкополосных услуг VPN – MPLS, VPLS, которые буду подробно рассмотрены в главе 3.

1.3. Проблемы передачи разнотипного трафика

Предоставление рассмотренных в первом параграфе широкополосных услуг требует определенного качества, причем для каждой услуги параметры качества различны и определены в специальных документах отрасли, руководящих документах и т.д. Технологии, описанные в параграфе два, призваны обеспечить требуемое качество услуг, для этого они обладают специальными механизмами. Тем не менее, до последнего времени сети передачи данных, голоса и видео строились независимо друг от друга, базировались на разных технологиях и инфраструктурах, а как известно, информационные потоки разных приложений требуют разных уровней обслуживания или типов качества.

Каждому типу трафика требуется свой, определенный уровень качества обслуживания, соответственно технологии обладают различными механизмами обеспечения требуемого качества обслуживания, так в технологии ATM определены 5 классов услуг, которые характеризуются

набором параметров. Так, например, класс UBR позволяет пользователю передавать трафик с изменяемой в зависимости от объема информации скоростью, как, например, при организации мультимедийной почты по e-mail. Для оптимального использования сетевых ресурсов здесь применяется статическое мультиплексирование. А в технологии Frame Relay организация управления нагрузкой в узле осуществляется с использованием прямого и обратного явного уведомления о перегрузках. Вопрос о качестве услуги зачастую связан с соглашениями об уровне обслуживания, которые обычно описываются на трех параметрах: на доступности услуги, на задержках в сети, на пропускной способности. В соглашениях обычно оговаривается гарантированность доставки определенного процента трафика.

Развитие технологии транспортировки информации привело к тому, что появилась возможность создать такую сеть, которая обеспечила бы удовлетворительные характеристики в смысле передачи информации для практически всех без исключения приложений - от публичной телефонии и интерактивного видео до опроса электросчетчиков. NGN - сеть связи следующего поколения - это мультисервисная сеть, обеспечивающая передачу всех видов медиатрафика, и распределенное предоставление неограниченного спектра телекоммуникационных услуг, с возможностью их добавления, редактирования, распределенной тарификации. Сеть поддерживает передачу разнородного трафика с различными требованиями к качеству обслуживания и обеспечивает соответствующие требования. Таким образом мы можем наблюдать процесс конвергенции, происходящий в современных сетях. В общем случае, под конвергенцией понимают слияние сетей передачи речи и видео с сетями передачи данных, и в первую очередь с Интернет, с целью предоставления одинакового набора услуг пользователям любой сети. Работа по созданию сетей NGN ведется с учетом трех основных требований:

- обеспечение передачи трафика реального времени
- обеспечение передачи данных

- предоставление гарантированного качества обслуживания

При этом выделяют три основных направления работ:

- создание единой транспортной инфраструктуры, реализующей обеспечение гарантированного QoS.
- организация доступа к сети
- единое управление сетью.

Следует отметить, что на сегодняшний день еще не создано единой системы управления, правда уже существует и активно внедряется устройство, которое будет управлять всеми соединениями в сети NGN - Softswitch.

Сеть доступа

В процессе конвергенции сетей, продвигаются и начинают активно внедряться устройства мультисервисного доступа, позволяющие операторам внедрять новые услуги.

Транспортная сеть

Перед транспортным уровнем NGN стоит задача объединения технологий, связанных с различными протоколами и интерфейсами таким образом, чтобы наиболее экономично удовлетворить потребности в скорости, пропускной способности и качестве обслуживания передаваемого трафика.

Сегодня наиболее развитыми технологиями являются технологии IP и ATM. В силу того, что эти технологии имеют много недостатков, они не подходят в качестве решения для транспортной сети. Так, протокол IP, прекрасно удовлетворяет первому требованию, а благодаря технологии VoIP (передаче речи по IP сетям) и второму, но в протоколе IP не предусмотрено функций по обеспечению гарантированного качества обслуживания, соответственно, IP не может быть взят в качестве транспортной технологии сети NGN. В качестве транспортной технологии сети будущего подходит технология MPLS – многопротокольная коммутация на основе меток. Данная технология удовлетворяет заявленным требованиям и не обладает

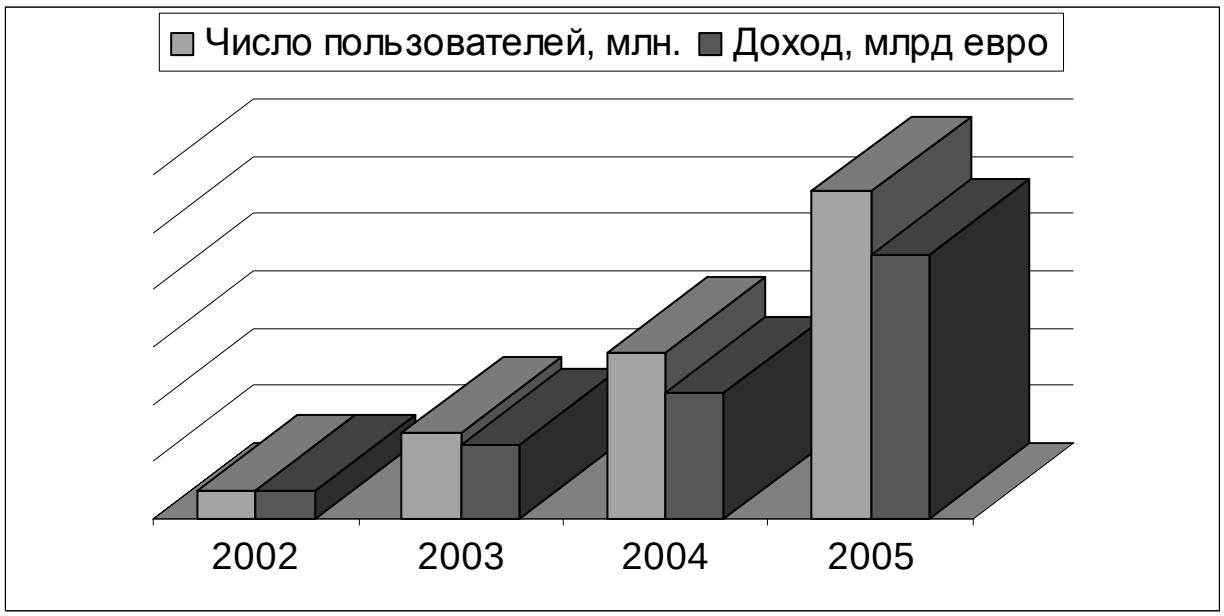
недостатками технологий IP и ATM, кроме того, сам механизм коммутации по меткам в ней реализован весьма удачно.

Качественное обслуживание разнотипного трафика в MPLS реализуется за счет использования механизмов Traffic Engineering. Применение Traffic Engineering позволяет организовать для передачи трафика различных приложений свой туннель LSP в соответствии с необходимым этому потоку уровнем QoS.

Подробно технология MPLS будет рассмотрена во 2 главе данной работы.

1.4. Актуальность темы дипломной работы

В связи с тем, что в последние годы интерес к широкополосным услугам сильно возрос, большинство ведущих телекоммуникационных компаний стараются наиболее качественно предоставить весь спектр услуг. Если раньше, говоря о широкополосных услугах, в основном имели в виду интеграцию речи и данных, то сегодня к ним все чаще добавляют видео. Причем видеоприложения начинают играть ключевую роль: они не только делают пакет услуг более привлекательным, но и значительно расширяют круг его потенциальных потребителей. Как видно из рисунка 1.1 число пользователей услуги «видео по запросу» в Западной Европе увеличивается с каждым годом.



Год	2002	2003	2004	2005
Число пользователей, млн.	0,5	1,5	2,9	5,7
Доход, млрд евро	0,15	0,4	0,7	1,5

Рис.1.1. Рынок услуг «видео по запросу» в Западной Европе

По информации TIA (Telecommunication Information Agency), совокупный оборот в телекоммуникационной отрасли США увеличился в прошлом году на 4,7% и достиг 720 млрд долларов, причем в отношении таких услуг, как унифицированные коммуникации, аудио- и видеоконференции, высокоскоростной доступ в Интернет, рост превысил 10%. Росту телекоммуникационного рынка способствует развитие услуг передачи данных (в том числе услуг на базе технологий IP, включая широкополосный доступ и виртуальные частные сети) и голосовых услуг, на долю которых сегодня приходится около двух третей доходов отрасли. Значительно возрастут и объемы данных, передаваемых в корпоративных сетях. Вследствие чего технологии VPN и VPLS входят в группу важнейших технологий, которые предприятия собираются использовать в ближайшем будущем.

Возможно, виртуальные частные сети станут основой для поддержки услуг, предоставляемых сетями нового поколения, поэтому задача выбора технологии построения имеет большое значение.

В последнее время большую популярность приобрела технология MPLS. Данная технология позволяет строить виртуальные частные сети с гарантированным уровнем сервиса, а коммутация на основе меток реализует ускоренное продвижение информационного потока по сети провайдера. Передача трафика по туннелю MPLS дает требуемый уровень безопасности и снимает необходимость в дополнительном шифровании информации и других мерах защиты.

Все выше сказанное, говорит о том, что у технологий VPN MPLS и VPLS несомненно, есть будущее и рассмотрение и сравнение параметров этих технологий довольно актуальный вопрос.

2. Технология MPLS.

MPLS стала основной магистральной технологией нового века. Она позволяет эффективнее передавать большие объемы трафика в магистральных сетях и рассматривается как основа для конвергенции услуг и фундамент для построения мультисервисных сетей следующего поколения, в которых станет возможна передача разнородного трафика через интегрированную телекоммуникационную инфраструктуру вместо нескольких раздичных сетей. В сфере будущих телекоммуникаций MPLS уготована роль ведущей технологии. Она рассматривается в качестве фундамента для инфраструктуры сетей следующего поколения и предоставления новых услуг. Обладая целым рядом преимуществ, она была призвана дополнить «мир IP» достоинствами унаследованных инфраструктур frame relay, ATM и TDM, а также способствовать внедрению протокола IP как универсального транспорта для всех видов приложений. В случае применения MPLS в качестве базового механизма коммутации можно упростить развитие операторских сетей IP, объединить разные технологии доступа, повысить масштабируемость маршрутизации IP и сделать сети IP столь же пригодными для передачи голоса и видео, как сети ATM, где обеспечение качества и резервирование ресурсов для передачи разнородного трафика заложены на протокольном уровне. При том, что операторы достаточно взвешенно подходят к технологии MPLS, популярность ее растет. Многопротокольная коммутация информационных потоков в соответствии с метками (Multiprotocol Label Switching, MPLS) рассматривается как перспективная, хотя и не единственная основа для конвергенции услуг и построения мультисервисных сетей следующего поколения (NGN), в которых станет возможна передача разнородного трафика через интегрированную телекоммуникационную инфраструктуру вместо нескольких различных сетей. Принятие MPLS в качестве унифицирующей, замещающей технологии должно привести к значительному упрощению сетевых инфраструктур и управления ими. Внедрение MPLS позволяет

повысить уровень сервиса, предоставлять востребованные услуги на базе IP (с гарантированным уровнем качества) и услуги конвергентных сетей для корпоративных клиентов, включая создание виртуальных частных сетей (VPN) и передачу голоса поверх IP (VoIP). Инфраструктура MPLS VPN дает возможность соединять узлы по схеме «любой с любым» независимо от технологии доступа (frame relay, выделенная линия, DSL или Ethernet), повышает производительность, масштабируемость IP и надежность маршрутизации в приложениях Triple Play (голос, данные, видео). С MPLS хорошо сочетается Ethernet — благодаря такой комбинации открывается возможность экономичного предоставления целого комплекса услуг и внедрения широкополосных приложений в городских сетях и сетях доступа.

2.1. Общие принципы

Каждый пакет при использовании на сетевом уровне протокола, не предусматривающего создания виртуальных соединений, на своем пути следования передается независимо от одного маршрутизатора к другому. Соответственно, при определении маршрута следования пакета каждый маршрутизатор тратит свои ресурсы на анализ IP-заголовка. Возможность избежать этих затрат позволяет реализовать передачу пакетов по сети значительно быстрее.

В качестве технологии, обеспечивающей ускоренную передачу пакетов по сети, применяется технология MPLS. MPLS (Multiprotocol Label Switching) – это технология многопротокольной коммутации на основе меток.

Основной ценностью технологии MPLS является возможность организации в IP сети «виртуальных каналов», а также возможность переноса трафика одной сессии по нескольким «виртуальным каналам».

«Multiprotocol» в названии технологии означает многопротокольный. Это говорит о том, что технология MPLS применима к любому протоколу сетевого уровня, т.е. MPLS – это своего рода инкапсулирующий протокол,

способный транслировать информацию множества других протоколов высших уровней модели OSI. Технология MPLS остается независимой от протоколов уровней 2 и 3 в сетях IP, ATM и Frame Relay, а также, взаимодействует с существующими протоколами маршрутизации, такими как протокол резервирования ресурсов RSVP или сетевой протокол преимущественного выбора кратчайших маршрутов OSPF.

2.2. Основные понятия

Комитет IETF определил три основные элемента технологии MPLS:

- Метка
- FEC – класс эквивалентной пересылки
- LSP – коммутируемый по меткам тракт

Рассмотрим каждый из них подробно.

2.2.1. Метки

Метка - это идентификатор фиксированной длины, определяющий класс эквивалентной пересылки FEC. Метки имеют локальное значение, т.е. привязка метки к FEC используется только для пары маршрутизаторов. Метка используется для пересылки пакетов от верхнего маршрутизатора к нижнему, где, являясь входящей, заменяется на исходящую метку, имеющую также локальное значение на следующем участке пути.

Метка передается в составе любого пакета, при этом ее место в пакете зависит от используемой технологии канального уровня.

Протокол MPLS поддерживает различные типы меток: это может быть 4-байтовая метка MPLS, которая вставляется между заголовками канального и сетевого уровня. Это может быть метка идентификаторов виртуального канала и виртуального пути (VCI/VPI) или метка идентификатора соединения канального уровня (DLCI).

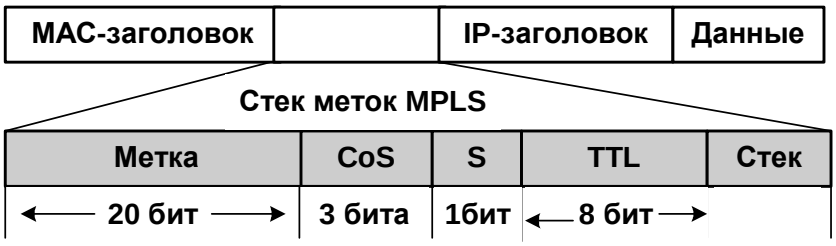


Рисунок 2.1.

Размер метки составляет 4 байта. Идентификатор самой метки занимает первые 20 бит.

Информация об уровне качества обслуживания в сети MPLS может передаваться в поле CoS, занимающем следующие три бита в поле метки. Это поле необходимо предназначено предоставления дифференцированных услуг в сети MPLS.

Последний бит (S) третьего байта используется для указания окончания стека меток.

Четвертый байт в формате поля метки занимает параметр TTL (Time to Live), который огнаничивает предельное время, существования пакета в сети, для защиты от образования петель и ограничения области распространения пакета.

Стек меток

Пакет, передаваемый по сети MPLS, как правило, содержит не одну, а несколько меток. Такой набор меток образует стек. Основное назначение стека меток – поддержание древовидности множества трактов LSP, заканчивающихся в одном входном LSR, а, кроме того, в том, чтобы использовать метки при создании так называемых LSP-туннелей.

Свойство древовидности сводится к следующему: если в одном LSR сливается несколько потоков пакетов, то этот LSR не заменяет метки, связанные с этими потоками, а оставляет их, помещая сверху метку нового FEC, который соответствует объединенному потоку пакетов, образующемуся в результате слияния.

Метки в стеке располагаются по принципу «последний пришел – первый вышел». Каждый маршрутизатор работает только с верхней меткой. Остальные метки стека передаются прозрачно до удаления вышестоящей.

Для переадресации пакета, поступающего на один из интерфейсов маршрутизатора, необходимо проведение двух процедур:

- Во-первых, необходимо определить следующий шаг маршрутизации.
- Во-вторых, нужно знать, какая операция требуется для стека меток. Это может быть операция извлечения метки из стека, замены метки в стеке.

После того, как из стека меток будет удалена последняя метка, дальнейшая обработка пакетов должна осуществляться на основе заголовка сетевого уровня.

Для создания таблиц коммутации по меткам используются разные методы:

- метод на основе топологии. Для создания таблиц в этом случае используются стандартные протоколы маршрутизации. К таким протоколам относятся OSPF, IS-IS, BGP.
- метод на основе запросов. Данный метод основан на работе управляющего протокола, на основе запросов (например, протокол RSVP).
- метод на основе трафика. В данном варианте создания меток процедура назначения и распределения меток запускается только после поступления пакета.

2.2.2. Класс эквивалентной пересылки FEC

FEC - это форма представления группы пакетов с одинаковыми требованиями к передаче по сети.

Как говорилось ранее, в заголовке IP-пакета содержится гораздо больше информации, чем требуется для выбора следующего маршрутизатора. Этот выбор можно организовать путем выполнения следующих двух групп функций в маршрутизаторе:

- маршрутизатор относит пакет к определенному классу FEC.
- ставит в соответствие каждому FEC следующий шаг маршрутизации.

В MPLS пакет ставится в соответствие определенному классу FEC только один раз на входе в сеть MPLS. Этому FEC присваивается метка, передаваемая затем вместе с пакетом при его пересылке к следующему маршрутизатору. В остальных маршрутизаторах заголовок пакета не анализируется. Определение FECs реализуется на основе требований к обслуживанию данной совокупности пакетов или просто адресного префикса.

Класс FEC представляет собой набор FEC-элементов, каждый из которых идентифицируется определенной меткой. На сегодняшний день для международного использования определено всего два FEC-элемента: Address Prefix и Host Address, но конкретные реализации учитывают массу других параметров.

При соотнесении пакетов по различным FEC большую роль играют IP-адреса, приоритеты обслуживания и другие параметры трафика. Каждый FEC обрабатывается отдельно, что позволяет поддерживать требуемое качество обслуживания в сети MPLS.

Коммутируемый по меткам тракт LSP

Коммутируемый по меткам тракт – это последовательность MPLS-маршрутизаторов и последовательность меток в них. По сути LSP представляет собой виртуальный канал в сети передачи данных.

Набор пакетов, передаваемый по LSP, относится к одному FEC, и каждый маршрутизатор LSR в LSP назначает для него свою метку. Иногда поток данных может быть настолько велик, что для него создается несколько LSP между отправителем и получателем.

Возможны два варианта создания LSP: по принципу hop-by-hop, который предполагает, что каждый маршрутизатор самостоятельно выбирает дальнейший путь следования пакета, или по принципу явной маршрутизации, в котором маршрутизаторы передают пакет в соответствии

с указаниями, полученными от верхнего, в данном тракте, LSR. Таким образом, в первом случае маршрут следования пакетов определяется случайным образом, а в случае явной маршрутизации он известен заранее.

В сети MPLS может существовать набор маршрутизаторов, которые являются входными для конкретного FEC, тогда, считается, что для этого FEC существует LSP с разными точками входа и выхода. Если для некоторых из этих LSP выходным является один и тот же LER, то можно говорить о дереве LSP, корнем которого служит данный выходной маршрутизатор.

LSP можно рассматривать как тракт, создаваемый путем сцепления одного и более участков маршрута, который позволяет пересылать пакет, заменяя на каждом узле сети MPLS входящую метку исходящей меткой (так называемый алгоритм перестановки меток). Таким образом, тракт сети MPLS можно рассматривать как туннель, для создания которого в IP-пакет вставляется заголовок – метка, о котором речь шла ранее.

LSP устанавливаются либо перед передачей данных (с управлением от программы), либо при обнаружении определенного потока данных (управляемые данными LSP).

На сегодняшний день применение туннелирования реализовано во многих технологиях. Образование в виртуальном тракте туннелей, по которым проходят другие виртуальные тракты, основывается на инкапсуляции передаваемых пакетов в пакеты, следующие по этому тракту к данному адресу назначения. LSP-туннели, широко используемые в технологиях поддержки широкополосных услуг в MPLS будут подробнее рассмотрены после описания принципов функционирования сети MPLS.

2.3. Принцип работы

Используя уже рассмотренные понятия, опишем функционирование сети MPLS. Любой IP-пакет на входе в сеть MPLS, независимо от того поступает этот пакет от отправителя или же он пришел из смежной сети, которая может быть MPLS-сетью более высокого уровня, относится к

определенному классу эквивалентной пересылки FEC (Forwarding Equivalence Class). Напомню, что анализ заголовка IP-пакета и назначение FEC производится только один раз на входе в сеть.

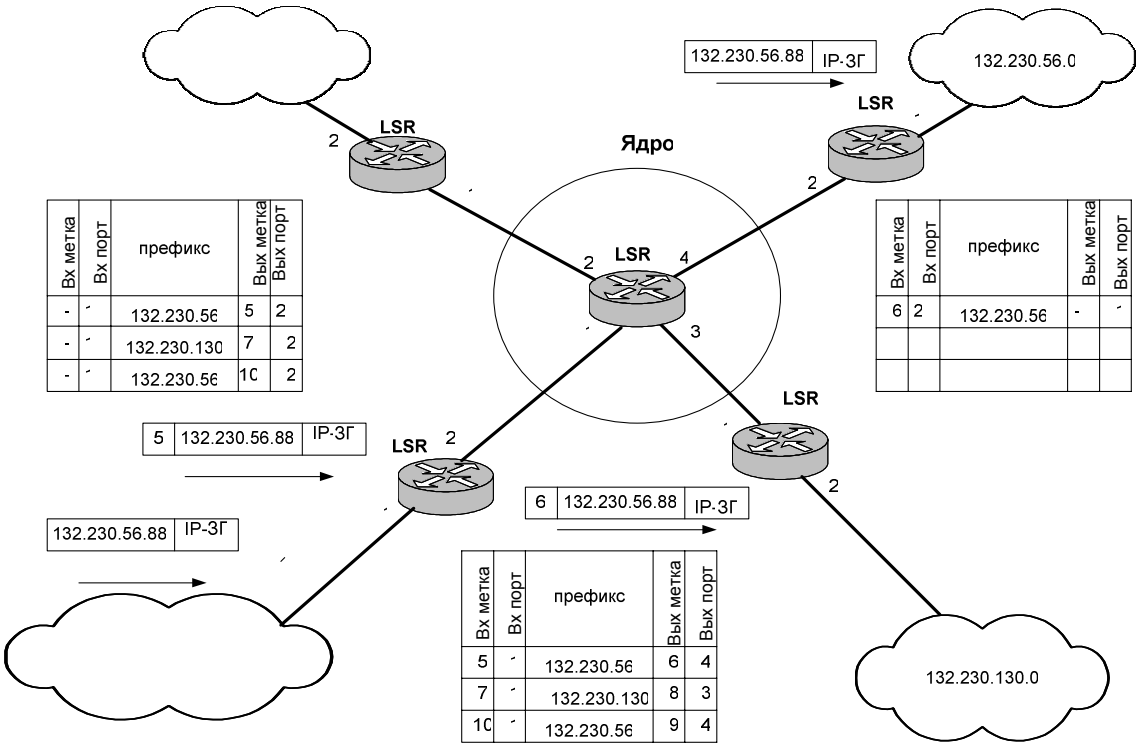


Рис 2.2. Сеть MPLS.

FEC идентифицируется определенной меткой, представляющей собой поле фиксированной длины, и имеющей локальное значение на участке между двумя соседними маршрутизаторами. При переадресации пакета на следующем шаге, метка посылается вместе с ним, таким образом, пакеты оказываются помеченными еще до того, как будут переадресованы. Принятая с пакетом метка используется маршрутизатором как указатель входа таблицы, которая определяет очередной маршрутизатор для пересылки к нему пакета, а также новую метку для FEC, к которому относится этот пакет. Модуль коммутации по меткам, как правило, заменяет содержащуюся в пакете метку, некоторой новой меткой перед ее пересылкой на следующий участок маршрута (label swapping). Для

принятия решения о том, куда пересылать пакеты, используется алгоритм точного совпадения меток.

Использование метки для переадресации пакетов в MPLS позволяет значительно снизить время обработки пакетов в маршрутизаторе.

Маршрутизатор, поддерживающий MPLS и способный, кроме того, анализировать заголовки и производить пересылку пакетов, не содержащих меток, называется маршрутизатором коммутации по меткам. Технология MPLS предусматривает наличие маршрутизаторов двух типов:

LER (Label Enge Routers) – пограничные маршрутизаторы MPLS.

LSR (Label Switching Routers) – транзитные маршрутизаторы MPLS.

В точке входа в сеть MPLS стоят пограничные маршрутизаторы, на которые возлагаются функции классификации пакетов по различным классам FEC и реализация всевозможных дополнительных услуг. Входной LER добавляет метку всем пакетам, поступающим в сеть MPLS, а выходной LER удаляет метку и, либо осуществляет маршрутизацию на основе IP-адреса, либо сам является адресатом. Таким образом, чтобы переадресовывать пакеты, LSR должен уметь работать с IP-заголовком.

Задача транзитных маршрутизаторов MPLS заключается в продвижении пакетов на основе меток, т.е., маршрутизатор должен принять пакет со вставленной меткой, в соответствие со своей таблицей маршрутизации заменить ее новой и отправить пакет к следующему LSR.

Любой маршрутизатор MPLS содержит базу меток LIB, благодаря которой пакеты и маршруты связываются между собой. Для получнной метки в базе LIB содержится точная запись о соответствующей исходящей метке, интерфейсе и информации об инкапсуляции канального уровня, необходимой для продвижения пакета. Основываясь на информации, полученной из базы LIB, LSR заменяет полученную им входящую метку на исходящую и передает пакет на выходной интерфейс. Эта операция повторяется при прохождении каждого LSR маршрутизатора.

Когда в LIB нескольких LSR накапливается информация, относящаяся к одному и тому же пункту назначения, создается так называемый «коммутируемый по меткам тракт», представляющий собой последовательность узлов меток в узлах на пути следования потока от отправителя к получателю. Тракт LSP между двумя маршрутизаторами является однонаправленным.

Для реализации маршрутизации в сети MPLS необходимо заполнить таблицы маршрутизации. Алгоритм маршрутизации работает по протоколу OSPF, IS-IS или BGP, либо при помощи явной маршрутизации (будет рассмотрена в параграфе Traffic Engineering). После выбора оптимального маршрута маршрутизаторы распределяют по нему метки. Метки в LSP раздаются с помощью протокола распределения меток LDP.

Высокоскоростная передача данных в MPLS обеспечивается за счет того, что метки фиксированной длины вставляются в начале пакета и могут использоваться аппаратными средствами для быстрой коммутации пакетов между каналами связи.

При коммутации пакетов возможен случай, когда маршрутизатор получает пакет с входящей меткой, которой нет в его базе LIB. В таких ситуациях пакет отбрасывается. Также возможны случаи, когда пакет поступает на маршрутизатор, в котором по какой-либо причине не может быть установлена связь между входящей и исходящей метками. В сложившейся ситуации возможны два выхода. Во-первых, можно продолжить маршрутизацию пакетов традиционным способом. Но этот вариант решения подходит не всегда, так как может привести к образованию петель, да и содержания IP-заголовка не достаточно для переадресации пакета. В силу этих обстоятельств приоритетным является второй вариант – отбрасывание пакета.

Замена меток

Для переадресации пакетов, содержащих метки, LSR анализирует верхнюю метку стека и на основе FEC этого пакета, а также LIB, принимает

решение о дальнейшем пути следования пакета. Если пакет является непомеченным, то есть не содержит в себе стека меток, то маршрутизация пакета проводится на основе IP-заголовка, определяя, таким образом, класс эквивалентности пакета. Затем, маршрутизатор определяет путь следования пакета.

От маршрутизатора MPLS требуется, чтобы он мог связать набор входящих меток с одной исходящей. Данная процедура называется объединением меток. LSR способен объединять метки, если он при получении пакетов с разными входными метками пересылает их с одной и той же выходной меткой. При этом информация о том, что они пришли от разных интерфейсов теряется.

В архитектуре MPLS допускается наличие как объединяющих и не объединяющих маршрутизаторов, так и маршрутизаторов не поддерживающих коммутацию на основе меток.

2.4. Распределение меток

С технической точки зрения, распределение меток с целью заполнения таблиц LIB и установление LSP являются синонимами.

Введем следующие определения:

- маршрутизатор LSR называют нижестоящим, или downstream, если он является выходным по направлению передачи трафика;
- маршрутизатор называют вышестоящим, или upstream, если он расположен в начале пути по направлению передачи.

Распределение меток всегда проводится нижестоящим маршрутизатором, после чего он информирует соответствующие вышестоящие маршрутизаторы о привязке меток к FEC, поступающих к нему пакетов. Обмен информацией о привязке меток может проводиться с помощью различных протоколов сигнализации.

Технология MPLS предлагает несколько режимов назначения и распространения меток:

В режиме *независимого* распространения меток каждый нижестоящий маршрутизатор самостоятельно привязывает входящую метку и распространяет ее как исходящую среди вышестоящих маршрутизаторов. При этом получение входящей метки перед созданием и распространением исходящей необязательно. Другой режим распространения меток – *упорядоченный*. В этом случае маршрутизатор передает метку вышестоящему LSR только после получения метки от нижестоящего маршрутизатора.

Следует отметить, что инициатором распределения меток может быть, как сам нижний маршрутизатор, так и верхний LSR передающий запрос нижнему. Эти режимы называются, соответственно, *unsolicited downstream* и *downstream-on-demand*.

Нижний маршрутизатор может распределять метки не только по верхним LSR, имеющим с ним прямые связи, но и LSR, между которыми существует коммутируемая связь. Результат распределения меток, при этом, зависит от того, в каком режиме работает верхний LSR: *консервативном* или *либеральном*.

При работе верхнего LSR в консервативном режиме привязка «метка-FEC», получаемая от маршрутизаторов, между которыми существует лишь коммутируемая связь, отбрасывается. Привязка принимается только от соседнего LSR.

В либеральном режиме верхний LSR принимает привязки меток к FEC как от смежных, так и от несмежных LSR.

Выбор маршрута

Выбор маршрута сопряжен с методом, используемым при выборе LSP для определенного класса FEC. Архитектура MPLS поддерживает два варианта выбора маршрута:

- традиционная маршрутизация
- явная маршрутизация

Традиционная маршрутизация позволяет каждому маршрутизатору независимо выбирать следующий шаг для каждого FEC, и полагаться только на свой алгоритм маршрутизации, обычно базирующийся на традиционных для IP-сетей протоколах маршрутизации.

При явной маршрутизации путь, по которому будет должен следовать трафик, задается отправителем. Явная маршрутизация дает возможность проводить политику маршрутизации и управление трафиком. Задача поиска путей при явной маршрутизации трафика возлагается на оконечные маршрутизаторы LER, а внутренние маршрутизаторы лишь передают им информацию о состоянии сети. На основе этой информации LER принимают решение о выборе пути. Каждый пограничный LSR может работать по своей версии алгоритма явной маршрутизации.

Традиционная и явная маршрутизация полностью совместимы. Каждый LSR может поддерживать один или другой тип маршрутизации одновременно. Следует отметить, что выбор одного из методов маршрутизации не оказывает какого-либо влияния на механизм коммутации на основе меток.

2.5. Протокол распределения меток LDP

Путь LSP может быть создан при помощи различных протоколов рассылки меток, в этом технология MPLS не накладывает каких-либо ограничений. Протокол рассылки меток представляет собой набор процедур и сообщений, с помощью которых один LSR информирует другие о привязках «метка-FEC», которые он сформировал, а также о всевозможных согласованиях, использующихся для обмена информацией о возможностях LSR. Основным протоколом распределения меток в MPLS определён LDP.

Протокол LDP предназначен в первую очередь для дублирования деревьев маршрутизации и преобразования их в деревья маршрутизации на основе меток. Протоколы OSPF, BGP и IS-IS вычисляют и распространяют дерево выбора кратчайшего пути (SPF) до адресата от любого источника. LDP копирует вычисленное дерево маршрутизации и для каждого канала в

дереве выделяет метку. В точках дерева, где ветви сходятся, метки объединяются.

Маршрутные таблицы формируются на основе дерева кратчайших путей. Эти таблицы содержат упорядоченный набор адресов места назначения и информацию о ближайших соседях.

При формировании коммутируемого по меткам тракта LSP в первую очередь осуществляется обнаружение LSR, с которыми возможно установление протокольной сессии. Протоколом LDP предусмотрено два режима обнаружения: базовый и расширенный. В первом случае обнаружение LSR осуществляется путем периодической отправки на порт UDP-646 по широковещательному IP-адресу 224.0.0.2. приветственных сообщений Hello. Передавая эти сообщения, маршрутизатор тем самым сообщает о том, что он готов к взаимодействию.

В случае, когда маршрутизаторы находятся не в одной сети, применяется расширенный метод обнаружения. В данном случае приветственное сообщение Hello направляется по определенному IP-адресу к конкретному узлу.

В приветственных сообщениях Hello передается идентификатор пространства меток, которое передающий данное сообщение маршрутизатор планирует использовать в дальнейшем, в процессе открытия соединения между LSR по протоколу TCP, а также вспомогательная информация.

После процедуры обнаружения маршрутизаторы устанавливают через порт 646 TCP-соединение и передают сообщение инициализации сеанса связи. В сообщении инициализации маршрутизаторы обмениваются информацией о поддерживаемой версии протокола, дисциплине распределения меток, их диапазоне и других параметрах. По завершении сеанса инициализации маршрутизаторы LSR обмениваются сообщениями KeepAlive, которые служат для поддержания LDP-сессии в активном состоянии. После установления сессии инициатор раздачи меток может послать сообщение с запросом на получение метки Label Request, в котором

описывается FEC передаваемого потока. Если на пути следования сообщения не возникло никаких осложнений, то от нижестоящего маршрутизатора будет послано сообщение Label Mapping, содержащее в себе локальное значение метки. В противоположном случае будет послано сообщение Notification, в котором должны содержаться причина отказа и указания к дальнейшим действиям. Если на всех вышестоящих маршрутизаторах привязка «метка-FEC» прошла успешно, то после обработки на входном пограничном маршрутизаторе сообщения Label Mapping, полученного от соседнего с ним нижестоящего маршрутизатора, тракт LSP считается установленным.

Передача сигнальных сообщений в протоколе реализуется пересылкой блока протокольных данных PDU. В каждом из таких блоков может быть передано одно или несколько сообщений.

Структуру PDU можно подразделить на два части: заголовок сообщения, в котором передаются версия протокола, длина блока LDP и поле, определяющее диапазон меток LSR; и само сообщение. Следует также отметить, что все параметры в протоколе LDP кодируются по схеме тип-длина-значение (TLV).

2.6. Туннели в MPLS

Применительно к MPLS мы будем говорить об LSP-туннелях, образуемых не путем инкапсуляции пакетов, а с помощью средств коммутации по меткам. LSP-туннель представляет собой последовательность $< LSR_1, LSR_2, ... , LSR_n >$, в котором LSR_1 является передающим конечным пунктом туннеля, а LSR_n - приемным конечным пунктом туннеля. Пакеты, подлежащие транспортировке через LSP-туннель, относятся к одному FEC, и каждый LSR туннеля назначает метку для этого FEC, то есть метку для туннеля. Чтобы направить пакет в LSP-туннель, маршрутизатор передающего конечного пункта туннеля помещает метку, назначенную для этого туннеля, поверх существующего в пакете стека меток (заметим, что и в данном случае

предпоследний маршрутизатор LSP-туннеля может уничтожить верхнюю метку в стеке до передачи пакета к приемному конечному пункту).

LSP-туннель создается внутри LSP. Существенно, что начало и/или конец туннеля, как правило, не совпадают с началом и/или концом этого LSP, туннель обычно бывает короче LSP, в котором он создан. В одном LSP может быть создано несколько LSP-туннелей одного уровня с несовпадающими передающими и/или приемными конечными пунктами. Более того, внутри любого из этих туннелей можно создавать LSP-туннели следующего уровня. Количество таких уровней, по тем или иным причинам, не может быть сколь угодно велико, однако иерархичность архитектуры MPLS в данном случае вполне очевидна. Осуществляется она с помощью стека меток. Механизм стека меток позволяет осуществлять иерархическое функционирование в сети MPLS. Он, в частности, позволяет использовать MPLS для осуществления одновременно маршрутизации как между отдельными маршрутизаторами внутри сети данного Интернет-провайдера, так и высокоуровневой междоменной маршрутизации. Каждый уровень в стеке меток относится к некоторому иерархическому уровню, что облегчает поддержку туннелирования в MPLS.

Под LSP *уровня m* понимается LSP, образуемый последовательностью маршрутизаторов $<LSR_{вх}, LSR_2, \ldots, LSR_{n-1}, LSR_{вых}>$ со следующими свойствами:

- входной маршрутизатор $LSR_{вх}$ помещает в стек меток обрабатываемого пакета такую по счету метку, что стек приобретает *глубину m;*
- при всех *i* ($1<i<n$) пакет, поступающий к LSR_i, имеет стек меток глубины *m;*
- в процессе транспортировки пакета от $LSR_{вх}$ к LSR_{n-1} глубина его стека меток никогда не бывает меньше *m*;
- при всех *i* ($1<i<n$) LSR_i передает пакет LSR_{i+1} средствами MPLS.

Иными словами, LSP *уровня m* представляет собой последовательность маршрутизаторов, которая начинается с входного LSR, вставляющего в пакет метку уровня *m*, содержит промежуточные LSR, каждый из которых принимает решение о пересылке пакета на основе метки уровня *m*, и заканчивается выходным LSR, где решение о пересылке принимается на основе метки уровня *m - k*, где *k*>0, или на основе обычных (не MPLS) процедур пересылки. Отметим, что от LSR_{n-1} к LSR_n можно передавать пакеты со стеком меток глубины (*m*-1), поскольку метка уровня *m* выходному LSR не требуется. Это позволяет избавить выходной LSR от операций анализа ненужной ему метки и не требует никаких дополнительных операций, кроме простого уничтожения в предпоследнем LSR верхней метки в стеке. Т.е. в сети MPLS могут образовываться LSP-туннели произвольной степени сложности. Если оператор должен вложить один LSP-туннель в другой LSP-туннель, то потоку назначается рассмотренный выше стек меток, как это показано на рисунке 2.3. В таких случаях MPLS-метки помещаются в стек меток на входе в каждый туннель и извлекаются из стека меток на выходе из туннеля. Последняя метка из стека будет извлечена тогда, когда поток придет на пограничный маршрутизатор на пути к адресату.

Таким образом, путем создания туннелей через несколько сетевых сегментов достигается уникальная возможность MPLS управлять всем трактом передачи пакета без специфицирования в явном виде промежуточных маршрутизаторов. В связи с этим рассмотрим несколько более общую схему, представленную на рисунке 2.4.

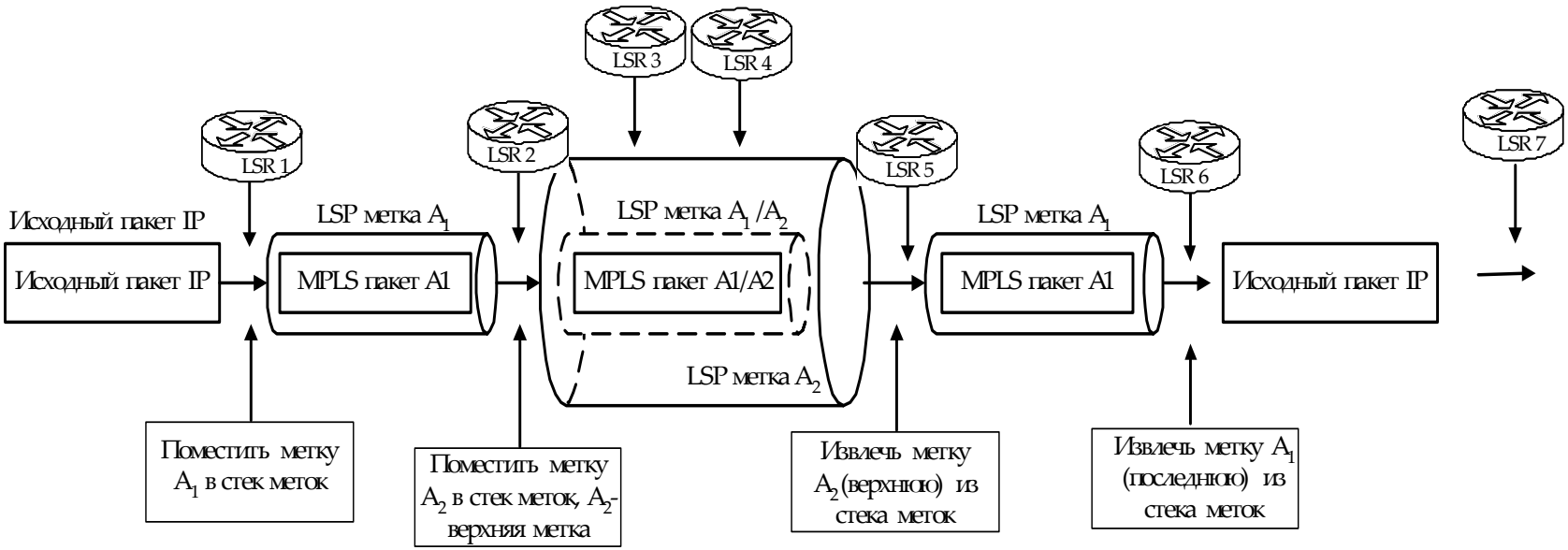


Рис.2.3. Туннелирование через LSP

Пусть здесь все пограничные маршрутизаторы MPLS (LSR1, LSR2, LSR3 и LSR4) используют протокол BGP и создают коммутируемый по меткам тракт LSP между ними (LSP1). LSR1 знает о том, что его следующий пункт назначения – LSR2, поскольку он передает данные от отправителя, которые должны пройти через два сегмента сети. В свою очередь, LSR2 знает о том, что его следующий пункт назначения – LSR3, и т.д. Эти пограничные LSR будут использовать протокол LDP для получения и хранения меток от выходного LSR4 вплоть до входного LSR1.

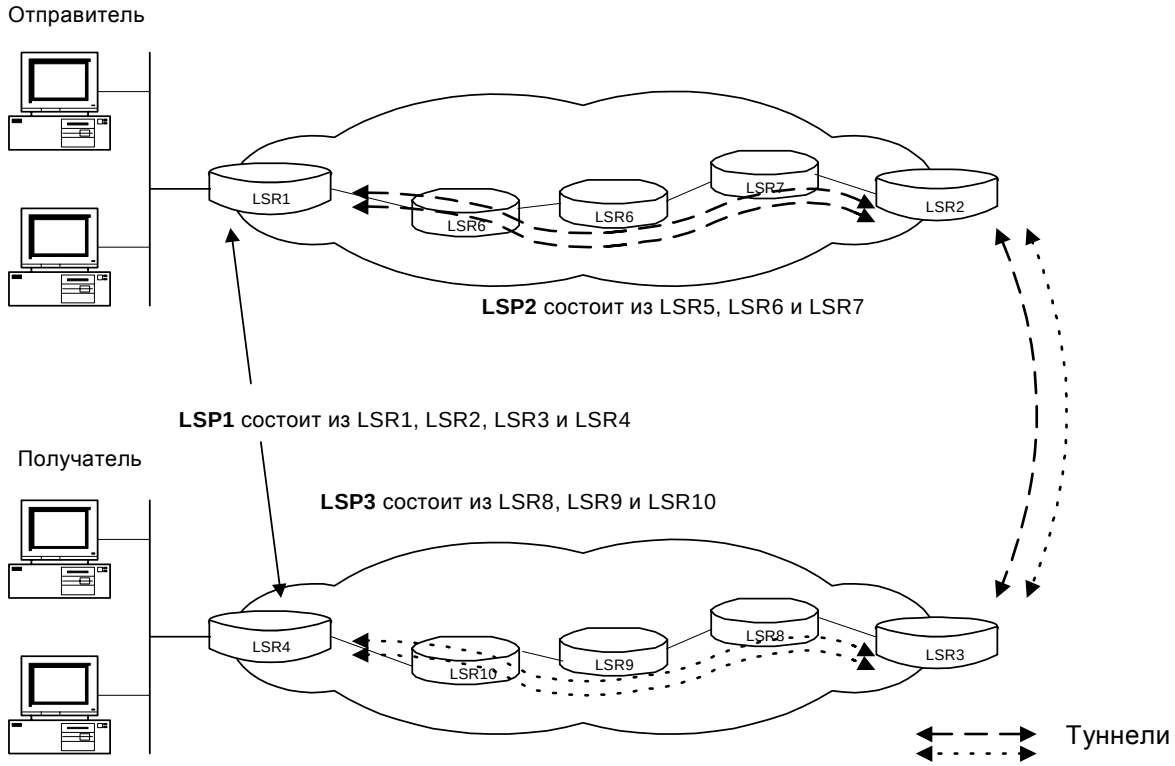


Рис.2.4. Туннели в сети MPLS

Однако, чтобы данные были переданы от LSR1 к LSR2, они должны пройти через несколько (в данном случае три) транзитных маршрутизаторов LSR. Таким образом, между двумя LSR (LSR1 и LSR2) создается отдельный тракт LSP (LSP2), который охватывает LSR5, LSR6 и LSR7. Он, в сущности, представляет собой туннель между этими двумя LSR. Метки в этом LSP отличаются от меток, которые LSR создали для LSP1. Это справедливо и для LSR3 и LSR4, равно как и для LSR, находящихся между ними. Для этого последнего сегмента создается тракт LSP3. Для достижения этого результата, т.е. для передачи пакета через два сетевых сегмента

используется изложенная в предыдущем параграфе концепция стека меток. Поскольку пакет должен следовать через LSP1, LSP2 и LSP3, он будет переносить одновременно две отдельные метки. Пары, используемые для каждого сегмента, следующие: для первого сегмента – метка для LSP1 и LSP2, для второго сегмента – метка для LSP1 и LSP3. Когда пакет покидает первую сеть и принимается пограничным маршрутизатором LSR3, тот удаляет метку для LSP2 и заменяет её на метку для LSP3, заменяя при этом метку LSP1 внутри пакета на метку следующей пересылки. Маршрутизатор LSR4 удаляет обе метки перед отправкой пакета адресату.

2.7. Traffic Engineering

Под термином Traffic Engineering понимают методы и механизмы достижения сбалансированности загрузки всех ресурсов сети за счет рационального выбора пути прохождения трафика через сеть. Механизм управления трафиком предоставляет возможность устанавливать явный путь, по которому будут передаваться потоки данных.

Привлекательность применения технологии MPLS при решении задач Traffic Engineering очевидна:

- явные пути коммутации на основе меток могут быть легко заданы сетевым администратором или с помощью стандартных протоколов.
- эффективно поддерживаются пути коммутации по меткам.
- каналы передачи данных могут быть смоделированы и поставлены в соответствие LSP.
- реализация MPLS дает сравнительно более низкую избыточность по сравнению с другими технологиями управления трафиком.

Раздельная статистика по каждому маршруту может быть использована для анализа загрузки каналов связи, поиска узких мест сети и планирования ее дальнейшего расширения.

Для осуществления Traffic Engineering в MPLS необходимы следующие компоненты:

Пользовательский интерфейс – для того, чтобы оператор мог задавать характеристики TE-туннелей, называемые в MPLS ограничениями

Модифицированный IGP-компонент – усовершенствованные протоколы маршрутизации, переносящие информацию о текущем состоянии сетевых ресурсов

Модифицированный алгоритм маршрутизации, позволяющий рассчитывать маршрут по ограничениям с пользовательского интерфейса и с учётом информации, полученной от IGP-компонента

Компонент сигнализации – протокол, который может устанавливать LSP в обход традиционной маршрутизации и осуществлять резервирование сетевых ресурсов на LSP

Компонент передачи данных – базовая технология MPLS.

При решении задач управления трафиком необходимо решить три основные проблемы:

- первая проблема заключается в определении соответствия пакетов определенному классу FEC.
- вторая заключается в определении соответствия FEC и каналов передачи данных.
- третья проблема состоит в определении соответствия каналов передачи данных физической топологии сети и маршрутов с коммутацией по меткам.

Маршруты, вычисляемые на основе алгоритмов управления трафиком, называются TE-туннелями. Эти туннели контролируются верхними маршрутизаторами. С целью избежания образования петель маршрутизаторы должны согласовывать использование TE-туннелей.

Протокол RSVP-TE используется в качестве протокола сигнализации TE-туннеля. Применение RSVP-TE позволяет оптимизировать сеть под конкретные задачи путем создания туннелей RSVP-TE.

Для создания явно заданного LSP-пути, в протокол RSVP введены дополнительные возможности: функция явной маршрутизации и метод привязки меток к RSVP-потокам.

TE-туннели получили широкое распространение, т.к. могут совмещать преимущества LSP-туннелей, средств поддержания QoS и управления полосой пропускания, что важно при предоставлении широкополосных услуг связи.

Рассмотренные выше механизмы, используемые технологией MPLS, делают эту технологию весьма многообещающей. Уже сегодня крупнейшие компании предлагают готовые MPLS-решения, способные не только повысить качество работы сетей, но и значительно расширить возможности их применения. Технологию быстрой коммутации на основе меток поддерживают устройства Cisco, Juniper, Nortel, Lucent и ряда других крупных производителей оборудования. Расширяется и область применения MPLS. Кроме изначальной цели – повышения качества магистральных сетей операторов, MPLS начинает распространяться на сети доступа.

3. Подходы к предоставлению широкополосных услуг на базе технологии MPLS

В рамках технологии MPLS, рассмотренной во второй главе, существует два подхода к предоставлению широкополосных услуг: VPN-MPLS и VPLS. Эти подходы сегодня пользуются все большей популярностью среди операторов, т.к. базируются на технологии MPLS, которая во многих странах уже стала ведущей магистральной технологией в силу ряда своих достоинств, и позволяют предоставлять весь спектр широкополосных услуг, описанных в первой главе.

3.1. MPLS-VPN

3.1.1. Основы VPN

Виртуальная сеть – это выделенная сеть на базе общедоступной сети, поддерживающая конфиденциальность передаваемой информации за счет использования туннелирования и других процедур защиты.

В основе технологии VPN лежит идея обеспечения доступа удаленных пользователей к корпоративным сетям, содержащим конфиденциальную информацию, через сети общего пользования. В качестве среды для создания VPN могут выступать сети Frame Relay, ATM, но наиболее популярны технологии VPN, рассчитанные на создание сетей VPN в среде Интернет.

Без сомнения, использование каналов Интернет для организации VPN позволяет выгодно решить проблему организации сети. Правда по причине ее общедоступности возникает проблема безопасности, ведь к ресурсам Интернет может получить доступ любой человек.

Виртуальные частные сети могут гарантировать, что направляемый через Интернет трафик так же защищен, как и при передаче внутри локальной сети, при сохранении всех экономических преимуществ, которые можно получить, используя Интернет.

Безопасность данных технологией VPN обеспечивается за счет применения специальных устройств и механизмов защиты. Для получения

доступа к сети пользователь VPN проходит через брандмауэр, где осуществляется его аутентификация и авторизация, благодаря чему VPN гарантирует, что доступ к ресурсам сети получат лишь авторизированные пользователи.

Кроме того, для передачи VPN-трафика в сети общего пользования применяются механизмы туннелирования и шифрования. Это позволяет сделать частную информацию невидимой для других пользователей Web и обеспечивает дополнительную защиту при передаче.

По своей сути VPN обладает многими свойствами выделенной линии, однако, как уже говорилось, реализуется она в пределах общедоступной среды Интернет.

Проводя сравнение между частными и виртуальными частными сетями, следует выделить ряд несомненных преимуществ VPN:

- технология VPN позволяет значительно снизить расходы по поддержанию работоспособности сети: пользователь платит только абонентскую плату за аренду канала. Кстати, аренда каналов также не вызывает каких-либо затруднений вследствие широкомасштабности сети Интернет.
- удобство и легкость при организации и перестроении структуры сети;

Разработка единой модели обслуживания виртуальной частной сети могла бы упростить сетевые операции, но такой подход не может удовлетворить различным требованиям клиентов, так как они уникальны. Каждый клиент предъявляет свои требования к безопасности, числу сайтов, сложности маршрутизации, критичным приложениям, моделям и объемам трафика. Для удовлетворения широкого спектра требований, поставщики услуг должны предлагать клиентам разные модели доставки услуг.

Все сети VPN условно можно разделить на три основных вида.

- Внутрикорпоративные VPN (Intranet VPN).
- Межкорпоративные VPN (Extranet VPN).

- VPN с удаленным доступом (Remote Access VPN).

Интрасеть

Представляет собой наиболее простой вариант VPN, он позволяет объединить в единую защищенную сеть несколько распределенных филиалов одной организации, взаимодействующих по открытым каналам связи.

Экстрасеть

Вариант построения VPN «Экстрасеть» предназначен для обеспечения доступа из сети одной компании к ресурсам сети другой, уровень доверия к которой намного ниже, чем к своим сотрудникам. Поэтому, когда несколько компаний принимают решение работать вместе и открывают друг для друга свои сети, они должны позаботиться о том, чтобы их новые партнеры имели доступ только к определенной информации. При этом конфиденциальная информация должна быть надежно защищена от несанкционированного использования. Именно поэтому в межкорпоративных сетях большое значение должно придаваться контролю доступа посредством брандмауэров (Firewalling). Важна и аутентификация пользователей, призванная гарантировать, что доступ к информации получают только те, кому он действительно разрешен.

VPN с *удаленным доступом*

Принцип работы VPN с удаленным доступом прост: пользователи устанавливают соединения с местной точкой доступа к глобальной сети (POP), после чего их вызовы туннелируются через Интернет, что позволяет избежать платы за междугородную и международную связь или выставления счетов владельцам бесплатных междугородных номеров (Toll-free Numbers). Затем все вызовы концентрируются на соответствующих узлах и передаются в корпоративные сети. Однако из-за использования Интернета в качестве объединяющей магистрали, механизмы защиты информации становятся жизненно важными элементами данной технологии.

Как правило, удаленный пользователь не имеет статического адреса и подключается к защищаемому ресурсу не через выделенное устройство VPN, а с помощью специального программного обеспечения, устанавливаемого на его компьютере.

Важную роль при построении VPN играют отношения предприятия с провайдером, в частности, распределение между ними функций по конфигурированию и эксплуатации VPN-устройств.

При создании защищенных каналов VPN-средства могут располагаться как в среде оборудования провайдера, так и в оборудовании предприятия. В зависимости от этого, выделяют два варианты построения VPN: пользовательская схема (Customer Provided VPN) и провайдерская схема (Provider Provisioned VPN).

Кроме вышеперечисленной классификации, все варианты создания VPN можно разделить на две категории: программные и аппаратные.

Программные решения представляют собой готовые приложения, которые устанавливаются на подключенном к сети компьютере со стандартным программным обеспечением.

Аппаратные VPN-решения включают в себя компьютер, операционную систему, специальное программное обеспечение.

Виртуальные частные сети можно считать полноценным видом транспорта для передачи трафика, только если есть гарантии на пропускную способность и другие параметры производительности, а также безопасность передаваемых данных.

3.1.2. Функции VPN по защите данных

Подключение любой корпоративной сети к публичной вызывает два типа угроз:

- несанкционированный доступ к ресурсам локальной сети, полученный в результате входа в эту сеть.
- несанкционированный доступ к данным при передаче трафика по публичной сети.

Функции VPN должны обеспечивать защиту от таких угроз путем.

Информационный поток по общественной сети передается по защищенному каналу. Для создания защищенного канала средства VPN используют процедуры шифрования, аутентификации и авторизации.

Шифрование

Методов шифрования довольно много, поэтому важно, чтобы на концах туннеля использовался один и тот же алгоритм шифрования. Кроме того, для успешного дешифрования данных источнику и получателю данных необходимо обменяться ключами шифрования. Следует отметить, что шифрование сообщений необходимо не всегда. Часто оно оказывается довольно дорогостоящей процедурой, требующей дополнительных приставок для маршрутизаторов, без которых они не могут одновременно с шифрованием обеспечивать приемлемый уровень быстродействия.

Аутентификация

Под аутентификацией понимается определение пользователя или конечного устройства. Аутентификация позволяет устанавливать соединения только между легальными пользователями и, соответственно, предотвращает доступ к ресурсам сети несанкционированных пользователей.

В процедуре участвуют две стороны: одна доказывает свою аутентичность, а другая ее проверяет и принимает решение.

Чаще всего для аутентификации используется пароль, но могут применяться и другие доказательства. Недостатками применения паролей являются их раскрытие, что частично компенсируется их простотой.

Аутентификация данных свидетельствует об их целостности, а также о том, что они поступили от конкретного пользователя (при этом используется электронная подпись).

Авторизация

Авторизация подразумевает разграничение предоставляемых абонентам видов услуг. Каждому пользователю предоставляются определенные администратором права доступа.

Эта процедура выполняется после процедуры аутентификации и позволяет контролировать доступ санкционированных пользователей к ресурсам сети.

Вообще, процедуры аутентификации и авторизации выполняют одну задачу и к ним предъявляются одинаковые требования.

Целостность передаваемых данных позволяет обеспечить применение электронной подписи.

3.1.3. Механизм VPN

На организацию виртуальных сетей оказывают влияние различные факторы, одним из них является выбор технологии построения VPN.

Среди технологий построения VPN можно назвать такие технологии как: IPSec VPN, MPLS VPN, VPN на основе технологий туннелирования PPTP, L2TP. Во всех перечисленных случаях трафик посылается в сеть провайдера по протоколу IP, что позволяет провайдеру оказывать не только услуги VPN, но и различные дополнительные сервисы (контроль за работой клиентской сети, хостинг Web и почтовых служб, хостинг специализированных приложений клиентов). Технология MPLS в настоящее время является одной из наиболее перспективных технологий создания VPN. Поэтому будем рассматривать построение VPN на базе MPLS.

Рассмотренное в предыдущей главе понятие LSP-туннелей составляет важный аспект MPLS VPN, т.к. прилагательное «частный» в VPN на базе MPLS относится к физическому разделению трафика между LSP-туннелями. В настоящее время в области сетей MPLS VPN существуют два главных направления: *BGP/MPLS VPN* и *VPN с виртуальными маршрутизаторами на базе IP*. Оба эти направления соответствуют общей модели MPLS VPN, представленной на рисунке 3.1.

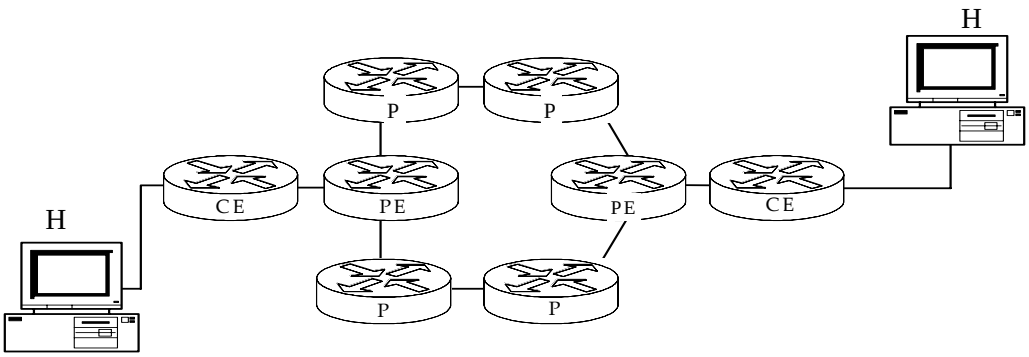


Рис.3.1. Эталонная модель MPLS VPN

Ядро сети на рисунке 3.1 строится на базовых маршрутизаторах MPLS, называемых *внутренними маршрутизаторами провайдера P* и взаимодействует с пользователем VPN не напрямую, а посредством соединения между *граничным устройством маршрутизации заказчика CE (Customer Edge router)* и *граничным устройством маршрутизации провайдера PE (Provider Edge router).* CE могут быть статически подсоединены к PE провайдера через закрепленные каналы или могут использовать коммутируемые линии связи.

Оба метода MPLS VPN сходны в создаваемой провайдером услуги VPN функциональности. В одном методе протокол BGP используется для создания специальных расширенных адресов при передаче пакетов через ядро MPLS, а в другом VR хранят отдельные таблицы путей MPLS для каждой VPN. Фактическая же реализация этих двух методов совершенно различна, а выбор метода - решение провайдера услуг VPN на основе возможностей оборудования, ситуации с взаимодействием сетей и других факторов. Создана новая рабочая группа IETF, названная *Provider-Provisioned VPNs (PPVPNs),* которая разрабатывает структуру и соответствующие спецификации для этих двух типов сетей VPN.

Сети MPLS/BGP-VPN.

Модель MPLS/BGP VPN базируется на расширениях протокола маршрутизации внешнего шлюза BGP, называемых многопротокольными расширениями BGP и касающихся специальных расширенных адресов. Эти адреса используются для обмена информацией о доступности между маршрутизаторами PE только между членами одной и той же VPN. Каждый маршрутизатор PE в MPLS/BGP VPN поддерживает отдельную *таблицу маршрутизации VRF (VPN Routing and Forwarding table)*. Такая таблица поддерживается для каждого сайта, подключенного к PE маршрутизатору. Если IP-адрес пакета указывает на то, что его надо передать в сайт A, его ищут в таблице (forwarding table) сайта A только в том случае, когда пакет прибывает из сайта, ассоциированного с таблицей сайта A. Если сайт связан с несколькими сетями VPN, его таблица VRF может включать данные о маршрутах всех этих сетей. К примеру, сайт CE1 принадлежит сети VPNA и VPNB. В этом случае таблица VRF устройства PE1, к которому подсоединён CE1, будет содержать информацию о маршрутах сети VPNA и VPNB. Другими словами на устройстве PE1 не будет двух отдельных таблиц VRF. Таблицы VRF на устройствах PE используются только для пакетов, поступающих из сайта, напрямую подключенного к данному устройству PE. Они не используются для маршрутизации пакетов, поступающих с других маршрутизаторов, установленных в магистрали сервис-провайдера. В результате к одному и тому же адресу в сети могут вести несколько маршрутов, потому что маршрут для передачи каждого пакета определяется в точке, через которую пакет попадает в магистраль. Данная модель позволяет использовать перекрытие пространств частных IP-адресаций разных предприятий. Основная цель этого типа реализации MPLS VPN – позволить провайдеру обеспечить создать требуемую заказчику конфигурацию VPN. Заказчиком в данном случае может быть предприятие, группа предприятий, которым нужна «Экстранет», другой сервис-провайдер или даже другой провайдер VPN, который может использовать это MPLS-приложение с целью построить сеть VPN своим собственным клиентам.

Существует и другая модель организации MPLS VPN на 3 уровне. Она базируется на принципе образования виртуальных маршрутизаторов. Эта модель не будет рассматриваться из-за малой распространённости. Сегодня если речь идёт о MPLS VPN L3, то понимается MPLS/BGP-VPN.

Организация MPLS VPN.

В общем случае у клиента может быть несколько территориально обособленных IP-сетей, каждая из которых, в свою очередь, может включать несколько подсетей, связанных маршрутизаторами. Такие территориально изолированные сетевые элементы корпоративной сети принято называть *сайтами*. Принадлежащие одному клиенту сайты обмениваются IP пакетами через сеть провайдера и образуют виртуальную частную сеть этого клиента. Как было указано при обсуждении рисунка 3.1, каждый сайт имеет один или несколько граничных пользовательских маршрутизаторов CE, соединённых с одним или более граничными провайдеровскими маршрутизаторами PE посредством каналов PPP, ATM, Ethernet, Frame Relay и т.п.

CE-маршрутизаторы различных сайтов не обмениваются маршрутной информацией непосредственно и даже могут не знать друг о друге. Адресные пространства подсетей, входящих в состав VPN могут перекрываться, т.е. уникальность адресов должна соблюдаться только в пределах конкретной подсети. Этого удается добиться преобразованием IP-адреса в VPN-IP-адрес и использованием протокола MP-BGP для работы с этими адресами.

Каждый PE-маршрутизатор должен поддерживать столько таблиц маршрутизации, сколько сайтов пользователей к нему подсоединено, то есть на одном физическом маршрутизаторе организуется несколько виртуальных. Причём маршрутная информация, касающаяся конкретной VPN, содержится только в PE-маршрутизаторах, к которым подсоединены сайты данной VPN. Таким образом, решается проблема масштабирования, неизбежно возникающая в случае наличия этой информации во всех маршрутизаторах сети оператора. Считается, что CE-маршрутизатор относится к одному сайту, но сам сайт может принадлежать к нескольким VPN. К PE-маршрутизатору

может быть подключено несколько CE-маршрутизаторов, находящихся в разных сайтах и даже относящихся к разным VPN.

3.1.4. Реализация VPN-MPLS

На рисунке 3.2 представлен фрагмент сети VPN MPLS. Данная сеть объединяет несколько удаленных пользователей и сайтов клиентов через сеть провайдера MPLS. Объединенные сайты и удаленные пользователи одной компании образуют виртуальную частную сеть данного предприятия. Таким образом, на рисунке представлены две VPN: предприятия A, включающая три сайта и удаленных пользователей и предприятия B, включающая два территориально распределенных филиала.

В VPN MPLS имеют место два основных потока трафика:

- поток управления, используемый для распространения маршрута VPN и установления пути коммутации меток LSP.
- поток данных, который используется для продвижения информационного потока.

В свою очередь поток управления состоит из двух субпотоков:

- Первый отвечает за обмен маршрутной информацией между PE и CE на границах магистрали поставщика услуг и между маршрутизаторами PE через магистраль провайдера.
- Второй субпоток отвечает за установление пути LSP между маршрутизаторами PE через магистраль поставщика услуг.

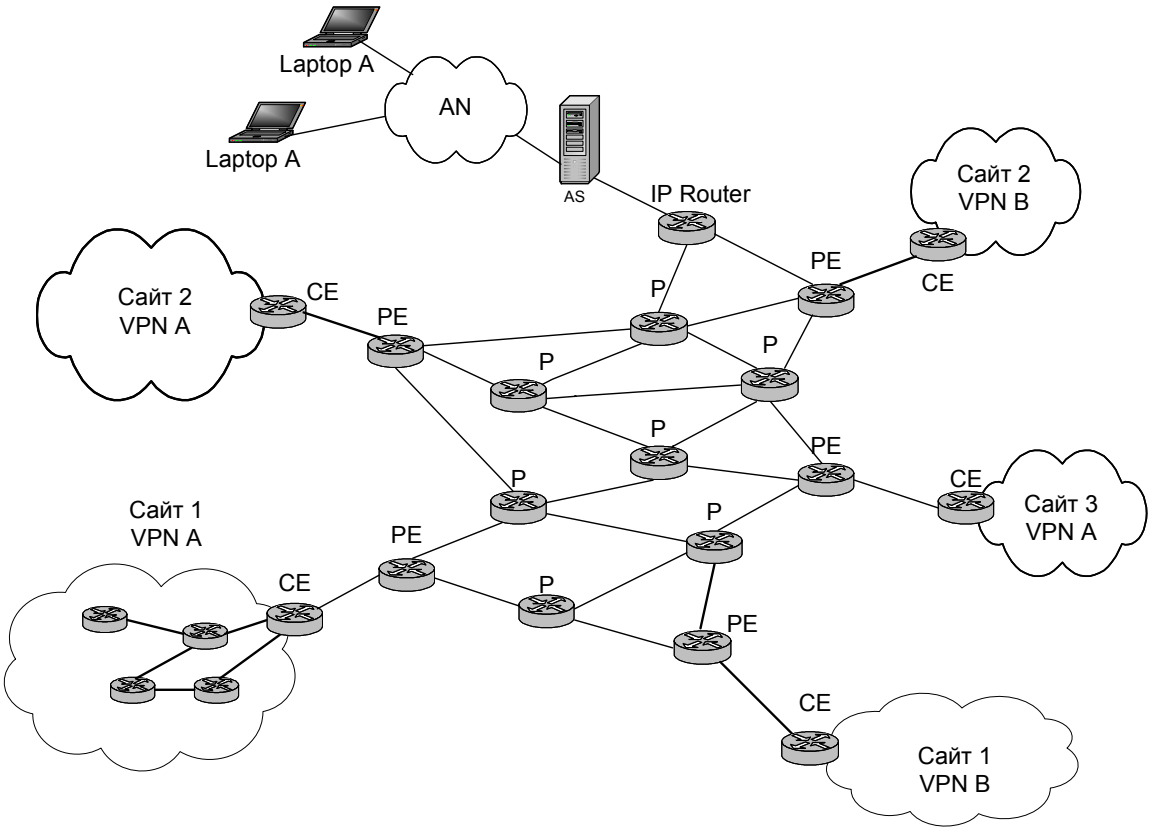


Рис 3.2. Виртуальная частная сеть на базе технологии MPLS.

3.1.4.1. Обмен маршрутной информацией

Механизмом, с помощью которого сайты одной VPN обмениваются маршрутной информацией, служит многопротокольное расширение протокола BGP – MultiProtocol Border Gateway Protocol. С помощью этого протокола пограничные маршрутизаторы PE организуют взаимные сеансы и в рамках этих сеансов обмениваются маршрутной информацией из своих таблиц маршрутизации VRF. Особенность протокола BGP и его расширений заключается в том, что он получает и передает свои маршрутные объявления не всем непосредственно связанным с ним маршрутизаторам, как протоколы IGP, а только тем, которые указаны в конфигурационных параметрах в качестве соседей.

Независимость адресных пространств VPN обеспечивается за счет применения разделителя маршрутов RD, при помощи которого IPv4 адреса преобразуются в VPN-IPv4 адреса. PE-маршрутизатор должен уметь соотносить маршруты, ведущие к конкретным маршрутизаторам CE с

определенным разделителем RD. Маршрутизатор PE может быть сконфигурирован таким образом, чтобы соотносить все маршруты, ведущие к одному CE с одним RD или соотносить разные маршруты с разными RD, ведущими к одному CE. Таким образом, применение RD позволило решить задачу установления различных маршрутов к устройствам, имеющим один и тот же IP-адрес, но принадлежащих разным VPN. Вопрос о том, кому отправлять маршрутные объявления, а кому нет, зависит от топологии виртуальной сети. Таким образом, кроме маршрутов, поступающих от непосредственно подсоединенных к PE сайтов, каждая таблица VRF дополняется маршрутами, получаемыми от других сайтов данной VPN по протоколу MP-BGP. Перед тем, как распространять маршрутные объявления, полученные от сайта, PE должен присвоить маршрутам атрибуты Site of Origin, VPN of Origin, Target VPN.

Атрибут *Site of Origin* (атрибут *сайт-источник*) уникальным образом идентифицирует сайт, от которого PE-маршрутизатор получил информацию о данном маршруте. Все маршруты, полученные от конкретного сайта должны быть ассоциированы с конкретным значением этого атрибута, даже если сайт имеет несколько соединений с одним PE или соединён с несколькими PE. Для разных сайтов должны использоваться разные атрибуты Site of Origin.

Маршрут VPN-IPv4 может быть опционально ассоциирован с атрибутом *VPN-источника (VPN of Origin)*. Этот атрибут однозначно идентифицирует группу сайтов и соответствующий маршрут, объявленный одним из маршрутизаторов, находящихся в этих сайтах. В качестве одного из применений данного атрибута может быть идентификация предприятия, владеющего сайтом, к которому ведёт маршрут или сети Intranet, к которой он принадлежит.

Каждой ассоциированной таблице маршрутизации в PE-маршрутизаторах присваивается один или несколько *атрибутов целевой VPN (Target VPN)*. Когда PE-маршрутизатором создаётся маршрут VPN-IPv4,

он ассоциируется с одним или более атрибутами Target VPN. Они переносятся протоколом BGP как атрибуты маршрута. Каждый маршрут, ассоциированный с Target VPN «T», должен быть объявлен всем PE-маршрутизаторам, имеющим таблицу маршрутизации, ассоциированную с Target VPN «T». Когда такой маршрут принимается PE-маршрутизатором, он имеет право быть включенным в любую из ассоциированных таблиц маршрутизации, имеющих атрибут Target VPN «T».

Для обмена маршрутной информацией между CE и PE существует несколько способов (статическая маршрутизация, протоколы IGP, EBGP). Возможность применения той или иной технологии обмена маршрутной информацией между PE и CE зависит от того, принадлежит ли CE к «транзитной VPN» или нет.

Сайты виртуальной сети могут принадлежать как одной, так и находится в разных автономных зонах. В первом случае обмен маршрутной информацией производится по протоколу IBGP. Если же сайты находятся в разных AS, то по протоколу IBGP реализуется обмен информацией до граничного маршрутизатора ASBR, а затем этот маршрутизатор должен будет передавать маршрутные объявления ASBR, находящемуся в другой автономной зоне по протоколу EBGP.

3.1.4.2. Установление LSP-туннеля

Для передачи трафика по сети MPLS следует установить LSP-тракт между маршрутизаторами PE.

Пути LSP могут быть проложены через сеть поставщика услуг двумя способами: либо с применением технологии ускоренной маршрутизации (IGP) с помощью протоколов LDP, либо на основе технологии Traffic Engineering с помощью протоколов RSVP-TE или CR-LDP.

При этом, если путь прокладывается при помощи протокола LDP, то обслуживаться он будет согласно модели Best Effort. Если же поставщик услуг хочет выделить полосу пропускания для пути LSP или использовать регулирование трафика для установления явного пути LSP, используется

протокол RSVP, позволяющий поддерживать заданное качество обслуживания и регулирование трафика.

Стоит отметить, что для взаимной совместимости оборудования различных производителей от всех маршрутов PE требуется поддержка протокола LDP. При этом для поддержки связей между маршрутизаторами PE создаются туннели, обслуживаемые в соответствии с моделью Best Effort.

При выборе провайдером протокола резервирования ресурсов, образованные на основе данного протокола туннели будут иметь больший приоритет, чем туннели LDP. Между парой маршрутизаторов присутствуют как те, так и другие.

Прокладка LSP означает создание таблиц коммутации меток на всех маршрутизаторах PE и P, образующих данный LSP.

На каждый подключенный сайт PE-маршрутизатор поддерживает по одной таблице маршрутизации. Эти таблицы используются маршрутизаторами только при получении пакетов от присоединенных к данным PE сайтам.

После того, как маршрутизатор CE назначит маршрут, связанный с ним маршрутизатор магистральной сети провайдера прописывает локальный путь в своей базе LIB, а затем выбирает из своей базы метку для объявления ее вместе с маршрутом.

В одной системе может существовать несколько путей, которые зависят от передающего информационный трафик сайта.

3.1.4.3. Поток данных

Передачу трафика пользователя от одного сайта на другой сайт виртуальной частной сети можно разделить на четыре этапа:

- передача потока от CE-маршрутизатора источника до входного пограничного маршрутизатора сети провайдера.
- передача информационного потока от PE до P
- передача трафика по транзитной области MPLS.

- передача потока от выходного маршрутизатора PE до маршрутизатора назначения CE.

Первый этап

Пакет данных, предназначенный для другого сайта, поступает на пограничный маршрутизатор клиента CE. Маршрутизатор CE принимает исходящий пакет данных на своем сайте, определяет маршрут следования пакета и передает его к связанному с ним PE-маршрутизатору.

Второй этап

При поступлении пакета от маршрутизатора CE, маршрутизатор PE производит поиск маршрута в таблице VRF. Если пакет предназначается узлу CE, подсоединенному непосредственно к рассматриваемому PE, он немедленно отсылается этому маршрутизатору. В противоположном случае, маршрутизатор PE обращается к своим таблицам VRF и LIB, формирует стек меток и отправляет пакет на следующий маршрутизатор. После передачи информационного трафика по сети MPLS, PE-получатель удаляет метки и отсылает пакет CE-маршрутизатору, который определяет дальнейший путь пакета на основе анализа его IP-заголовка.

Третий этап

Маршрутизаторы магистральной сети не имеют сведений о маршрутах к сайтам VPN. Пересылка пакетов осуществляется посредством технологии MPLS: внутренние маршрутизаторы магистральной сети провайдера коммутируют пакет с меткой, меняя верхнюю метку стека на каждом участке пока не достигнет предпоследнего маршрутизатора PE перед тем, к которому отправлен пакет. Этот маршрутизатор извлекает верхнюю метку из стека и отправляет пакет к PE пограничному маршрутизатору назначения магистральной сети провайдера.

Четвертый этап

Маршрутизатор PE, присоединенный к определенной виртуальной сети должен уметь определять как распределены адреса данной сети по ее сайтам.

При получении пакета маршрутизатор PE на основе анализа нижней метки стека определяет маршрутизатор CE назначения и направляет к нему пакет.

3.2. Технология VPLS

VPLS – новая технология и одновременно – услуга, которая может предоставляться большому количеству корпоративных заказчиков и обеспечивать значительные прибыли операторам. Как уже упоминалось в главе 1, услуга заключается в объединении двух и более удаленных офисов клиента в единую высокоскоростную и защищенную сеть обмена информацией.

3.2.1. Основы VPLS

Основу концепции VPLS составляет идея передачи пакетов Ethernet из сети заказчика (включая информацию о внутренних VLAN) по операторской сети «прозрачным» образом абсолютно без изменений. Для этого пакеты инкапсулируются по технологии MPLS, обеспечивающей создание туннелей в сети оператора связи, которые независимы от пользовательского трафика. Для реализации этой задачи сеть оператора должна быть высоконадежной, поддерживать новейшие механизмы отказоустойчивости, такие как механизм связующего дерева (Rapid Spanning Tree), обеспечивающие наивысшие гарантии доставки пакетов по назначению, также механизмы поддержки качества услуг. Заказчикам не требуется подключаться к IP-сети оператора и настраивать сложные протоколы IP-маршрутизации, они используют простые соединения Ethernet, которые позволяют работать с гораздо большим числом различных сетевых архитектур и топологий.

VPLS особенно эффективна в условиях динамично развивающегося рынка, где прибыль является важнейшей задачей. Вместо установки дорогостоящих маршрутизаторов и оборудования для IP-туннелирования для построения сети доступа и операторской сети могут быть использованы обычные коммутаторы Ethernet, что обеспечивает предоставление высокоскоростных сервисов при меньших затратах. Операторы могут

использовать возможности классификации трафика для предоставления услуг, требующих высокого приоритета, например передача голоса по IP.

VPLS использует стандарты IEEE 802.1q и MPLS Martini для инкапсуляции пакетов и их транспорта, также сигнализация VPLS описана ещё в ряде документов IETF.

На входе в сеть оператора, обычно в помещении заказчика, коммутатор Ethernet инкапсулирует пакеты локальной сети в пакеты с тегами 802.1q VLAN, даже если заказчик уже использует VLAN. Этот процесс, называемый VMAN, добавляет к пакету дополнительный тег VLAN, что позволяет идентифицировать принадлежность данного пакета конкретному заказчику. Исходный тег, описывающий принадлежность пакета к одной из внутренних VLAN в сети заказчика, остается на месте и восстанавливается на выходе из операторской сети. Внутри операторской сети работа VPLS может осуществляться двумя основными способами. Если абонентов немного (менее 4 тыс.), тэги VMAN могут без изменений использоваться для организации соединений. При большем количестве абонентов (тысячах и десятках тысяч) сеть необходимо сконфигурировать для применения инкапсуляции MPLS, которая помещает в пакеты метки, позволяющие определить их происхождение и способы пересылки внутри сети оператора. Независимо от архитектуры сети оператора на выходе из сети пакет заказчика восстанавливается в своем исходном виде, включая возможное наличие тэга VLAN. Это дает заказчику возможность быть полностью независимым от конфигурации сети оператора, что является важнейшей функцией любой услуги по созданию виртуальных частных сетей.

При использовании VPLS допускаются соединения типа «точка-точка» и многоточечные конфигурации. В последнем случае оборудование изучает расположение различных устройств в сети и построение соответствующих таблиц для правильной пересылки пакетов между подключенными точками. С этой целью операторская сеть должна обеспечивать предоставление гарантированной полосы пропускания и защиту от перегрузок и заторов

трафика. Для решения этой проблемы существуют механизм классификации трафика Ethernet. При его применении оператор может управлять выделяемой полосой пропускания с высоким уровнем контроля над реальной скоростью прохождения пакетов в сети. Кроме того, для обеспечения работы приложений, требующих наивысшего приоритета для их трафика, он может использовать классификацию и дополнительные возможности MPLS.

3.2.2. Механизм VPLS

VPLS предоставляет многоточечные услуги Ethernet. VPLS может соединить большое количество областей и обеспечить соединения между многочисленными сайтами так, словно эти сайты принадлежать одному частному сегменту локальной сети Ethernet. В то время как для осуществления многоточечного Ethernet соединения провайдер использует базирующуюся на коммутаторах Ethernet архитектуру, для построения VPLS используется масштабируемая структура сети IP/MPLS. С точки зрения провайдера, использование маршрутных протоколов и процедур маршрутизации IP/MPLS вместо протокола связующего дерева (Spanning Tree Protocol) и меток MPLS вместо VLAN IDs (идентификаторов VLAN), а также использование различных служб провайдера ведет к значительному улучшению масштабируемости VPLS.

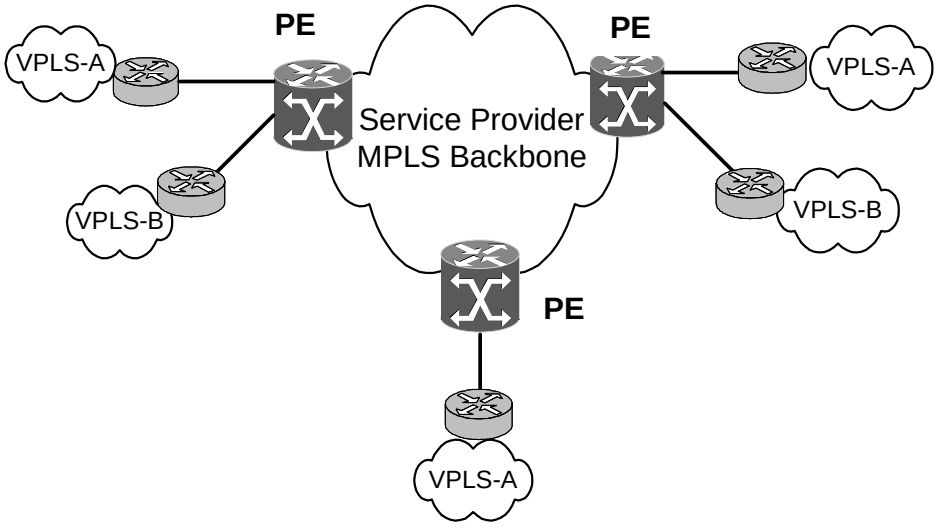


Рис.3.3. Пример сети VPLS

Каждый маршрутизатор провайдера PE (Provider Edge), расположенный на границах IP/MPLS сети, обладает особыми качествами VPLS, определенными стандартами IETF, о которых подробнее будет рассказано позже. Каждому предприятию, желающему использовать прозрачные службы Ethernet, оператор выделяет домен VPLS. Каждый такой домен может рассматриваться как частная сеть Ethernet, которую провайдер реализует в своей сети, а каждый связанный с филиалом маршрутизатор создает «экземпляр VPLS». Каждый VPLS домен состоит из некоторого количества PE, соединяющих экземпляры VPLS, находящиеся в этом определенном VPLS домене, между собой. Упростим ситуацию, допустим, что есть только один VPLS домен для какого-то предприятия и на один экземпляр VPLS приходится один PE, соединяющий принадлежащие этому предприятию сайты. Первым делом в домене VPLS провайдерской сети для всех экземпляров VPLS, необходимо создать полный набор путей коммутации по меткам (LSP). В зависимости от реализации VPLS издержки на LSP при добавлении новых экземпляров VPLS могут оказаться более или менее значительными.

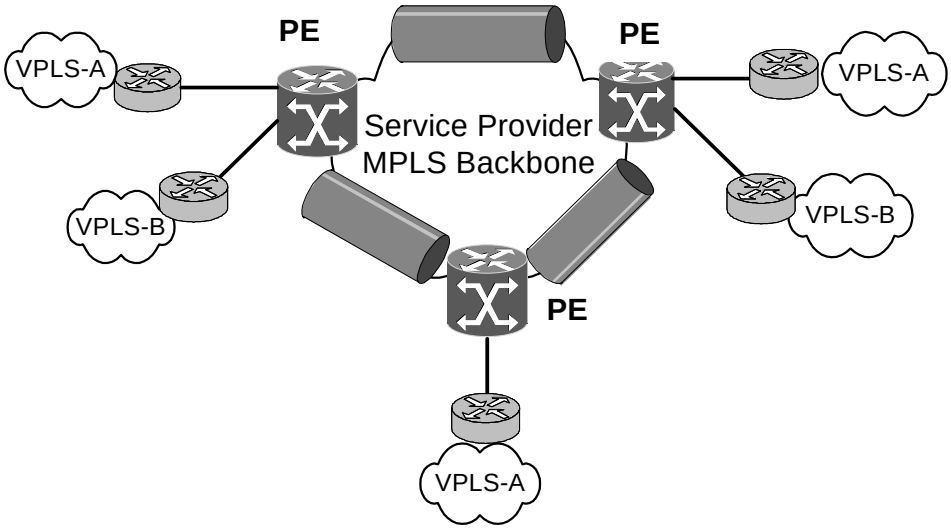


Рис.3.4. Полный набор путей коммутации меток (LSP) между PE.

Для организации необходимого количества внешних туннелей для PE используется расширенный метод обнаружение соседей MPLS, то есть направленные сообщения Hello, передаваемые по UDP. Потом

устанавливается TCP сессия, и далее для создания LSP используются сигнальные сообщения протокола LDP.

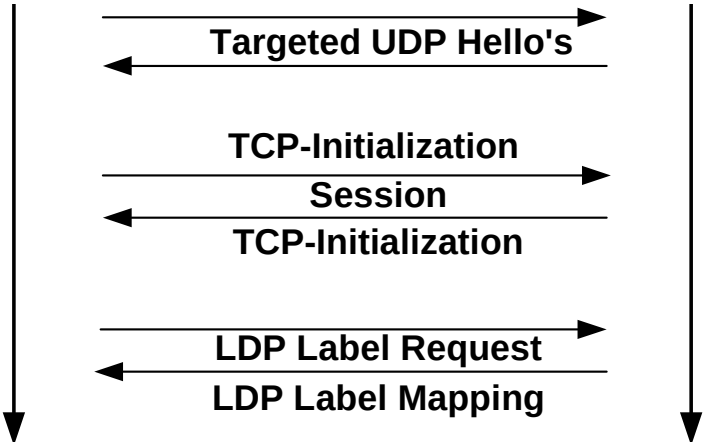


Рис.3.5. Использование протоколов UDP, TCP, LDP для создания LSP.

После того как полный набор LSP туннелей будет организован для всех PE, экземпляр VPLS должен назначить идентификаторы VPLS и, получив сигнал от каждого PE, сообщить ему идентификатор VPLS Virtual Circuit Label или VC Labels. Для установления VPLS или VC-ID туннелей каждый PE инициирует направленную LDP сессию с каждым PE в экземпляре VPLS, чтобы организовать два виртуальных канала (т.к. виртуальные каналы как и туннели однонаправленные, то, соответственно, организуется один виртуальный канал в одном туннеле и второй виртуальный канал в обратном направлении в другом туннеле) – VC или VPLS LSP, внутри внешнего туннеля LSP.

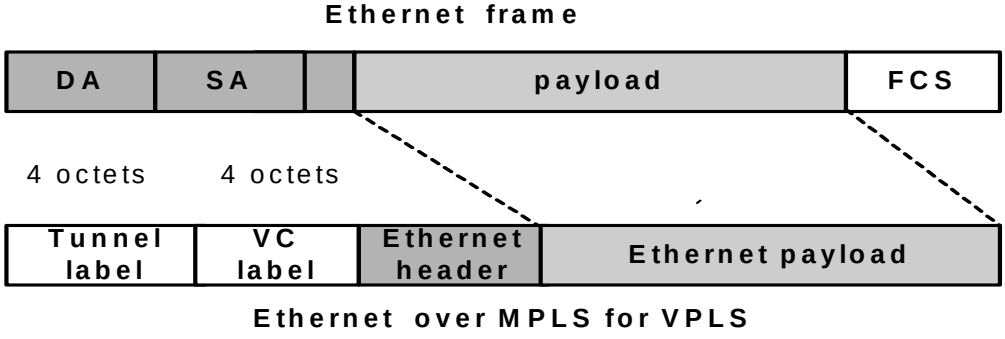


Рис.3.6. MPLS VPLS Label Stacking.

Если построение связной сети LSP завершено, то экземпляры VPLS могут принимать кадры Ethernet от любого филиала и в зависимости от MAC-адреса передавать дальше по соответствующим LSP. Это возможно

благодаря тому, что VPLS позволяет PE маршрутизатору работать в качестве «обученного» моста, т.е. для каждого экземпляра VPLS каждый PE имеет таблицу MAC-адресов. Основными функциями VPLS моста являются: «Обучение» и удаление MAC-адресов, передача неизвестного трафика, дублирование и многоточечная или широковещательная рассылка неизвестных пакетов. «Обучение»VPLS мостов MAC-адресам происходит также, как и «обучение» мостов Ethernet. А именно, MAC-адрес XXX посылается широковещательно, как ARP-запрос. Устройства запоминают этот MAC-адрес и ассоциируют его с конкретным LSP.

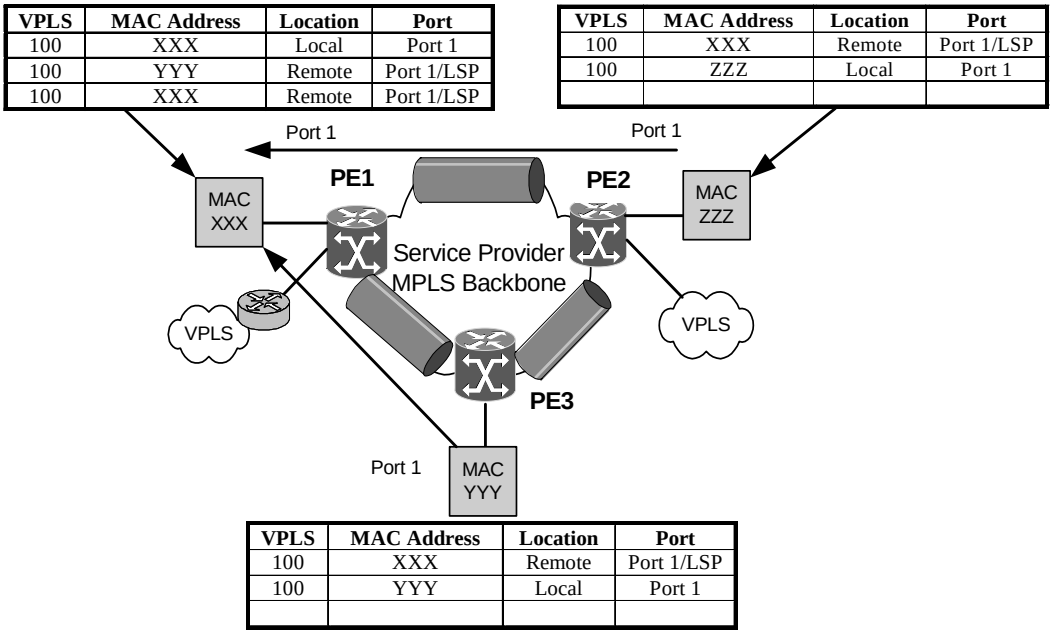


Рис.3.7. «Обучение» MAC-адресам.

PE1 запоминает, что VPLS 100 имеет MAC-адрес XXX, принадлежащий порту 1. Когда PE2 и PE3 широковещательно получают запрос, они фиксируют у себя MAC-адрес XXX и ассоциируют его с LSP, который ведет к PE1. Далее когда с MAC-адреса ZZZ посылается ответ на адрес XXX, PE2 закрепляет за адресом ZZZ у себя порт 1, а PE1 запоминает, что ZZZ принадлежит PE2 удаленно и ассоциирует его с LSP, связывающим PE1 и PE2. Тоже самое происходит, когда посылается ответ с адреса YYY на адрес XXX, т.е. PE3 локально прикрепляет к YYY порт 1, а PE1 - удаленно и ассоциирует этот адрес с LSP, идущим от него к PE3.

Другими словами, у каждого экземпляра VPLS есть PE маршрутизатор, которому предоставляется таблица MAC-адресов, которая заполняется в процессе отслеживания MAC-адресов или процессе «обучения», когда Ethernet кадры поступают на специальный физический или логический порт, т.е. по этой таблице маршрутизатор проверяет и распознает поступающие на порт кадры Ethernet. Таким же образом работают и коммутаторы Ethernet сегодня. После поступления кадра на порт со стороны предприятия маршрутизатор сверяет MAC-адрес места назначения с таблицей и без изменений направляет кадр на LSP или дальше к определенному пограничному маршрутизатору. Если этого MAC-адреса нет в таблице, Ethernet кадр дублируется и рассылается на все логические порты, связанные с этим экземпляром VPLS, за исключением порта доступа, куда этот кадр только что пришел (лавинная маршрутизация). Если пограничный маршрутизатор получает информацию о назначении адреса на особый порт, он обновляет таблицу. Как и в коммутаторе, MAC-адрес, долгое время неиспользуемый, устаревает и в целях сохранения компактности таблицы MAC-адресов удаляется.

3.2.3. Сигнализация в VPLS

Существует два лидирующих предложения, в настоящее время обсуждаемых в IETF, которые претендуют на то, чтобы стать основными подходами построения VPLS. Первый стандарт - это draft-ietf-ppvpn-vpls-ldp (VPLS LDP), который будем называть «стандарт Kompella», предложенный Киреети Компелла. Второй – draft-ietf-ppvpn-vpls-bgp (VPLS BGP), который будем называть «стандарт Lasserre-Kompella», предложенный Марком Лассерром и Вахом Компелла. Рассмотрим оба стандарта и сравним по следующим критериям:

- Эффективность распространения сигнальной информации.
- Эффективность распределением меток.
- Поиск взаимодействующих в рамках VPLS PE устройств.
- Масштабируемость.

- Наличие инструментария администрирования и отладки.
- Возможность организации VPLS на сетях нескольких взаимодействующих операторов.

3.2.3.1. Сигнализации VPLS на основе L2VPN-LDP

Стандарт описывает использование MPLS или IP туннелей для передачи трафика VPLS сервисов. Документ определяют дополнительный набор меток (так называемые метки виртуальных каналов – vc-labels), служащих для разделения, демультиплексирования виртуальных каналов (pseudowires), передаваемых внутри одного туннеля. Отметим (это верно при использовании MPLS как транспортной инфраструктуры), что один или несколько виртуальных каналов могут передаваться по одному MPLS туннелю, несколько путей Label Switch Pass (LSP) могут использоваться для организации одного MPLS туннеля, к примеру, основной и запасной (standby) пути. Для сигнализации vc-labels предлагается использовать расширение протокола LDP. PE маршрутизаторы договариваются об использовании vc-labels меток в рамках данной VPLS для определения соответствия полученного пакета какому-либо VPLS сервису, то есть задается соответствие между виртуальным каналом и VPLS. Также протокол LDP используется для организации LDP сессий (target LDP) между взаимодействующими в рамках организации VPLS устройствами.

Эффективность распространения сигнальной информации

LDP - сигнальный протокол «точка-точка» может использоваться для сигнализации, установления виртуальных каналов между устройствами, взаимодействующими при построении VPLS сети. Если учесть, что для построения некоторой VPLS может быть задействована лишь небольшая часть всех PE маршутизаторов оператора, то намного эффективнее позволить PE устройствам напрямую взаимодействовать друг с другом, чем рассылать сигнальную информацию всем устройствам сети с возможностью дальнейшей фильтрации ими полученных данных. Достигается эффективность распространения сигнальной информации в смысле

минимизации нагрузки на маршрутизаторы, отстутствия «лишнего» трафика в сети за счет увеличения административных накладных.

Эффективность распределением меток

MPLS метки представляют собой довольно ценный ресурс, так как PE маршрутизаторы обычно поддерживают единое пространство меток на устройство (к примеру, это верно для frame-mode интерфейсов согласно RFC 3036). Если учесть, что MPLS метки используются следующими протоколами:

- RSVP-TE для установления Traffic-Engineered (TE) транспортных LSP.
- LDP для установления основанных на информации IGP протоколов маршрутизации транспортных LSP.
- LDP для установления виртуальных каналов передачи данных в Virtual Leased Line сервисах.
- LDP для установления виртуальных каналов передачи данных в VPLS.
- BGP для установления L3 VPN сервисов согласно RFC 2547,

вопрос масштабирования требует динамического выделения/возврата меток в пул по запросам от сигнальных протоколов.

Использование LDP полностью устраняет необходимость административного контроля за распределением меток, используемых для сигнализации VPLS, что крайне немаловажно в больших сетях.

Поиск взаимодействующих в рамках VPLS PE устройств

Стандарт L2VPN-LDP не определяет механизмов автоматического поиска PE устройств (autodiscovery), взаимодействующих в рамках построения какой-либо VPLS сети. В современных реализаций VPLS сервиса необходимо явно указать – к каким PE маршрутизаторам подключены клиентские устройства. В большинстве случаев на практике для этого используется система управления. В последнем случае механизм auto-discovery будет лишним, привнесет дополнительную сложность в протокол сигнализации и затруднит отладку. Отметим, что стандарт не отрицает возможности использования механизмов автоматического поиска

взаимодействующих устройств на основе, к примеру, BGP. На данный момент все производители оборудования, реализующие VPLS на базе LDP, разработали системы управления автоматизирующие поиск, настройку PE устройств для организации L2 сервисов.

Масштабируемость

Архитектура VPLS предполагает «плоскую» или иерархическую топологию. В случае «плоской» топологии необходима организация IP или IP/MPLS туннелей и установление LDP сессий между всеми PE устройствами (target-LDP сессии) для согласования VC меток виртуальных каналов (pseudo-wires). В данном случае вопрос масштабируемости следует рассматривать с позиции числа target-LDP (направленных) сессий, которые могут поддерживать PE устройства. Если число подобных сессий ограничено производительностью маршрутизаторов, то единственным выходом наращивания сети является иерархическая архитектура, ограничивающая число устройств в полносвязном ядре. Как видно на рисунке, полносвязный граф LDP сессий и IP/MPLS туннелей между PE устройствами заменен на ‘hub’ ядро и ‘spoke’ ответвления в сети оператора. Иерархический VPLS использует протокол LDP для установления hub и spoke соединений. Подобный подход за счет единого сигнального протокола и использования IP/MPLS во всей сети предоставляет унифицированный механизм установления соединений, резервирования туннелей, обеспечения качества сервиса и администрирования.

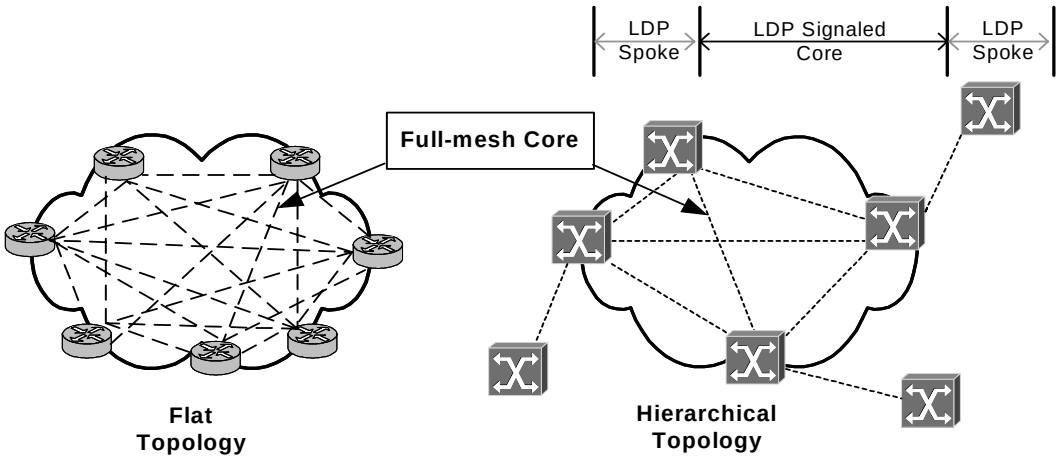


Рис.3.8. Минимизация числа target-LDP сессий при переходе от полносвязной топологии к иерархической.

Иерархическая структура позволяет переложить функциональность spoke маршрутизаторов на более дешевые устройства, поддерживающие MPLS, LDP сигнализацию и pseudo-wire туннели до маршрутизаторов ядра. В конечном счете, использование MPLS в сети доступа позволяет избежать использования протоколов подобных Spanning-Tree.

Организация VPLS сервиса поверх сетей нескольких операторов

Требования к построению VPLS поверх сетей нескольких операторов:

1. Архитектура: Архитектура должна быть эффективна в смысле сигнализации и репликации пакетов, то есть эффективность напрямую зависит от необходимости установления туннелей между всеми PE устройствами через границу сетей операторов. Действительно, если все PE устройства соединены MPLS туннелями, то в случае передачи широковещательного пакета, он будет передан по каналу связи между операторами несколько раз. Использование LDP spoke сигнализации при иерархическом построение VPLS, очень кстати оказывается при построении межоператорского VPLS сервиса. Как показано на рисунке, межоператорская VPLS может быть построена на основе определения нового уровня иерархии между пограничными PE устройствами операторов.

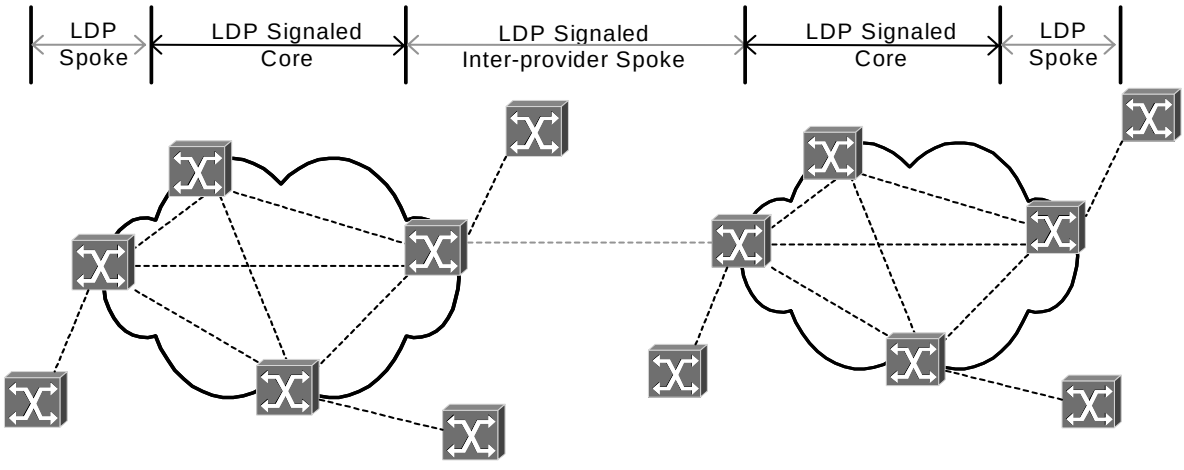


Рис.3.9. Организация межоператорской сети как следствие развития концепции иерархической VPLS.

2. Уникальный глобальный идентификатор: для организации любого междоменного или межоператорского сервиса необходим глобальный уникальный идентификатор. В случае VPLS-LDP используется 32 битный параметр VC-id, его значения должны совпадать в сетях двух операторов для одной и той же VPLS.

3. Избежание маршрутных петель: подход VPLS-LDP устраняет необходимость в Spanning Tree протоколе за счет реализации split-horizon коммутации пакетов на full-mesh соединениях. Например, если пакет получен на одном full-mesh виртуальном канале (виртуальный канал образует hub сети), то PE устройство не пересылает пакет никому другому в ядре, так как считает, что все устройства получили данный пакет благодаря полносвязной схеме туннелей, но в тоже время пересылает пакет в ‘spoke’ ответвление.

4. Безопасность: так же как и в BGP, MD5 аутентификация может использоваться в LDP для аутентификации сессий между PE маршрутизаторами на границе доменов операторов. Использование LDP сигнализации для организации межоператорского VPLS сервиса не требует разработки дополнительных процедур, усложнения настройки, однако необходимо отметить, что способы резервирования соединения между сетями операторов в настоящее время не стандартизованы и большинство производителей оборудования в этой области реализуют собственные подходы.

Инструментарий управления и отладки

Для администрирования VPLS сервиса необходимы средства отладки сигнализации, передачи Ethernet фреймов и заучивания MAC адресов. Стандарт stokes-vkompella определяет механизмы позволяющие проверить:

- Соединение между PE маршрутизаторами.
- Корректность передачи данных и сигнализацию между PE узлами сети.
- Определить, кто анонсировал MAC адрес в VPLS.

Так как LDP сигнализация применяется и в ядре сети, и на границе, то нет необходимости разрабатывать отдельный механизм отладки в случае иерархической VPLS.

3.2.3.2. Сигнализации VPLS на основе L2VPN-BGP

Стандарт L2VPN-BGP описывает механизм автоматического определения PE устройств, взаимодействующих при построении VPLS сервисов, и сигнализации меток виртуальных каналов на основе расширения протокола BGP. Данное расширение, а именно MP-BGP, уже используется при построении L3 VPN (RFC 2547). Рассмотрим, насколько протокол BGP применим для сигнализации VPLS.

Эффективность распространения сигнальной информации

При использовании протокола BGP для распространения сигнальной информации необходима full-mesh связь между всеми PE маршрутизаторами, этого можно избежать при использовании Route Reflectors (RR). В последнем случае каждый маршрутизатор должен поддерживать только одно TCP соединение с RR или несколько, в случае кластера RR для целей обеспечения отказоустойчивости. На первый взгляд проблема масштабирования сети устранена, однако объем информации ранее передаваемой по множеству full-mesh соединений теперь передается по одному, то есть достигнута только эффективность конфигурации, но не объема передаваемых данных.

Рисунок отражает объем реплицируемых данных в случае всего лишь трех VPLS сервисов, в среднем образуемых 3 PE маршрутизаторами.

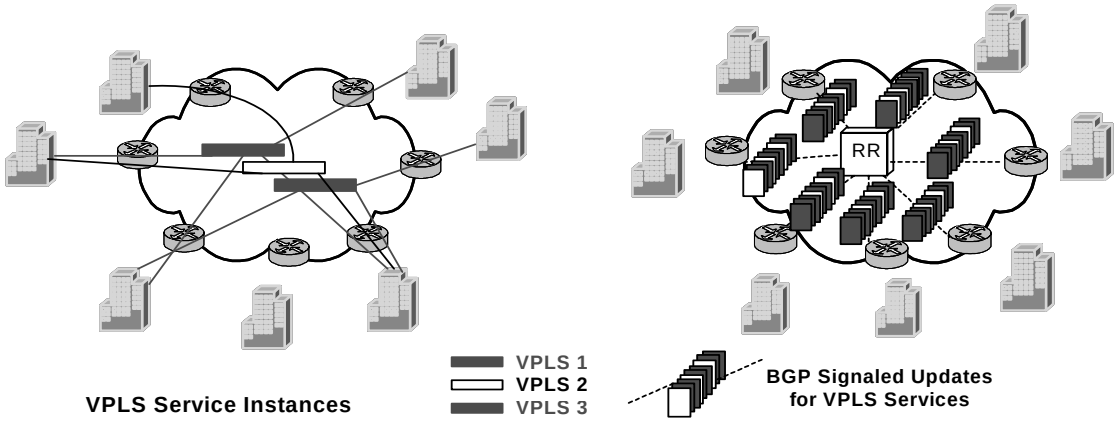


Рис.3.10. Объем дублируемых данных растет как число PE умножить на среднее число VPN на устройство.

В настоящее время BGP используется как протокол маршрутизации сети Интернет, где доказал свою эффективность при распространении сотен тысяч IP маршрутов – определенно неэффективность распространения сигнальной информации не скажется на работоспособности сети, возможно несколько замедлит скорость сходимости BGP, но это в большинстве случаев некритично. Преимуществом является уменьшение ручной настройки.

Эффективность распределением меток, сигнализирующих виртуальные каналы

Принцип работы протокола BGP определяет режим передачи сигнальной информации point-to-multipoint, что означает принципиальную невозможность распределять метки, сигнализирующие виртуальные каналы на основе механизма «запрос-ответ» (в принципе, конечно, можно, но с учетом того, что подобная информация будет рассылаться всем PE устройствам сети это неэффективно). Решением данной проблемы является анонсирование PE маршрутизаторами диапазона меток, что могут использоваться взаимодействующими устройствами при организации виртуальных каналов, составляющих VPLS. Столкновений при выборе меток не происходит, так как все маршрутизаторы знают число устройств, организующих VPLS сервис. Подобный подход априорного задания множества меток виртуальных каналов VPLS и соответственно максимального числа PE устройств, организующих VPLS сервис, приводит к

нерациональному использованию пространства меток, его фрагментации, что негативно сказывается на масштабируемости сети и сложности конфигурации.

Поиск взаимодействующих в рамках VPLS PE устройств

При использовании протокола BGP сигнальная информация распространяется всем PE маршрутизаторам в пределах автономной системы. Для фильтрации, получения только необходимой в рамках организации определенной VPLS информации, применяются routing policies. Применение подобных механизмов на границе автономной системы является обычным делом, но внутри может привести к трудно отлавливаемым ошибкам. Например, число VPLS сервисов в сети может быть несколько сотен, и для каждой должен быть настроен разрешающий фильтр в routing policies. По логике работы протокола BGP база данных RIB-IN может содержать NLRI для всех VPLS, даже тех, в образовании которых маршрутизатор не участвует. Этого можно избежать двумя способами:

- Удалением всех неактуальных NLRI записей, это возможно, если маршрутизаторы поддерживают Route Refresh функциональность.
- Использованием Outbound Route Filtering (ORF), что позволяет PE маршрутизаторам динамически установить, к примеру, на RR фильтр, препятствующий передаче ненужной информации. Однако это приведет к снижению предсказуемости работы сети.

Встроенный механизм обнаружения взаимодействующих PE устройств значительно упрощает жизнь администраторам, однако при росте сети можно негативно сказаться на масштабируемости.

Масштабируемость

VPLS может строиться на основе «плоской» или иерархичекой топологии виртуальных каналов. В случае LDP сигнализации иерархическая топология предлагает большие возможности масштабирования за счет ограничения числа устройств, образующих полносвязную сеть виртуальных каналов. Вариант построения VPLS с использованием BGP сигнализации не

страдает проблемой ограниченного числа target-LDP сессий между PE устройствами. На первый взгляд иерархическая топология здесь кажется лишней, однако нужно учесть, что в случае «плоской» топологии все PE устройства должны быть дорогостоящими маршрутизаторами с полноценным BGP. Драфт L2VPN-BGP определяет иерархическую топологию на основе использования устройств Layer 2 агрегации, то есть организацию уровня доступа на базе L2 коммутаторов, что в итоге негативно сказывается на устойчивости сети за счет использования Spanning-Tree протокола.

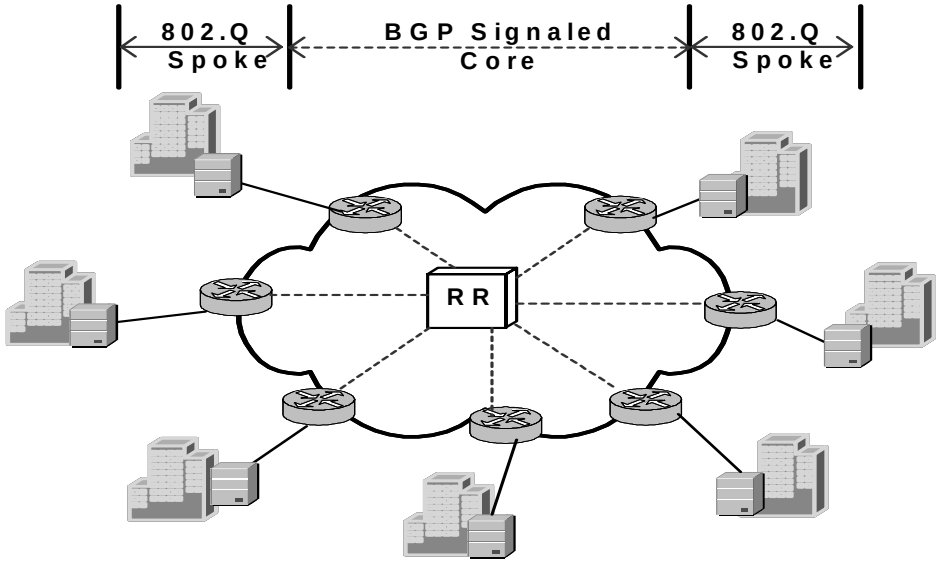


Рис.3.11. Организация иерархической топологии на базе Layer 2 устройств агрегации трафика.

Организации VPLS на сетях нескольких взаимодействующих операторов

Для передачи информации внутри автономной системы (AS) используется iBGP, при организации VPLS сервиса на сетях нескольких операторов возникает вопрос о сигнализации между AS и организации MPLS туннелей между PE маршрутизаторами в разных автономных системах. Стандарт L2VPN-BGP предлагает следующие решения:

a. На границе автономных систем VPLS терминируется в определенный VLAN, то есть для PE маршрутизаторов межоператорский канал связи выглядит обычным абонентским подключением. Для резервирования

подобных подключений требуется применение протокола Spanning Tree, что сказывается на масштабировании.

b. Организация eBGP сессий между PE ASBR маршрутизаторами операторов.
c. eBGP сессия между RR операторов. ASBR маршрутизаторы на границах сетей в данном случае не взаимодействуют по eBGP, а только коммутируют MPLS пакеты, выполняют функциональность P маршрутизаторов. RR передают NLRI информацию о VPLS сервисах с применением опции next-hop-unchanged, что позволяют сигнализировать MPLS туннели между PE маршрутизаторами операторов. Решение аналогично описываемому в стандарте draft-ietf-l3vpn-rfc2547bis раздел 10(c).

В случае резервирования каналов связи между операторами в двух последних случаях не требуется применение Spanning Tree протокола, разрешение колец в топологии происходит за счет работы протокола BGP.

В случаях b) и c) так или иначе устанавливаются туннели между всеми PE устройствами (fullmesh), что означает многократную передачу широковещательных (broadcast, multicast, unknown) данных по каналу связи между операторами.

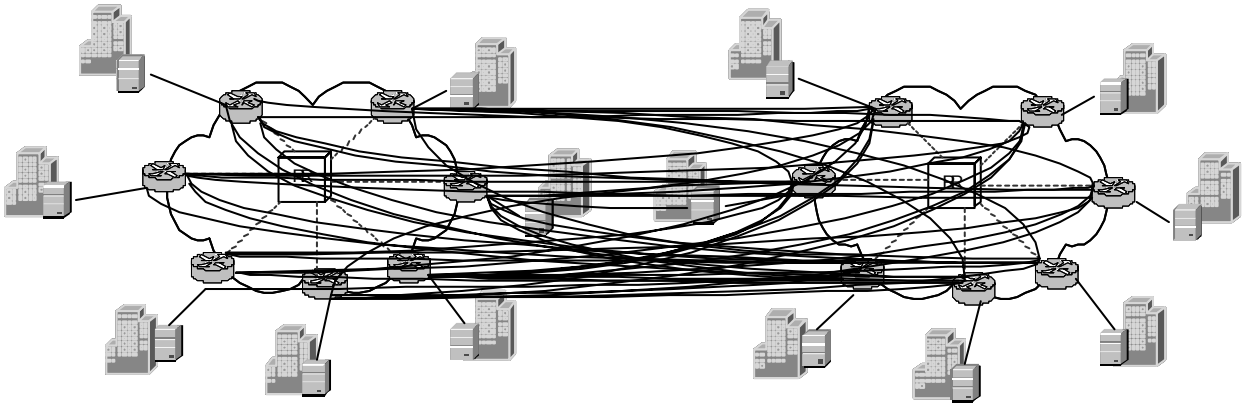


Рис.3.12. Многократная пересылка широковещательных данных по каналу связи между операторами.

С учетом тенденции переложить на BGP задачи сигнализации межоператорских MPLS L3 VPN unicast/multicast сервисов, использование протокола BGP для сигнализации VPLS выглядит продолжением единой концепции, однако очень проблематичны вопросы администрирования, поиска неисправностей.

Инструментарий администрирования и отладки

Никаких специализированных механизмов отладки L2VPN-BGP в настоящее время не разрабатывается, остается надеяться только на собственные навыки работы с протоколом BGP.

В настоящее время VPLS сервис на основе LDP поддерживается такими производителями как Alcatel, Cisco, Riverstone. Иерархический VPLS с поддержкой PWE3-CONTROL (то есть используется не Q-in-Q, а LDP) пока реализует только Alcatel. Драфт на основе BGP был разработан и реализован Juniper.

3.2.4. Масштабируемость VPLS

Стандарт IETF VPLS-LDP определяет способы использования иерархических топологий VPLS (HVPLS) для создания масштабируемых служб VPLS. Благодаря топологии «иерархической звезды» масштабируемость возможна как на уровне управления, так и данных. Масштабируемость накладывает определенные ограничения на сеть такие, как ограничение количества LSP, числа партнеров LDP, также необходимо распределять тиражированные пакеты между узлами.

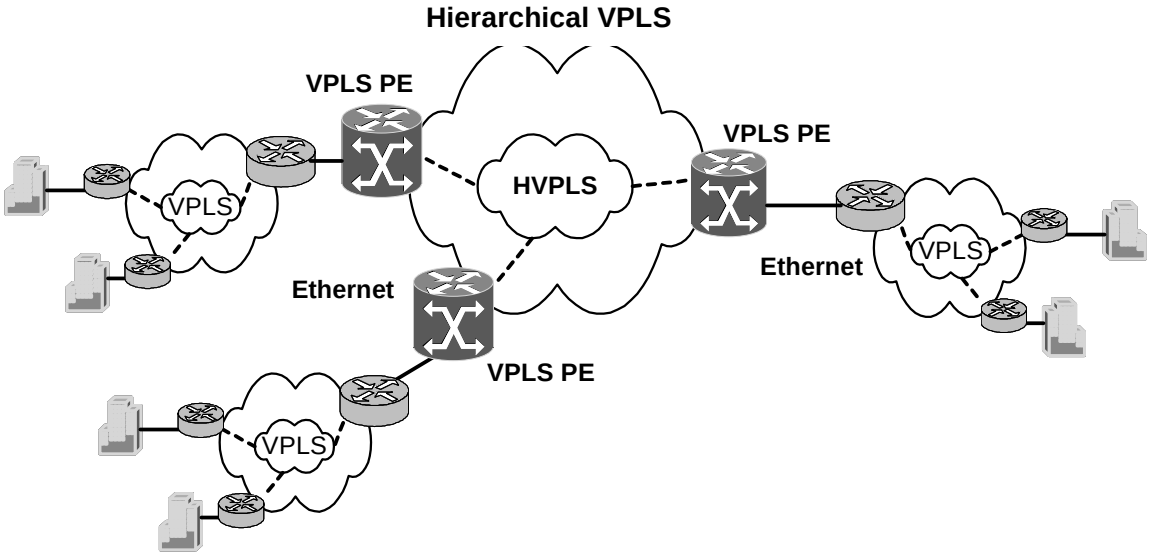


Рис.3.13. Иерархическая VPLS (HVPLS).

Другой важный аспект масштабируемости на втором уровне – это управление MAC адресами. В отличие от IP-адресов MAC-адреса не могут быть систематизированы, поскольку не обладают никакой иерархией. В VPLS предусматриваются различные способы для обращения с большим количеством MAC-адресов. Первая возможность заключается в применении со стороны клиента маршрутизатора в качестве оборудования CPE. Результатом становится использование одного MAC-адреса на узел. Вторая – использовать в качестве CPE коммутаторы Ethernet. Это требует наличия у провайдера устройств, способных ограничить общее количество MAC-адресов для каждого канала доступа, что особенно полезно для предупреждения «отказов в обслуживании».

Анализ и исследование подходов VPN-MPLS и VPLS для предоставления широкополосных услуг на базе технологии MPLS, произведенные в настоящей главе, позволяют перейти к выработке критериев сравнения и непосредственно к самому сравнению подходов, а также к анализу их применимости.

4. Сравнение VPN-MPLS и VPLS

В первой главе были рассмотрены широкополосные услуги, рынок которых заметно увеличился в последние годы. Далее речь шла о наиболее перспективных технологиях, позволяющих предоставлять все интересующие заказчика широкополосные услуги. А именно подробно рассматривались два подхода VPN-MPLS и VPLS, построенные на базе технологии MPLS, которая сегодня весьма популярна как магистральная технология. В главе 4 сравниваются изученные подходы по разработанным в этой же главе критериям и как результат сделаны выводы о возможностях их применения для предоставления широкополосных услуг.

4.1. Выработка критериев сравнения

Оба подхода VPN-MPLS и VPLS реализуются на базе MPLS/IP сети, которая используется для предоставления разнообразных услуг многочисленным клиентам. Так в сети может существовать несколько клиентов VPN, владеющих большими объемами конфиденциальной внутрикорпоративной информации, помимо услуги VPN сеть используется для организации многочисленных сервисов, соответственно в сети помимо клиентов VPN есть большое количество других пользователей, также сеть обеспечивает доступ в и из Интернет, что ещё больше расширяет круг возможных пользователей. Следовательно, встает вопрос защиты информации, передаваемой через MPLS/IP сеть. Соответственно, первый критерий, по которому будут сравниваться оба подхода, - защищенность виртуальной частной сети заказчика. Под защищенностью будем понимать предотвращение кражи трафика клиентов VPN при передаче через сеть провайдера, предотвращение доступа злонамеренного пользователя к ресурсам, расположенным в сайтах клиента, а также предотвращение раскрытия топологии сети пользователя.

Другой не менее важной характеристикой операторской сети является надежность. При предоставлении услуг провайдер должен поддерживать требуемое качество обслуживания. Одной из основных составляющих

поддержки требуемого качества обслуживания является обеспечение надежности сети провайдера. При разработке критерия надежности я не буду рассматривать характеристики конкретного оборудования, т.к. моей задачей является сравнение технологий VPN-MPLS и VPLS, а не обзор существующего оборудования. С точки зрения сетевых технологий под надежностью будем понимать возможность сети по организации резервных каналов, по реконфигурации, т.е. реакция сети на возникновение различных аварийных ситуаций.

Клиентские сети могут быть построены с использованием различных технологий и сетевых протоколов, например протоколов IPX, SNA, технологий ATM, FR. Следовательно, технология объединения сетей должна обладать свойством мультипротокольности, которое означает возможность сети по обеспечению прозрачной передачи пользовательских данных разного формата.

Для того, чтобы иметь возможность развиваться сообразно требованиям современного рынка технология должна обеспечивать масштабируемость, построенной на базе неё сети. Рассмотрим Масштабируемость как с точки зрения клиента, так и с точки зрения оператора. С точки зрения клиента сеть должна обеспечивать возможность роста компании клиента, а следовательно организацию новых сайтов. Со стороны оператора сеть тоже должна быть масштабируема, т.к. расширяется оператор как компания, было 10 клиентов стало 110, соответственно должна обеспечиваться возможность увеличения клиентской базы. Также оператор может расширять географически область действия своей сети. В последнее время широкополосные услуги становятся все более популярны и востребованы в корпоративном секторе, и именно крупные компании, как правило, являются основными заказчиками новых услуг, так корпоративный клиент может запросить расширение полосы пропускания для своих виртуальных частных сетей. Поэтому масштабируемость является важным критерием выбора технологии. Под масштабируемостью будем

подразумевать способность сети оператора к географическому расширению, увеличению клиентской базы и наращиванию мощности сети.

Успех провайдера сильно зависит от того, насколько полно он сможет удовлетворить запросы клиента. Поэтому некая гибкость в поддержке различных сетевых топологий позволит удовлетворить эти запросы оптимальным образом. Под поддержкой различных топологий связности будем рассматривать возможность обозначенных подходов поддерживать следующие сетевые топологии связности: точка-точка, hub-and-spoke, полносвязная топология, частично связная и перекрытие VPN.

Сравнивать технологии имеет смысл, если перед нами стоит проблема выбора, которая возникает, когда стоит задача построения сети на основе новой технологии. Соответственно немаловажным фактором, влияющим на выбор той или иной технологии, является сложность её внедрения оператором. Под сложностью внедрения технологии будем понимать сложность создания новой сетевой инфраструктуры и сложность адаптации существующей сетевой инфраструктуры оператора для реализации технологии.

После создания сетевой инфраструктуры для предоставления услуг виртуальных частных сетей необходимо осуществлять администрирование с целью предоставления услуг конкретным заказчикам. Чем сложнее механизм администрирования, тем больше временных затрат он потребует от персонала и соответственно более высокой квалификации обслуживающего персонала. Следовательно, больше вероятность ошибки на стадии организации предоставления услуги. Поэтому одним из критериев, которым следует руководствоваться при выборе технологии, является сложность организации предоставления услуги, под этим критерием будем понимать следующее – конфигурацию устройств сети для предоставления услуг VPN новому клиенту либо включение в VPN новых элементов сети клиента.

После создания инфраструктуры и подключения клиента необходимо управлять виртуальной частной сетью клиента и поддерживать её в

работоспособном состоянии. Под критерием «управление и поддержка» будем подразумевать управление конфигурацией созданной виртуальной частной сети и устранение возникающих неисправностей. От простоты и функциональности средств управления сетью напрямую зависят такие характеристики предоставления услуги, как качество и гибкость предоставления услуги, т.е. быстрое изменение полосы пропускания по требованию клиента и т.д.

Под экономическим критерием будем понимать относительную потенциальную экономическую эффективность двух подходов. В рамках этого экономическую эффективность целесообразно разделить на клиентскую и провайдерскую. Этот критерий для клиента будет определяться потенциальными затратами на использование этой услуги, а для провайдера будет определяться его затратами на организацию услуги.

4.2. Сравнение VPN-MPLS и VPLS

В этом параграфе будет производится анализ и сравнение рассмотренных в главе 3 подходов к предоставлению широкополосных услуг VPN-MPLS и VPLS на базе технологии MPLS по разработанным в предыдущем параграфе критериям.

4.2.1. Защищенность

Говоря о защищенности информации, обеспечиваемой VPN-MPLS и VPLS можно найти много общего. Т.к. обе технологии построены на базе MPLS, при передаче трафика через сеть провайдера организуются туннели, что в свою очередь затрудняет процесс перенаправления трафика злонамеренным пользователем. Обе технологии предполагают, что IP-заголовок не анализируется в сети провайдера, т.е. в таблицах маршрутизации ядра сети провайдера нет информации о клиентской сети, что позволяет защитить топологию клиентской сети. VPN-MPLS для обеспечения безопасности использует протокол IPSec. Протокол IPSec обеспечивает защиту на сетевом уровне и требует поддержки стандарта IPSec

только сообщающихся между собой устройств по обе стороны соединения. Все остальные устройства, расположенные между ними, просто передают трафик IP. IPSec охватывает несколько совершенно разных областей, в число которых входят аутентификация, шифрование и управление ключами защиты. В обеспечении безопасности в сетях VPN-MPLS большую роль играет протокол BGP. BGP присваивает уникальный параметр RD логическим портам. Значения параметра RD неизвестны конечным пользователям, и поэтому они не могут получить доступ к этой сети через другой порт и перехватить чужой поток данных. BGP распространяет таблицы FIB с информацией о VPN только участникам данной VPN, тем самым логически разделяя трафик и обеспечивая защиту передачи данных. Именно провайдер, а не заказчик присваивает порты определенной VPN во время её формирования. В сети провайдера каждый пакет ассоциирован с RD, и поэтому попытки перехвата пакета или потока трафика не могут привести к прорыву хакера в VPN. VPLS обеспечивает прозрачную передачу трафика, следовательно может использовать различные методы шифрования. Следовательно в силу своих особенностей и специальных механизмов обе технологии и VPN-MPLS и VPLS обеспечивают достаточно высокий уровень защищенности.

4.2.2. Надежность

Обеспечение надежности в сети VPN-MPLS организуется с помощью MPLS-TE и стандартными средствами MPLS Fast Reroute, а также возможностями протокола BGP. MPLS-TE предполагает возможность автоматического реконфигурирования TE-туннеля при возникновении неисправности с сохранением характеристик этого туннеля. Под средствами MPLS Fast Reroute понимается защита звена данных резервным туннелем с локальным принятием решения о перенаправлении трафика. VPLS работает на базе протокола LDP, который не имеет механизмов обнаружения петель, быстрого реконфигурирования сети, отказоустойчивости и т.д. При обеспечении надежности технология VPLS в клиентской сети использует

Ethernet решения, в частности протокол STP, в сети провайдера принято использовать решения MPLS/IP. STP – протокол связующего дерева, который призван обнаруживать и устранять петли при произвольной топологии LAN с диаметром сети, не превышающим 7 подряд идущих мостов. Также STP осуществляет резервирование трактов и восстановление сети в случае возникновения неисправности. RSTP – модификация STP (rapid STP), быстрее реконфигурирует сеть, чем STP, в сетях малого диаметра. Наравне с протоколом STP может использоваться протокол VRRP (Virtual Router Redundancy Protocol). При выходе из строя маршрутизатора на несколько минут может прерваться передача и обработка трафика клиентской сети. VRRP призван устранить столь длительный перерыв связи путем замены физического маршрутизатора по умолчанию виртуальным маршрутизатором по умолчанию (логическим), включающим в себя несколько физических маршрутизаторов. Таким образом эти маршрутизаторы дублируют друг друга, при нормальном функционировании сети они работают в режиме разделения нагрузки, например с несколькими пользовательскими устройствами. В аварийном режиме исправный маршрутизатор берет на себя всю нагрузку. Изначально виртуальные частные сети построенные на базе VPN-MPLS считались более надежными, чем сети, построенные на базе VPLS в силу того, что технология VPN-MPLS основывается на протоколе BGP. Для повышения надежности сетей VPLS технология предполагает использование специальных протоколов и механизмов, что ставит её в один ряд с технологией VPN-MPLS по обеспечению надежности.

4.2.3. Мультипрокольность

Сравнивая оба подхода, становится очевидно, что VPN-MPLS предполагает передачу только IP-трафика. Подход же VPLS позволяет работать с любым протоколом уровня 3 и передавать любые пакеты, поступающие из сети клиента: IPv4, IPv6, IPX, DECNet, OSI и т.д. Многие клиенты применяют не только протокол IP, но и другие протоколы для создания своей инфраструктуры, а подход VPLS не ограничивает их в выборе

протокола в отличие от VPN-MPLS. Сегодня становится все более популярным протокол IPv6, и многие организации уже внедряют его и в ближайшем будущем собираются широко его использовать. Для продолжения взаимодействия такого рода организаций с сетями VPN-MPLS требуется улучшение существующего стандарта, а именно создание адресного пространства VPN-IPv6, а также расширение возможностей маршрутизаторов в сети провайдера. Сети же VPLS могут продолжать обслуживать подобные организации, даже если сеть провайдера ещё не внедрила IPv6 в своей сети.

4.2.4. Масштабируемость

Говоря о масштабируемости технологий VPN-MPLS и VPLS можно найти много общего. Обе технологии считаются хорошо масштабируемыми по сравнению со схожими технологиями организации виртуальных частных сетей, за счет того, что информация о сети клиента на хранится в маршрутизаторах ядра сети, а хранится только на граничных маршутизаторах, которые непосредственно связывают сеть клиента с сетью провайдера. Ограничивающим масштабируемость фактором для обоих подходов будет максимальное число LSP или VC, которое сможет поддерживать данный LSR. Другим ограничивающим фактором опять таки для обоих подходов будет максимальный размер данных конфигурации, которые могут хранится на одном PE маршрутизаторе, т.к. данные конфигурации содержат всю информацию, относящуюся к виртуальной частной сети заказчика. В технологии VPN-MPLS данные конфигурации содержат информацию для VRF, RD, удаленных областей, фильтрации маршрутов. В технологии VPLS данные конфигурации содержат информацию для VPN, связанных с различными PE и для портов, ассоциированных с VPN пользователя. Использование автоматического обнаружения в совокупности с решениями VPLS уменьшает объем информации конфигурации для VPN, связанных с различными PE и следовательно уменьшает степень влияния размеров данных конфигурации

на масштабируемость. Для VPN-MPLS количество маршрутов, которое может хранится на одном PE также накладывает определенные ограничения на возможности масштабируемости сети, т.к. PE маршрутизатор хранит маршруты для всех виртуальных частных сетей, с которыми он связан. Чтобы смягчить влияние данного фактора на возможность масштабируемсоти, где возможно используется объединение маршрутов. Для VPLS максимальное число forwarding table entries , поддерживаемых одним PE маршрутизатором, вносит некоторые ограничения. PE маршрутизатор создает entries для того, чтобы иметь возможность осуществлять функции коммутации. Уменьшения влияния этого фактора требует, чтобы CE устройства были маршрутизаторами и/или ограничивалось число (MAC) entries, создаваемых для каждой виртуальной частной сети. Это помогает пользовательской VPN избежать перегрузки PE большим числом MAC-адресов источника. Следовательно, существуют некоторые ограничения мастштабируемости технологий VPN-MPLS и VPLS, однако существует также и ряд способов уменьшения влияния этих факторов. Поэтому технологии VPN-MPLS и VPLS считаются хорошо масштабируемыми. Для VPLS в целях повышения способности масштабируемости разработана иерархическая VPLS (HVPLS).

4.2.5. Поддержка топологий связности

Подход VPN-MPLS наиболее приемлем для реализации следующих топологий связности: точка-точка, полносвязная и перекрытие VPN, т.к. они прозрачны для CE устройств. Однако, VPN-MPLS преодолев определенные сложности может работать с топологиями hub-and-spoke и частично связной. Для работы VPLS более подходят топологии точка-точка, полносвязная, частично связная, hub-and-spoke. Очевидно, что hub-and-spoke и частично связная топология легче реализуется VPLS, за счет использования VC, чем VPN-MPLS, т.к. BGP осуществляет контроль маршрутов. VPLS также может использовать топологию перекрытия VPN, однако это потребует вовлечение CE устройств сайта, где это перекрытие происходит: CE должно будет

контролировать какой маршрут соотносится с каким VPN, т.е. при такой топологии CE устройства не являются прозрачными как в случае VPN-MPLS. Благодаря своим функциональным особенностям технология VPN-MPLS лучше реализует одни топологии связности , а VPLS другие. Соответственно в зависимости от того, какая топология связности наиболее импонирует оператору выбирается та или иная технология.

4.2.6. Сложность внедрения

Для создания виртуальных частных сетей на базе технологии VPN-MPLS обычно требуется наличие высококлассных конечных маршрутизаторов LSR, способных поддерживать многочисленные маршруты и пересылку данных на граничный маршрутизатор провайдера PE. Также необходимо, чтобы осуществлялся равноправный информационный обмен между этими маршрутизаторами. Если службы провайдера уже достаточно широко используют протокол BGP по всей сети, то в случае интенсивного IP трафика целесообразно использовать VPN-MPLS, т.к. это позволит использовать уже существующие BGP соединения и естественно LSP, уже организованные между PE для переноса трафика. Однако, при использовании существующих BGP соединение, следует внести некоторые изменения в область, обслуживаемую одним отражателем маршрутов для того, чтобы отражатель маршрутов не рухнул от слишком большого количества маршрутов к разнообразным VPN. Если провайдер использует конфедерацию, то эта проблема становится похожей на проблему inter провайдера, где VPN следует объединить множество автономных систем. Похожая ситуация и с отражателем маршрутов, провайдеру следует тщательно продумать, что должно быть сделано во избежание возникновения соединений маршрутизаторами и членами ASes, чтобы не происходило переполнение маршрутами. Технология VPLS требует более простых в функциональном плане PE маршрутизаторов и не требует наличия равноправных BGP сессий, установленных между PE. Служба провайдера, которая не основывается на BGP или не склонна к построению новых

сервисов VPN на базе BGP, избежит тем самым многих сложностей, решения технологии VPLS могут оказаться более привлекательными. Использовать ли BGP для сигнализации между PE или нет решает каждый провайдер для себя сам. В случае, если BGP уже внедрен, дальнейшее его использование сулит определенные выгоды, например, как уже упоминалось, наличие LSP соединений между PE для передачи трафика. Как следует из вышесказанного технология VPN-MPLS менее сложна в адаптации к существующей сетевой инфраструктуре оператора, если там используется протокол BGP. А технология VPLS является более простой с точки зрения внедрения оператором.

4.2.7. Сложность организации предоставления услуги

Сложность организации предоставления услуги для технологии VPN-MPLS заключается в организации процесса маршрутизации для каждой топологии связности виртуальной частной сети, требуемой заказчиком. Это означает создание VRF, которые будут содержать всю информацию о маршрутах пользователя и выбирать как назначать RD и Route Target Communities. Заметим, что служба провайдера должна решить следует ли VRF подключать пользователей к определенным интерфейсам, тем самым разделяя их или стоит собрать маршруты к различным VPN, как в случае перекрытия VPN. Также следует распределить RD и Route Target Communities для предоставления услуг VPN. PE маршрутизаторы соединяются с сайтами пользователей, что заставляет VPN конфигурировать требуемые VRF, RD и Route Targets и другое, что может потребоваться для работы с определенной топологией. Клиентский маршрутизатор CE должен обладать теми же функциями, что и PE маршрутизатор провайдера, чтобы иметь возможность изменить маршрут, при необходимости. Организация предоставления услуги на базе технологии VPLS несколько проще. Каждому PE маршрутизатору, соединенному с виртуальной частной сетью, необходимо иметь информацию о других PE для установления VC с заданной VPN. Порт PE маршрутизатора, соединенный с сайтом пользователя

соотносится с конкретной VPN. Заметим, что использование автоматического обнаружения исключает необходимость детально конфигурировать PE, имеющие отношение к той же VPN.

4.2.8. Управление и поддержка

Управление виртуальной частной сетью, построенной на базе технологии VPN-MPLS, заключается в том, что при изменении конфигурации или решении проблем, возникающих при устранении неисправности, инженеры службы провайдера должны вручную произвести все необходимые операции с BGP соединениями, BGP маршрутами к различным удаленным областям, их распределение и выбор PE, который будем осуществлять равноправный информационный обмен с клиентским CE маршрутизатором и т.д. Как и в большинстве масштабируемых IP сетях, область отражателя маршрутов или конфедерация с многочисленными членами ASes могут способствовать усложнению вышеупомянутой задачи. Работа с большим числом маршрутов, относящихся к многочисленным таблицам маршрутизации и пересылки, помимо глобальной таблицы конечно требует больше возможностей нежели работа с одной таблицей. Наконец, данные конфигурации, находящиеся на PE маршрутизаторе, разрастутся до такой степени, что будет сложно покрыть неконфигурированную область. Подход VPLS решает эту задачу проще, т.к. провайдер не хранит никакой информации, связанной с маршрутами клиента, не контролирует их распределение или обмен информацией между различными клиентскими CE маршрутизаторами. Т.к. не используется протокол BGP управление и устранение неисправностей также упрощаются, инженеры службы провайдера имеют дело с VC, создаваемых для VPN и портами, соединенными с конкретной VPN. На одном PE маршрутизаторе инженеры имеют дело только с одной таблицей маршрутизации, несмотря на то, что VFI таблица MAC адресами источника в процессе обучения. Также как и в случае VPN-MPLS, при сильном увеличении объема данных конфигурации становится сложнее распознавать неконфигурированные области сети. Как

уже говорилось ранее использование автоматического обнаружения может существенно снизить объем данных конфигурации.

4.2.9. Экономический критерий

Сравнивая стоимость внедрения технологий следует отметить, что стоимость решений VPN-MPLS будет незначительно выше, но все же выше, чем решения технологии VPLS, за счет того, что подход VPN-MPLS предполагает более сложные маршрутизаторы, способные поддерживать многочисленные VRF. Стоимость управления и поддержки рассматриваемых подходов напрямую зависит от сложности подхода. Очевидно, что VPN-MPLS будет обладать более высокой стоимостью, за счет своей сложности, по сравнению с VPLS. Сложность подхода требует наличия некоторого уровня применяемого оборудования, т.е. оборудования, удовлетворяющего современные требования провайдера.

4.3. Применение технологий VPN-MPLS и VPLS

В этом параграфе рассматривается применение технологий VPN-MPLS и VPLS на примере нескольких компаний с различными направлениями бизнеса. В зависимости от специфики деятельности предприятия предъявляются различные требования к построению виртуальной частной сети, исходя из которых выбирается наиболее подходящая технология.

Предприятия финансового сектора

Проанализируем требования, выдвигаемые предприятиями данного сектора.

Способность самостоятельно управлять шифрованием информации из конца в конец, т.е. возможность выбирать способ шифрования при передаче трафика от одного пользователя другому. Воспользуемся сравнением по критерию «защищенность». В результате чего, выбираем технологию VPLS, т.к. она обеспечивает прозрачную передачу трафика, следовательно заказчик может использовать различные методы шифрования, в отличие от VPN-MPLS, в которой способ шифрования определяется протоколом IPSec.

Сеть заказчика построена в соответствии с частично связной топологией. Как следует из критерия «поддержка топологий связности» для реализации данной топологии наиболее приспособлена VPLS.

Минимальное время восстановления при возникновении любой неисправности, т.к каждая минута простоя может повлечь за собой большую потерю доходов. Согласно критерию «Управление и поддержка» устранение неисправностей в сети, построенной на базе VPLS, проще. За счет того, что инженеры службы провайдера имеет дело только с частью информации конфигурации, ограниченной конкретной VPN.

Способность работать с различными протоколами сетевого уровня. Очевидно, что свойством мультипротокольности обладает только технология VPLS.

Относительная простота оконечного устройства, находящегося на стороне клиента. Согласно анализу, проведенному в соответствии с критерием «сложности организации предоставления услуги» для построения сети на базе технологии VPLS, клиентский маршрутизатор CE не должен обладать теми же функциями, что и провайдерский PE, т.к. не требуется маршрутного разделения пользовательской информации. Также не предъявляются серьезные требование и к PE, т.к. нет необходимости поддерживать многочисленные таблицы маршрутизации, относящимся к разным VPN.

Способность сети к быстрой реконфигурации. При рассмотрении критерия «надежность», говорилось о специальных протоколах, работающих на пару с LDP, в частности протокол RSTP, который призван быстро обнаруживать и устранять петли, другими словами быстро реконфигурировать сеть при произвольной топологии.

За счет использования более простых оконечных устройств клиента и резервирования только критичных приложений построение сети на базе VPLS буде дешевле нежели на VPN-MPLS.

Как следует из всего вышесказанного для предприятий финансовой отрасли виртуальные частные сети наиболее приемлемо строить на базе технологии VPLS.

Предприятия торговли

При построении виртуальных частных сетей предприятия, работающие в области торговли, предъявляют следующие требования.

Возможность создания экстрасети на базе нескольких различных технологий передачи (на втором уровне). При организации экстрасети немедленно встает вопрос о защите информации, аутентификации, авторизации. Протокол IPSec обладает целым набором механизмов, способных обеспечить все вышеперечисленные требования к защищенности, а следовательно в данном случае наиболее подходит технология VPN-MPLS для создания VPN.

Передача только IP-трафика, таким образом свойство мультипротокольности не является обязательным.

Наличие большого количества соединений многочисленных поставщиков, складов с главным офисом, в настоящее время соединенных устаревшей пакетной технологией, например Frame Relay. Возможность добавления новых сайтов (складов, поставщиков) без изменения используемой сетевой топологии. Согласно критерию «управление и поддержка» сеть, построенная на базе VPN-MPLS, наиболее приемлема для работы с многочисленными постоянно меняющимися удаленными сайтами, за счет использования протокола BGP, обладающего механизмом автоматического обнаружения. С точки зрения сложности организации предоставления услуги легкое согласование соединений при частых добавлениях, изменениях, передвижениях поставщиков и других участников экстрасети также наиболее приемлема технология VPN-MPLS, за счет механизмов, используемых протоколом BGP.

Обеспечение топологии «перекрытие VPN», что с легкостью реализуется технологией VPN-MPLS.

Создание масштабируемой сети. Сеть, построенная на базе VPN-MPLS, достаточно хорошо масштабируема и ограничивается только возможностями BGP.

Таким образом для предприятий торговли больше подходит технология VPN-MPLS, а не VPLS.

Предприятия медицинской отрасли

При построении виртуальной частной сети для медицинского учреждения важен вопрос обеспечения строгой конфиденциальности определенных данных, в тоже время нежелание разделять потоки маршрутной информации. Как неоднократно упоминалось, технология VPLS позволяет заказчику выбирать различные методы шифрования в том числе в зависимости от секретности передаваемой информации. Поэтому с точки зрения защищенности в данном случае следует выбрать технологию VPLS.

Т.к. к различным учреждениям сферы медицинского обслуживания медицинским обращаются как многочисленные организации, так и частные лица возникает вопрос поддержки не только IP-трафика, т.е. сеть должна обладать свойством мультипротокольности.

Как видно из рассмотренных примеров выбор технологии является сугубо индивидуальным для каждого предприятия. Хоть между VPN-MPLS и VPLS не так много существенных различий, при построении виртуальной частной сети для определенного предприятия следует ясно представлять требования к сети и возможности, которые предоставляют технологии

Заключение

В дипломной работе, посвященной разработке критериев сравнения технологий VPN-MPLS и VPLS, были рассмотрены современные технологии построения виртуальных частных сетей, проведен сравнительный анализ подходов к предоставлению широкополосных услуг, построенных на базе технологии многопротокольной коммутации на основе меток MPLS.

В результате проведенного анализа можно сделать вывод о том, что технологи VPN MPLS и VPLS на сегодняшний день являются ведущим технологиями не только построения виртуальных частных сетей, но и предоставления всего существующего многообразия широкополосных услуг. Они обладают хорошей масштабируемостью, гибкостью, надежностью, не накладывает каких-либо ограничений на протоколы вышестоящего уровня, а применение меток для коммутации в сети провайдера MPLS позволяет реализовать ускоренную передачу трафика по магистральной сети.

Совместная работа MPLS, механизмов Traffic Engeenering и VPN-MPLS или VPLS позволяет предоставить для каждого информационного потока безопасный туннель с гарантированным уровнем качества обслуживания, что имеет большое значение в свете перехода к мультисервисным сетям.

Разработанные в данной работе критерии сравнения и рассмотренные примеры возможного применения подходов для предоставления широкополосных услуг на базе технологии MPLS могут быть взяты на вооружение провайдерами, стоящими перед выбором той или иной технологии и крупными корпоративными клиентами, имеющими острую необходимость в создании своих виртуальных частных сетей.

Список литературы

1. Гольдштейн А.Б., Гольдштейн Б.С. Технология и протоколы MPLS. С-Пб.: БХВ-Санкт-Петербург, 2005.
2. Cisco Systems и др. Руководство по технологиям объединения сетей. 3-е издание. М.: Издательский дом «Вильямс», 2002.
3. Засецкий А.В., Иванов А.Б., Постников С.Д., Соколов И.В. Контроль качества в телекоммуникациях и связи. Часть 2. М.: Компания Сайрус Системс, 2001.
4. Abdelhalim A. IP/MPLS – Based VPNs. Layer-3 vs Layer-2 / Foundry Networks, 2002.
5. Greene T. LAN Services to get new look / Network world, 2004, №9.
6. Capuano M. VPLS: Scalable Transparent LAN Services / Junipier Networks, 2003.
7. Барсков А.Г. Как нести бродбэнд в массы? / Сети и системы связи, 2002, № 13.
8. Петрусов Д. Metro Ethernet как синоним оптических городских сетей / Connect! Мир связи, 2003, № 11.
9. Захватов М. Построение виртуальных частных сетей (VPN) на базе технологии MPLS. М.: Риверсайд Тауерз, 2004.
10. Лассерре М. Межсоединение локальных сетей посредством MPLS / Журнал сетевых решений LAN, 2004, № 8.
11. Сянбин Л. Как построить практическую и управляемую широкополосную сеть / Вестник связи, 2002, № 1.
12. Вишняков А. Сигнализация VPLS: LDP или BGP? / mpls-exp, 2005.
13. Орлов С. Перекресток миров / Журнал сетевых решений LAN, 2004, № 5.
14. Песков С.Н., Шишов А.К. Интерактивные мультимедийные кабельные сети / Информ Курьер Связь, 2004, № 1.
15. Тема номера. Знакомтесь: Ethernet Virtual Private LAN / Connect! Мир связи, 2004, № 2.
16. www.vpls.org
17. www.cisco.com
18. www.mrv.com
19. www.alcatel.com
20. www.ietf.org/internet-drafts/draft-ietf-l2vpn-vpls-ldp-05.txt