

Виртуальные частные сети уровня 2 на основе MPLS

Киреети Компелла, старший инженер

Мэтт Колон, инженер по маркетингу

Пьер Бишон, системный инженер

Аннет Кэй Доннелл, инженер по маркетингу

Содержание

Введение	2
Историческая перспектива	2
ВЧС уровня 2 на основе MPLS	3
Неотъемлемая масштабируемость	3
Разделение административной ответственности	4
Конфиденциальность и безопасность маршрутизации	4
Простота конфигурирования	4
Стандартная многопротокольная поддержка	4
Гибкость сигнализации	4
Защита трафика MPLS	5
Разработка стандартов MPLS	5
Экономичный переход от традиционных ВЧС уровня 2	5
ВЧС уровня 2 на основе MPLS компании Juniper Networks	5
Замещение ATM	7
Дополнительные услуги	7
Оператор операторов	7
Услуги высокоскоростной связи ЛВС	8
Точки доступа сети Интернет на базе MPLS	9
Заключение	11

Введение

Виртуальные частные сети (ВЧС) на основе Frame Relay или ATM распространены достаточно широко, но стоимость содержания отдельных сетей для трафика Интернет и ВЧС, а также сложности администрирования ВЧС вынуждают искать альтернативные решения. Наша статья обсуждает одну из альтернатив, а именно ВЧС поверх каналов уровня 2, использующих протокол MPLS. Также рассказывается, какие решения компания Juniper Networks, Inc. предлагает для ВЧС уровня 2.

В решении уровня 2 на основе MPLS поставщик услуг, или провайдер, поддерживает единую сеть, поверх которой могут выполняться другие службы, такие как стандартный IP класса best-effort, ВЧС уровня 3, регулирование трафика, Diffserv и другие службы конвергентных сетей. Juniper Networks® предлагает ряд гибких и масштабируемых решений ВЧС, развертываемых в одной сети. Объединение различных служб в единой инфраструктуре существенно снижает стоимость эксплуатации и сложность сети.

Историческая перспектива

Первые корпоративные сети использовали для связи отдельных офисов выделенные каналы. Такие сети обеспечивали связь, но были дороги, и полоса пропускания в них использовалась неэффективно.

Первые ВЧС строились на основе каналов уровня 2: X.25, Frame Relay и ATM. Эти ВЧС проще параметризовать, чем выделенные линии, а виртуальные каналы позволяют использовать общую

инфраструктуру для всех ВЧС. Такие традиционные ВЧС являются существенным шагом вперед относительно выделенных линий, но и они имеют свои недостатки.

Небольшая скорость передачи. Без поддержки каналов OC-192c/STM-64 они не могут удовлетворить все возрастающие требования по скорости, предъявляемые Интернетом.

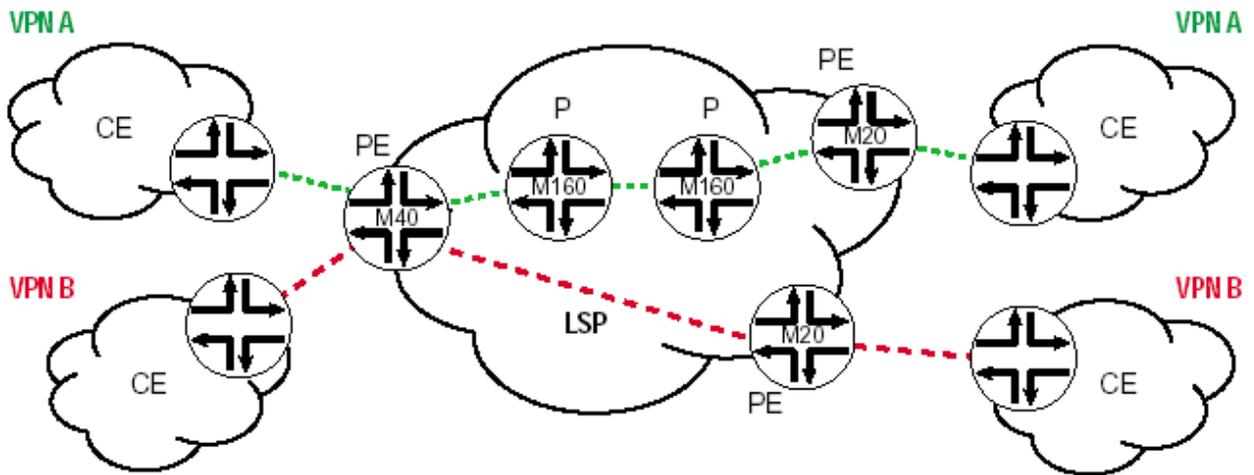
Инфраструктура ВЧС привязана к единственной среде передачи, например, ATM. Трудности усугубляются, если инфраструктура Интернета использует те же самые физические линии.

Хотя формирование параметров намного проще, чем в выделенных линиях, сложности остаются, что становится особенно очевидным при добавлении нового сайта в существующую ВЧС.

Решение ВЧС уровня 2 на основе MPLS сохраняет преимущества традиционных ВЧС уровня 2, используя достижения современных технологий маршрутизации в отношении скорости, гибкости и легкости параметризации. Услуги ВЧС уровня 2 на основе MPLS можно предлагать вместе с IP класса best-effort и ВЧС уровня 3, управляя всеми службами по одной сетевой инфраструктуре.

ВЧС уровня 2 на основе MPLS

Решение ВЧС уровня 2 на основе MPLS позволяет провайдеру использовать свою сеть MPLS для предоставления клиенту услуг уровня 2. С точки зрения клиента, он получает каналы, соединяющие отдельные сайты; каждое граничное клиентское устройство (CE) имеет идентификатор DLCI (в случае Frame Relay), на основе которого идет передача к другим CE через сеть провайдера, видимая клиенту как традиционное облако уровня 2. В провайдерской сети MPLS пакеты уровня 2 транспортируются по путям коммутации меток (LSP). Провайдер не участвует в маршрутизации клиентской сети уровня 3, что дает ощутимые преимущества, особенно с точки зрения граничных маршрутизаторов (PE) поставщика услуг.



CE (Customer Edge) – граница абонента
P (Provider Router) – маршрутизаторы поставщика услуг
PE (Provider Edge) – граница поставщика услуг

Рисунок 1. ВЧС уровня 2 на основе MPLS

Неотъемлемая масштабируемость

В ВЧС уровня 2 на основе MPLS маршрутизаторы PE разделяют между собой только малое количество информации о каждом маршрутизаторе CE. Поэтому каждый PE хранит только один адрес от каждого CE и поддерживает один маршрут к каждому CE во всех ВЧС. Базы информации форвардинга и маршрутизации маршрутизаторов поставщика услуг масштабируются линейно с увеличением числа клиентских сайтов.

Разделение административной ответственности

В ВЧС уровня 2 провайдер отвечает за связь уровня 2, тогда как клиент отвечает за связь уровня 3, предполагающую маршрутизацию. Как только PE проложит маршрут от подключенного к нему CE к другим CE в той же самой ВЧС, его работа закончена. Так, если у клиента проблемы со связью, провайдеру необходимо продемонстрировать, что сайт А связан с сайтом В. Организация маршрутизации в частной сети клиента – это задача клиента.

Такое разделение ответственности также изолирует проблемы в сети клиента от сети поставщика услуг. Неправильно сконфигурированный клиентский маршрутизатор CE может в худшем случае нестабильно поддерживать маршрут, но это мало повлияет на сеть провайдера. Клиент может реализовать в своей сети любую интересную ему технологию без опасений дестабилизировать сеть провайдера.

Конфиденциальность и безопасность маршрутизации

Провайдера не должны интересовать вопросы масштабируемости таблицы маршрутизации или наложения адресных пространств, так как разделение маршрутной информации по каждой ВЧС создает естественные границы как между различными клиентами, так и между сетью провайдера и клиентами. Это естественное разделение уменьшает административную нагрузку на провайдера и обеспечивает клиентам тот же уровень безопасности маршрутизации и конфиденциальности данных, к которому они привыкли в традиционных ВЧС уровня 2.

Простота конфигурирования

Трудности конфигурирования традиционных ВЧС уровня 2 определяются "проблемой N квадрат" в условиях полной связности. Если N - число CE в полносвязной ВЧС Frame Relay, то провайдер должен администрировать в своей сети $N*(N-1)/2$ постоянных виртуальных каналов (PVC). На каждом CE необходимо сконфигурировать (N-1) идентификаторов DLCI для связи с другими CE. Более того, когда добавляется новый CE, необходимо параметризовать N новых постоянных виртуальных каналов DLCI PVC и обновить DLCI на всех CE, чтобы они могли связываться с добавленным маршрутизатором CE.

Стандартная многопротокольная поддержка

Так как провайдер просто обеспечивает связь уровня 2, клиент может реализовать любой протокол уровня 3 по своему усмотрению. Эта гибкость позволяет клиентам использовать ВЧС уровня 2 как стандартный транспорт для IBM SNA, Novell IPX или любого другого стека протоколов без дополнительной инкапсуляции. Это также позволяет провайдеру развертывать новые службы, такие как связь территориально разнесенных ЛВС (transparent LAN) или услуги multicast.

Гибкость сигнализации

Для прокладывания путей ВЧС через маршрутизаторы провайдера можно использовать протоколы сигнализации LDP или RSVP. Возможно гибридное решение: LDP на границе сети, RSVP - в магистрали. RSVP предоставляет возможности регулирования трафика, что позволяет явно выбирать пути для конкретных ВЧС. С помощью RSVP можно регулировать трафик данных клиента для обеспечения, например, заданной задержки, включая этот параметр (дополнительно оплачиваемый клиентом) в соглашение об уровне обслуживания.

Маршрутизатор PE может сигнализировать о своей принадлежности к ВЧС уровня 2 двумя способами: по протоколу LDP или BGP4. Пока предпочтение не отдано ни одному из этих протоколов, но BGP4 имеет некоторые преимущества.

- Практически все граничные маршрутизаторы поддерживают BGP4
- BGP4 разработан для транспорта многочисленных маршрутов различных типов.
- BGP4 лучше работает с междоменной маршрутизацией, необходимой в ВЧС, охватывающих несколько поставщиков услуг, и в ВЧС, принадлежащих "оператору операторов".

- Маршрутизаторы PE могут обслуживать сессии протокола IBGP для рефлекторов маршрута в качестве альтернативы полносвязным сессиям IBGP. Развертывание множества рефлекторов маршрута улучшает масштабируемость, так как устраняется необходимость в наличии такого компонента сети, который должен был бы хранить все маршруты ВЧС.
- Цели импорта и экспорта маршрута позволяют управлять точкой, где объявляется конкретный маршрут.

Защита трафика MPLS

MPLS предлагает многочисленные способы защиты целостности трафика, включая вторичные пути LSP и быструю ремаршрутизацию, которые увеличивают надежность услуг, предлагаемых в магистральной MPLS. Наличие этих механизмов позволяет провайдеру обеспечивать различные уровни защиты трафика, оговаривая это в соглашениях об уровне обслуживания.

Разработка стандартов MPLS

Ширится сфера охвата MPLS, растет уровень разработок, магистраль MPLS готовится к их внедрению. Новый стандарт Generalized MPLS предлагается внедрить и в оптических сетях, динамически управляя с его помощью отдельными световыми волнами. Выбирая решение MPLS, провайдер выбирает его существующие и перспективные преимущества.

Экономичный переход от традиционных ВЧС уровня 2

Так как ВЧС на основе MPLS с точки зрения клиента неотличима от традиционной ВЧС уровня 2, при переходе от одной к другой у клиента практически не возникает никаких проблем. Это помогает снять вопросы, касающиеся адаптации к новой технологии или ее воображаемой сложности.

Столь же прост и переход к ВЧС от арендуемых линий. Способ, которым линии ВЧС уровня 2 объявляются в протоколе маршрутизации, в основном идентичен способу объявления каналов ATM, Frame Relay, арендуемых и физических линий.

ВЧС уровня 2 на основе MPLS компании Juniper Networks

Реализация ВЧС уровня 2 на основе MPLS, предлагаемая компанией Juniper Networks, базируется на кросс-коммутации каналов MPLS. Этот метод инкапсуляции гарантирует прозрачный транспорт любого типа трафика по магистральной MPLS.

Эта функция гарантирует прозрачное соединение двух каналов уровня 2 на границах сети. Так как не производится проверки или поиска уровня 3, кросс-коммутация каналов поддерживает передачу любого протокола уровня 3 в данных пакета. При кросс-коммутации каналов осуществляется статическое отображение входящих логических портов, виртуальных каналов или DLCI в исходящие.

Поддерживается инкапсуляция следующих протоколов:

- ATM (AAL5 или cell relay)
- Ethernet 802.1Q VLAN
- Frame Relay
- HDLC
- MPLS (stitching)
- PPP

Этот механизм обеспечивает создание туннелей через облако магистральной сети DLCI между маршрутизаторами CE (см. рис. 2 и 3).

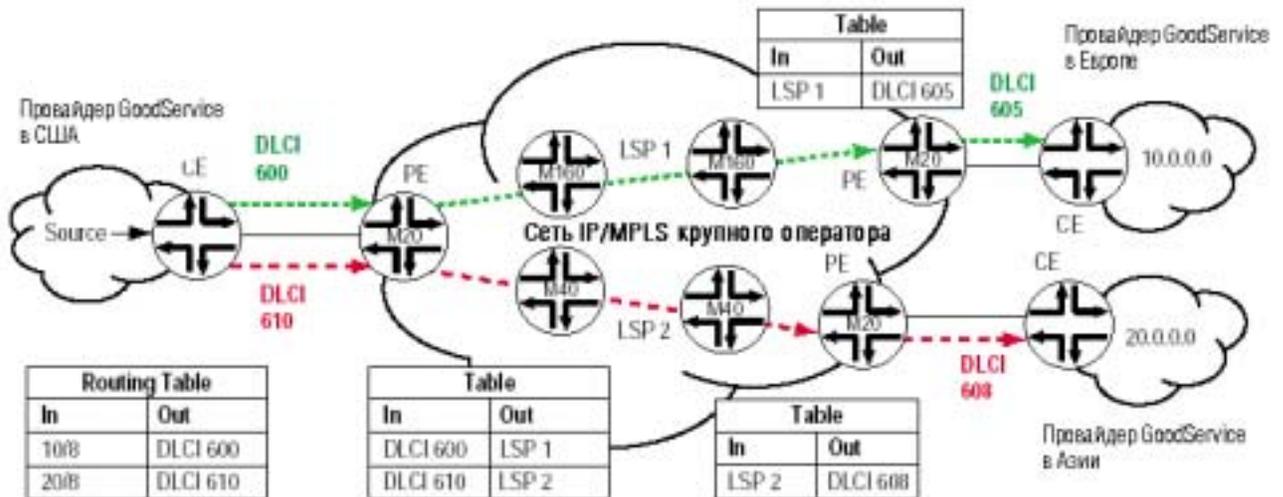


Рисунок 2. Пример сети с кросс-коммутицией каналов Frame Relay

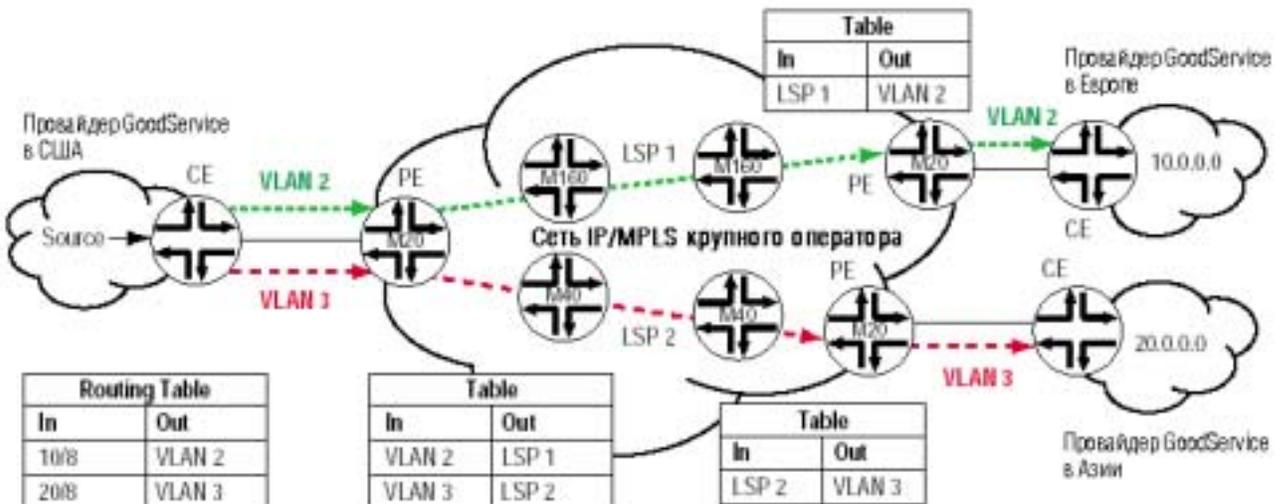


Рисунок 3. Пример сети с кросс-коммутицией каналов виртуальных ЛВС Ethernet 802.1Q

Блоки протокола данных (PDU) различных инкапсуляций обрабатываются функцией кросс-коммутиции следующим образом:

- В ВЧС поверх ATM AAL5 блоки PDU AAL5 транспортируются без непосредственного переноса идентификаторов VPI/VCI. На принимающем маршрутизаторе PE блок AAL5 PDU фрагментируется, идентификатор VPI/VCI добавляется к каждой ячейке, и ячейки пересылаются на маршрутизатор CE. Используемые VPI/VCI наследуются от верхней метки MPLS.
- В ВЧС поверх ATM cell relay ячейки, переданные одним маршрутизатором CE, транспортируются как есть, к каждой ячейке добавляется заголовок MPLS. Принимающий PE удаляет заголовок MPLS и продвигает ячейку к соответствующему CE.
- В ВЧС поверх Frame Relay два байта DLCI отбрасываются, и оставшаяся часть транспортируется как кадр уровня 2. На приемном PE к вновь созданному заголовку Frame Relay добавляется новый идентификатор DLCI, заголовок добавляется к кадру, и кадр отправляется на CE.
- В ВЧС поверх протоколов PPP, Cisco HDLC и Ethernet VLAN кадр уровня 2 транспортируется целиком, без изменений. Кадр уровня 2 не включает флаги HDLC, преамбулы Ethernet или

CRC. Предполагается, что битовое или байтовое заполнение не производится. На приемном маршрутизаторе PE кадр отправляется на маршрутизатор CE по соответствующему интерфейсу.

Замещение ATM

Благодаря возможностям кросс-коммутации MPLS оперировать службами ATM AAL5 и cell-relay, можно предлагать клиентам транзитные решения для приложений, использующих сквозную передачу ATM. Уровень AAL5 подходит для приложений, использующих ATM как общий транспорт уровня 2, и поэтому устойчивых к некоторым задержкам и вариациям задержки, характерных для AAL5. Служба cell-relay не знает ничего об уровнях адаптации AAL, не производит сегментации и повторной сборки в сети поставщика услуг и поэтому подходит для многих приложений класса VBR.

Если некоторые сети ATM используются в основном для эмуляции каналов и других услуг реального времени класса CBR, то практически все другие каналы ATM могут быть заменены на ВЧС уровня 2 на основе MPLS.

Дополнительные услуги

ВЧС уровня 2 на основе MPLS можно использовать для создания и продажи дополнительных IP услуг в единой магистральной инфраструктуре, включая услуги оператора для других операторов, ВЧС уровня 2, доступ к экстрасетям уровня 2, высокоскоростная связь ЛВС, доступ в Интернет.

Оператор операторов

Провайдер может предлагать другим провайдерам услуги с прозрачной полосой пропускания для развертывания магистрали без построения собственной транспортной сети (рис. 4). Такие услуги можно назвать *услугами виртуальной магистрали* на региональном, национальном или международном уровнях. Оператор будет управлять своим собственным сетевым оборудованием и подключаться к сети "оператора операторов" как сайт CE к узлу PE. При этом между CE и PE можно использовать любой поддерживаемый протокол уровня 2 при условии, что каждое сквозное соединение реализует один и тот же протокол доступа на обоих концах. Провайдеру для обслуживаемого им оператора необходимо только поддерживать пути LSP MPLS между любыми сквозными соединениями. В качестве дополнительной услуги можно предлагать регулирование трафика транзитных путей LSP.

Такие услуги намного эффективнее для оператора, чем использование арендуемых или оптоволоконных линий. При создании отображения между парой PVC или виртуальных ЛВС для подключения к нескольким удаленным маршрутизаторам CE достаточно одного CE. Более того, можно предлагать любую полосу пропускания, так как локальные соединения могут иметь скорость от T1/E1 до OC-48c/STM-16 и OC-192c/STM-64.

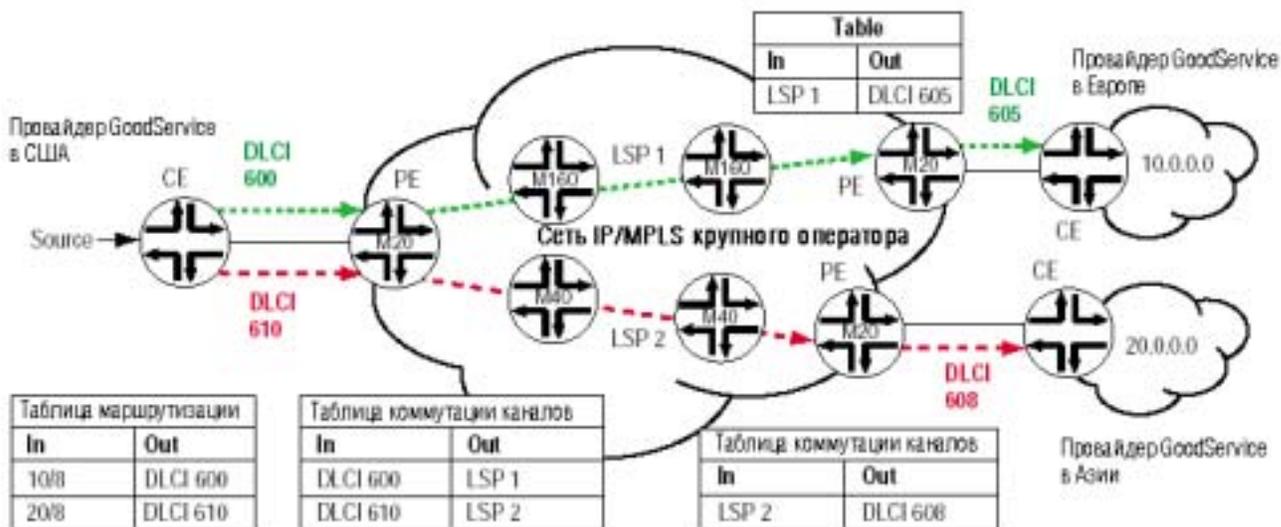


Рисунок 4. Оператор операторов

Для удовлетворения потребностей клиентов, являющихся операторами сетей MPLS, можно развернуть предлагаемую Juniper Networks функцию "сшивания" путей *LSP stitching* (см. рис. 5). Сшивание LSP позволяет провайдеру отображать входной LSP оператора на LSP в своей магистрале и далее на выходной LSP оператора. Такой метод позволяет провайдеру предоставлять клиентам услуги MPLS, делая свою сеть как бы мостом между другими разрозненными по разным причинам сетями.



Рисунок 5. Сшивание путей LSP

Услуги высокоскоростной связи ЛВС

В городских сетях та же инфраструктура IP/MPLS используется для предоставления клиентам высокоскоростной связи по интерфейсам ЛВС, таким как Fast Ethernet и Gigabit Ethernet. Развернуть эту службу при наличии магистрали IP/MPLS просто, так как необходимо поддерживать только одну сеть Ethernet через ГВС. Можно предлагать IP услуги и соединения ЛВС-ЛВС на уровне 2 (рис. 6). Клиент может использовать одну виртуальную ЛВС для доступа к IP-услугам, вторую - для организации внутренних или международных интрасетей, другие виртуальные ЛВС - для подключения к нескольким сайтам в том же городе. На границе клиентской сети можно использовать удаленное соединение Ethernet по оптоволоконному кабелю (например, для подключения к существующему коммутатору ЛВС), арендуемый концентратор Ethernet (к которому подключаются клиенты, находящиеся в одном здании) или маршрутизатор Juniper Networks для подключения нескольких клиентов с различными скоростями.

Преимущества применения маршрутизаторов Juniper Networks для высокоскоростного соединения ЛВС:

- Низкие и стабильные значения задержек в маршрутизаторах Juniper Networks позволяют проектировать сеть любой архитектуры, способную расширяться без пересмотра всей структуры сети.
- Бесшовный доступ со скоростями от 100 Мбит/с до 1 Гбит/с.
- Покрывание дистанций до 70 км с использованием передовых технологий Gigabit Ethernet.
- Избыточность магистрали MPLS: функция быстрой ремаршрутизации меняет путь LSP в случае отказа магистрального канала или узла менее чем за 100 миллисекунд, делая отказ незаметным для трафика пользователя.

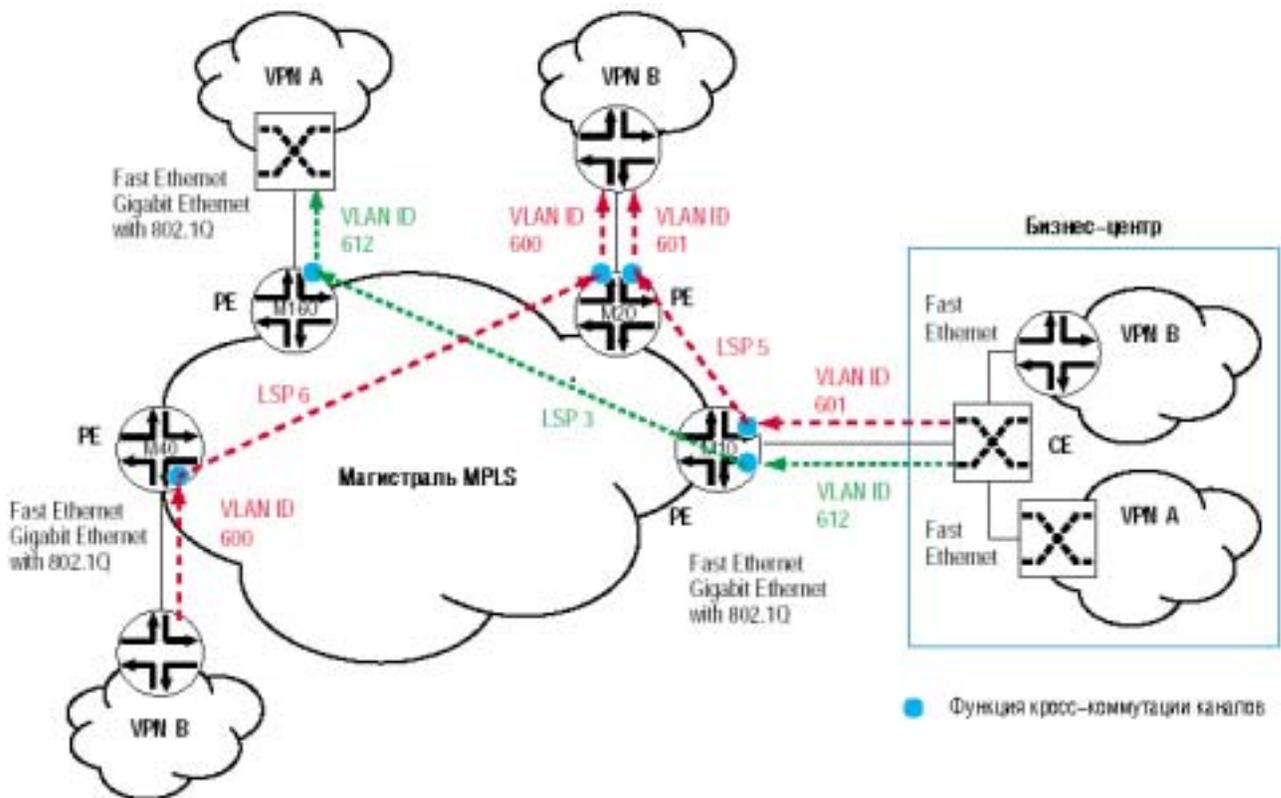


Рисунок 6. Высокоскоростные услуги соединения ЛВС

Точки доступа сети Интернет на базе MPLS

В настоящее время точки доступа Интернета сталкиваются с проблемами масштабирования, которые решаются при помощи MPLS (рис. 7). Например, можно организовать высокоскоростные гигабитные каналы, управлять обменом маршрутной информацией на уровне 2, организовать удаленные соединения обмена маршрутной информацией, управлять полосой пропускания и поддерживать классы обслуживания.

Для соединений обмена маршрутной информацией, или пиринга, MPLS использует скорости OC-192c/STM-64, при этом нет накладных расходов ATM, и есть возможность выполнения поверх любой среды или протокола уровня 2, такого как SONET/SDH (Frame Relay, PPP, HDLC), ATM или Ethernet. Технологии ATM не могут работать на скоростях выше OC-48c/STM-16 (из-за ограничений аппаратной реализации SAR), а в технологии Ethernet затруднена организация удаленных соединений пиринга.

Услугу точки доступа Интернета на базе MPLS можно реализовать двумя способами.

- Коммутируемые сквозные туннели с регулированием трафика, когда центральный маршрутизатор только коммутирует пути LSP MPLS и не выполняет маршрутизацию BGP. Сигнализация путей LSP – сквозная между реер-маршрутизаторами.
- Кросс-коммутация каналов MPLS, когда центральный маршрутизатор статически проключает пути LSP, приходящие от реер-маршрутизаторов.



Рисунок 7. Точка Интернет-доступа на базе MPLS

В отличие от коммутаторов на базе Ethernet или ATM, MPLS распространяет соединения пиринга через магистральную сеть, которая не зависит от среды передачи. Магистраль MPLS может опираться на Ethernet, Frame Relay, ATM или последовательные сегменты. MPLS используется только как общий транспортный уровень.

Эта возможность особенно важна сейчас, когда количество точек доступа Интернета растет по экспоненте, чаще всего путем физического дублирования сайтов. Организация прозрачной связи между сайтами на высоких скоростях становится проблемой, для решения которой требуется множество оптоволоконных каналов. Клиентам требуется максимальная гибкость с сохранением возможности при необходимости быстро устанавливать соединения пиринга.

MPLS поддерживает скорости OC-192c/STM-64 между сайтами, причем удаленный пиринг обеспечивается простым распространением путей LSP между сайтами с использованием ВЧС уровня 2 на основе MPLS. Точка доступа Интернет на базе MPLS может предлагаться как услуга связи между двумя сайтами или при аренде площадей, совместно используемых обоими сайтами.

Услуга удаленного пиринга может рассматриваться в национальном или международном масштабе, с использованием транзитного соединения для установления отношений пиринга с поставщиками услуг, находящимися в другом регионе или другой стране (рис. 8).

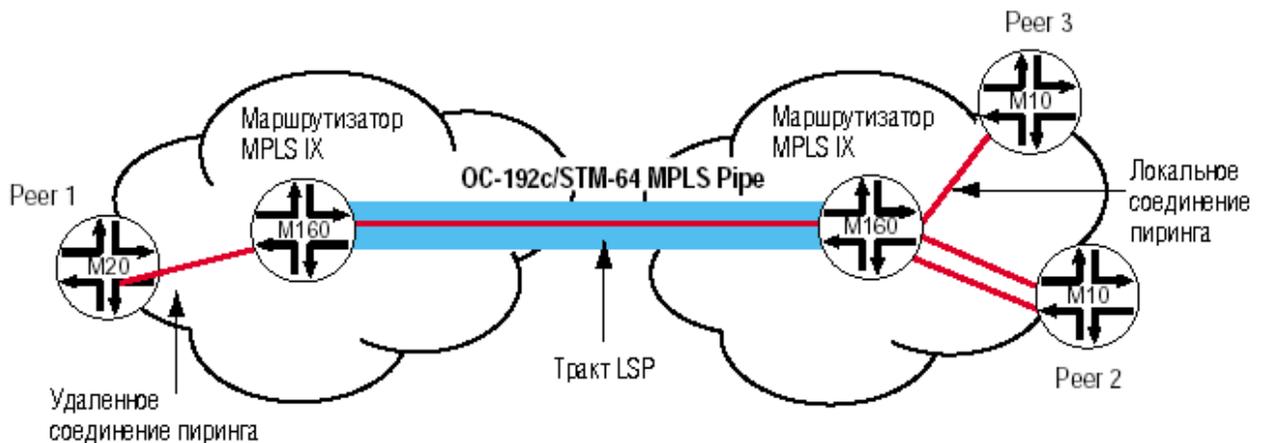


Рисунок 8. Пример локального и удаленного пиринга

Заключение

Виртуальные частные сети Juniper Networks уровня 2 на основе MPLS решают самые наболевшие проблемы современных ВЧС.

- Простота конфигурирования и обслуживания, увеличение рентабельности.
- Предоставление дополнительных услуг с предсказуемыми характеристиками.
- Конфиденциальная связь "каждый с каждым" для увеличения масштабируемости.
- Дифференциация трафика по каждому клиенту.
- Снижение стоимости эксплуатации за счет объединения трафик в одной IP инфраструктуре.

Кроме простоты и прозрачности ВЧС уровня 2 Juniper Networks делает возможным формирование ВЧС уровня 3 на основе MPLS, и за счет этого позволяет предоставлять клиентам услуги аутсорсинга маршрутизации, одноточечных соединений на границе, а также управление услугами со стороны провайдера.

Предлагая клиентам любой из перечисленных вариантов развертывания ВЧС, провайдер сохраняет существующую клиентскую базу, привлекает новых клиентов, обеспечивая их надежно и быстро формируемыми услугами, а также гибко использует новые направления бизнеса.

Copyright © 2002 Poplar systems

Poplar
SYSTEMS

<http://www.poplar.ru>