

Базовые сервисы технологии MPLS

Скайпу - дорогу!
© Минсвязи Р

Пока Связьинвест приватизируют, пока дополнения примут, пока действующие лицензии у операторов кончатся... Куда торопиться? Взятый диверсифицированным курсом отрасль и дотянут года эдак до 2008. А там уж как в поговорке - "или ишак сдохнет, или эмир...".

Что бы не было уж совсем скучно - маленькая ремарка о положении конкурентов, а именно провайдеров АДСЛ.

Наиболее принципиальный вопрос перспектив технологии АДСЛ, на мой взгляд - количество широкополосных линий связи, которые можно разместить в одном многопарнике. Понятно, что "100-200к" особых проблем не возникнет. Но чем выше по дереву частот, тем мрачнее становится прогноз...

Увы - точной статистики операторы DSL не предоставляют. Даже достоверных в статистическом плане слухов нет из-за сравнительной нераспространенности технологии (массовый проект в России вообще один - Стрим).

Поэтому посмотрим, что скажет ОСТ 45.81-97 "Каналообразующая аппаратура телеграфирования и аппаратура передачи данных высокого уровня". Понятия широкополосных сигналов в нем отсутствует. Однако, можно посмотреть нижнюю строчку таблицы 3, там где говорится про 72 кГц, и сопоставить это с таблицей 5, можно получить следующее:

Для кабелей с числом пар количество цепей передачи данных в абонентской линии:

Количество пар в кабеле	Количество цепей передачи данных в линии
100	3
200	6
300	9
400	12
500	15
600	18

Видно, что зависимость совершенно линейная - примерно 3 линии передачи данных на каждые 100 пар. Составители документа только тратили зря бумагу на таблицы.

Конечно, методы цифровой обработки и компенсации помех делают чудеса. По крайней мере, указанные нормы перекрываются на практике как минимум в разы. Но слишком красноречиво цифры показывают сложность передачи широкополоски по стандартной телефонной меди...

Базовые сервисы технологии MPLS.

MPLS ATM интеграция.

MPLS QoS.

MPLS Traffic Engineering (TE).

Traffic Engineering (TE).

Fast Re Route (FRR).

MPLS L3 VPN.

MPLS L2 VPN.

Point-to-Point VPN (AToM, EoMPLS).

Multi-Point VPN (VPLS).

GMPLS.

Заключение.

Основным преимуществом MPLS считается ускорение скорости продвижения пакетов (IP) в ядре сети. Однако существуют и другие, не менее важные, приложения для этой технологии.

MPLS ATM интеграция.

Прежде всего, MPLS предоставляет дополнительную возможность соединения IP и ATM-сетей.

Считается, что на сегодня это наилучший вариант консолидации сетевой инфраструктуры, содержащей ATM элементы. MPLS и ATM обычно рассматривают как дополняющие друг друга технологии. Возможность развернуть MPLS поверх ATM инфраструктуры практически дает вторую жизнь ATM.

MPLS QoS.

MPLS не определяет новую QoS архитектуру, а базируется на использовании широко известной и зарекомендовавшей себя на практике IP QoS парадигмы.

Для IP QoS определено две модели: IntServ и DiffServ.

IntServ определяет потоковый QoS и использует RSVP для сигнализации.

DiffServ использует маркировку пакетов на границе сети и дальнейшую обработку. Трафик разбивается на классы и в зависимости от этого обрабатывается механизмами ограничения, выравнивания и приоритизации.

MPLS QoS использует DiffServ подход, помещая необходимую маркировку в заголовке. Эквивалентом DSCP метки может являться трехбитовое Experimental поле в MPLS.

Кроме того, реализация TE в принципе может автоматически выполнять функции QoS.

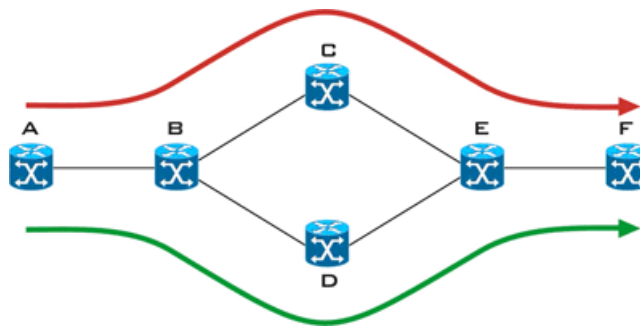
MPLS Traffic Engineering (TE).

Traffic Engineering (TE).

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

Обычные протоколы маршрутизации (IGP протоколы IS-IS, OSPF) предоставляют ограниченные возможности по управлению трафиком на основе метрик составляющих сеть линков.

Основной механизм TE в MPLS – использование однонаправленных туннелей (MPLS TE tunnel) для задания пути прохождения определенного трафика. Например, для одного вида трафика, например высокоприоритетного голосового можно проложить один путь через сеть, а для низкоприоритетного – другой. Так как туннели – однонаправленные, то обратный путь может быть совершенно другим.



Технологически MPLS TE основывается на формировании маршрутов прохождения пакетов (LSP) через сеть с помощью механизма создания туннелей (MPLS Tunnel), который в свою очередь базируется на стекировании меток (Labels Stack).

Примитивный MPLS TE можно обеспечить, вручную установив туннели, соответствующие требуемым направлениям прохождения трафика.

Однако полный комплекс мероприятий MPLS TE выглядит несколько сложнее и условно разбивается на следующие стадии (этапы).

1. Организация MPLS домена.

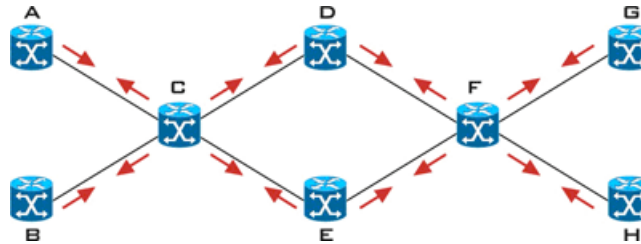
Имеется определенная сетевая топология, состоящая из набора маршрутизаторов и каналов с определенными свойствами между ними (полоса пропускания и прочее).

2. Наложение ограничений.

В MPLS домене включается механизм TE и описываются минимальные требования к сети: начальные и конечные точки прохождения трафика, графы путей между ними (не обязательно все) и методы вычисления маршрутов по ним (явный или динамический), требуемая полоса пропускания.

3. Изучение параметров сетевой среды.

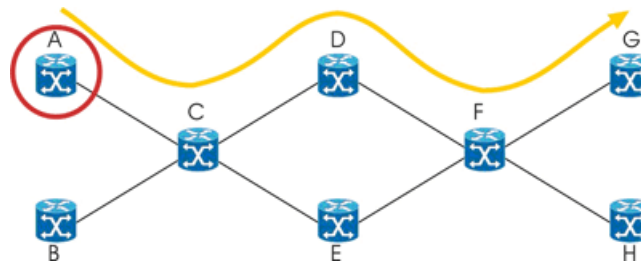
Для распространения информации о каналах (атрибутах линков) используется механизм расширения протоколов маршрутизации (Link State Protocols: IS-IS, OSPF).



В итоге каждый маршрутизатор получает расширенную топологическую информацию о сети, включающую пропускную способность каждого канала связи (линка). Получается база линков и их состояний (свойств) link state database.

4. Вычисление путей прохождения трафика в соответствии с административными требованиями и возможностями сети.

На граничных входных (по отношению к потоку трафика) маршрутизаторах выполняется специальный алгоритм Constrained Base Algorithm, учитывающий политику выбора лучшего пути для LSP туннеля (то есть набор роутеров, через которые передавать трафик): как возможности каналов, так и административные требования (границы MPLS домена, полоса пропускания). Алгоритм перебирает линки (их свойства) и в итоге по меркам вычисляет маршруты (пути) прохождения трафика с учетом накладываемых ограничений. То есть в итоге на входном маршрутизаторе (head-end) конструируются требуемые LSP до выходного маршрутизатора (head-tail) в соответствии с наложенными требованиями на прохождение трафика между ними.



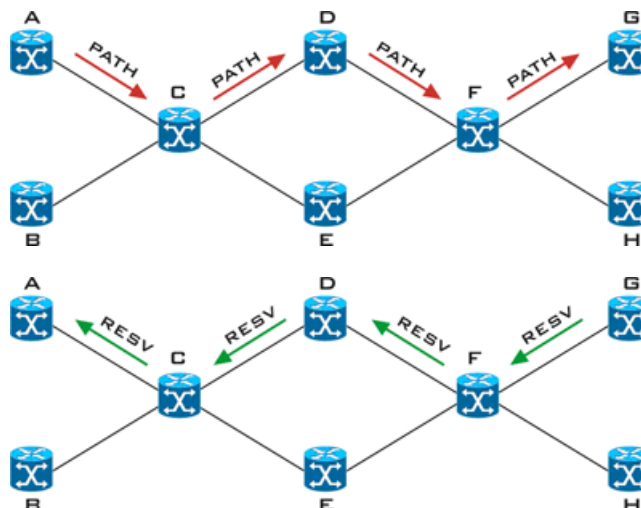
5. Установление путей.

Просчитанные пути устанавливаются в сети с помощью специального протокола сигнализации, который умеет распространять информацию о явном (explicit) маршруте.

Сегодня известно два таких протокола: RSVP-ext и CR-LDP.

MPLS поддерживает два вида явных путей: строгий (strict) с определением всех промежуточных узлов и свободный (loose), когда задается только их часть.

С помощью RSVP ext устанавливается LSP (TE Tunnel) вдоль вычисленного пути. Это автоматическая установка. RSVP использует PATH и RESV сообщения для проброса LSP вдоль рассчитанного пути. При этом согласуются еще и параметры полосы пропускания (Admission Control).

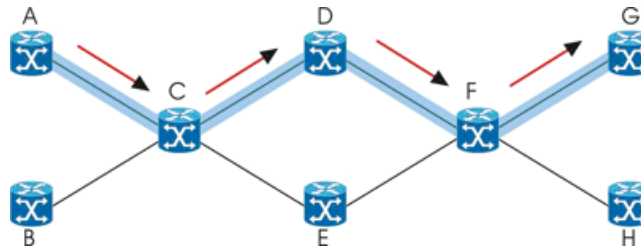


6. Установка маршрутов с учетом туннелей TE.

IGP устанавливает маршрут с учетом наличия туннелей (как tunnel интерфейсы). В итоге процесс маршрутизации на входном маршрутизаторе (head-end) просто оперирует LSP туннелями как интерфейсами. А в таблице маршрутов head-end будет маршрут к head-tail с next-hop – TE tunnel.

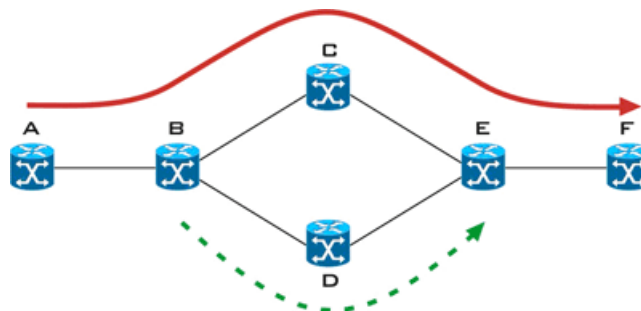
7. Продвижение пакетов.

С помощью механизма MPLS (Label Stacking) происходит обеспечение необходимого туннелирования и продвижение пакетов.



Fast Re Route (FRR).

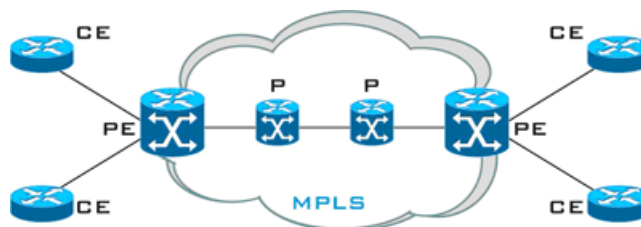
Технология Fast ReRoute (FRR) позволяет временно направить трафик по запасному каналу в обход отказавшего линка на участке пути LSP до тех пор, пока head-end сможет изменить весь LSP. Время восстановления порядка 50 ms. Предварительно конфигурируется запасной туннель (backup tunnel). Контролируется маршрутизаторами на концах отказавшего линка. Используется стекирование меток в случае обхода проблемного участка.



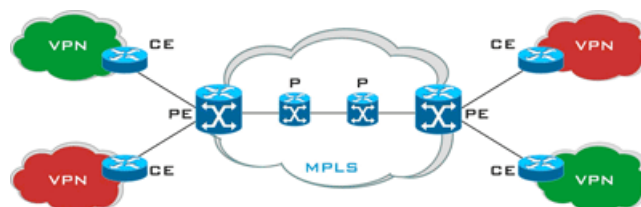
MPLS L3 VPN.

MPLS позволяет создавать виртуальные частные сети Layer 3, не прибегая к туннелированию (GRE) и шифрованию (IPsec).

MPLS VPN сеть делится на две области: IP сети клиентов и магистраль провайдера. Классическая конструкция MPLS L3 VPN состоит из следующих компонентов: граничные маршрутизаторы провайдера PE, обращенные к клиентскому оборудованию CE, соединены между собой P маршрутизаторами в MPLS домене. В принципе, P маршрутизаторов может и не быть, необходимо чтобы обеспечивалась связность между PE.



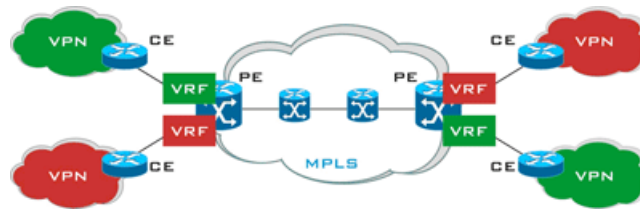
MPLS L3 VPN инфраструктура предполагает обеспечение изоляции распределенных клиентских IP сетей в рамках VPN. То есть обеспечивается только обмен пакетами между IP сетями одной VPN.



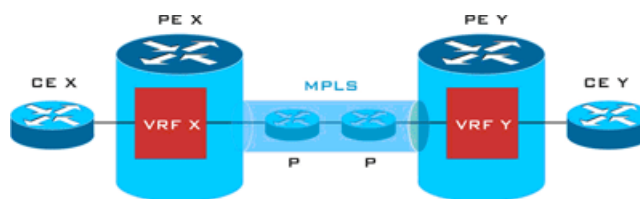
В терминах MPLS VPN отдельное CE подключение называется сайтом. Каждый сайт представляет

собой отдельную клиентскую подсеть, входящую в ту или иную VPN структуру.

Каждая VPN логически связана с одним или более комплексов маршрутизации и пересылки (VPN Routing and Forwarding instance – VRF). VRF определяет членство в VPN подсети за узлом CE, подключенного к PE. Интерфейсы PE маршрутизаторов, обращенные к CE, логически связаны с индивидуальными VRF.



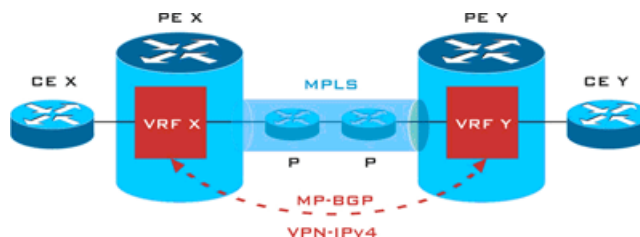
Экземпляр VRF состоит из таблицы маршрутизации (IPv4), получаемой из нее CEF, набора интерфейсов, использующих VRF и других данных. VRF таблицы IP маршрутизации используются для обмена информацией о маршрутах только внутри VPN сети и не выходят за границу VPN, то есть извне невозможно послать пакет на маршрутизатор, находящийся внутри VPN (этот маршрут попросту неизвестен). В итоге VRF представляет собой «виртуальный маршрутизатор» внутри PE.



В рамках MPLS L3 VPN в VPN включаются IPv4 клиентские подсети. В пределах одной VPN не допускаются пересекающиеся IPv4 адреса. Однако в разных VPN это допустимо. Отсюда потенциальная неоднозначность для PE маршрутизатора: разные VRF могут содержать одинаковые IPv4 адреса. Для получения уникальных адресов (и соответственно маршрутов), называемых VPN-IPv4, используется идентификатор VPN- Route Distinguisher (RD). VPN-IPv4 получается добавлением к IPv4 идентификатора RD. В итоге PE оперирует уникальными VPN-IPv4.

Для обмена маршрутной информацией между VRF разных PE используется MP-BGP протокол. MP-BGP оперирует VPN-IPv4 маршрутами.

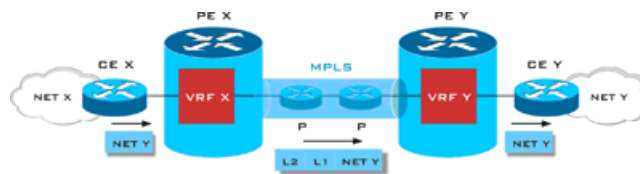
Таким образом, с помощью MP-BGP получается виртуальная связь между PE (между VRF одинаковых VPN). Для выполнения политики экспорта/импорта дополнительно вводится понятие адресата маршрута - Route Target (RT).



В итоге получается следующая схема. Каждый клиентский сайт (интерфейс на PE) имеет свою VRF (таблицу IPv4 маршрутизации). PE может узнать IP префикс клиента разными способами (статическая конфигурация, BGP, RIP, OSPF, IS-IS). PE помещает IPv4 маршрут клиента в VRF данного сайта. Кроме того, с помощью заранее выбранного идентификатора VPNов, в которые входит данный сайт, IPv4 маршруты (префиксы) преобразуются в VPN-IPv4 маршруты и помещаются в MP-BGP. MP-BGP согласно политике импорта/экспорта связывает между собой все PE маршрутизаторы (их VRF). В итоге в VRFы разных PE, но принадлежащих одной VPN, попадают все маршруты из данной VPN. Причем в записях VRF Next Хорами являются PE, как будто они связаны между собой (виртуально посредством MPLS).

Реальная передача пакетов (коммутация) происходит при помощи MPLS. MPLS метки используются следующим образом: пакет содержит два уровня меток (используется стек). Первая метка направляет пакет к требуемому PE (next hop), а вторая указывает комплекс VRF, логически связанный с выходным интерфейсом CE маршрутизатора пункта назначения.

Рассмотрим на примере прохождение пакетов в MPLS L3 VPN.



Предположим, CEX посылает пакет для CEY. От CEX к PEX приходит пакет с DST=NETY (сеть за CEY) и без меток. Данный пакет приходит с определенного интерфейса и поэтому обрабатывается конкретной VRFx. В VRFx есть маршрут к NETY с NEXT-HOP – PEY и метка VPN (метка L1 для попадания в необходимую VRFy на PEY). Метку для достижения PEY PEX ищет в своей глобальной таблице маршрутизации. Таким образом, PEX отправляет в сторону PEY пакет со стеком меток: L2 для достижения PEY как NEXT-HOP и L1 для достижения нужной VPN (VRFy) на PEY. По метке L2 пакет доходит до PEY и она там удаляется. PEY по метке L1 выясняет какой VRF пользоваться для достижения NETY. В VRFy для NETY указан соответствующий интерфейс PEY-CEY. В сторону CEY пакет уходит без меток в виде IPv4.

MPLS L2 VPN.

Современные реалии таковы, что конечный потребитель телекоммуникационных услуг начинает мыслить абстрактно и потребности свои выражает в категориях Metro (Ethernet) а не WAN (IP). Поэтому наиболее актуальной становится задача построения VPN Layer 2. Используя MPLS, данную задачу можно решить несколькими способами. Рассмотрим некоторые из них.

Point-to-Point VPN (AToM, EoMPLS).

Для создания VPN Layer 2 по схеме точка-точка (point-to-point) разработана технология Any Transport Over MPLS (AToM), обеспечивающая передачу Layer 2 фреймов через MPLS сеть. AToM – это интегральная технология, включающая Frame Relay over MPLS, ATM over MPLS, Ethernet over MPLS.

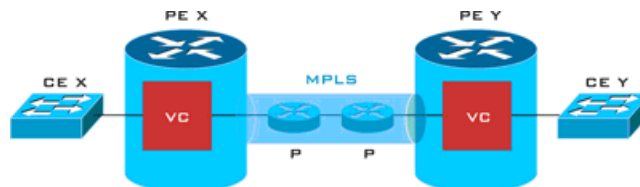
Для потребителя сеть провайдера услуг в рамках сервиса AToM выглядит как виртуальный патчкорд.



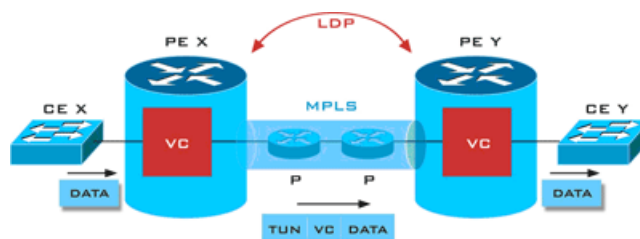
AToM использует непосредственные LDP сессии между граничными маршрутизаторами провайдерской сети (PE) для установления и поддержки соединений. Непосредственное продвижение пакетов происходит с использованием стекирования меток MPLS, когда одна метка (Top) соединяет граничные маршрутизаторы, а вторая (Bottom) – определяет непосредственно VPN клиента (интерфейс на PE маршрутизаторе).

Так как наиболее востребованной в настоящее время является технология Ethernet over MPLS (EoMPLS), то детали функционирования AToM рассмотрим на ее примере.

EoMPLS инкапсулирует Ethernet фреймы в MPLS пакеты и использует стек меток для продвижения через MPLS сеть. На каждом PE-CLE (Customer Leading Edge) организуется Virtual Circuit (VC). Обязательно устанавливаются прямые LDP сессии между входным и выходным PE-CLE для обмена информацией о VC. Каждая VC состоит из двух однонаправленных LSP.



Непосредственно передача пакетов использует стек меток Верхняя метка (Top Label), называемая еще Tunnel Label, используется для достижения выходного (Egress) PE-CLE. Нижняя метка (Bottom Label), называемая VC Label, используется для определения интерфейса на PE-CLE. VC Label обеспечивается Egress PE-CLE для Ingress PE-CLE для направления трафика в нужный интерфейс на Egress PE-CLE. VC Label отождествляется с VC ID и устанавливается на этапе VC setup.

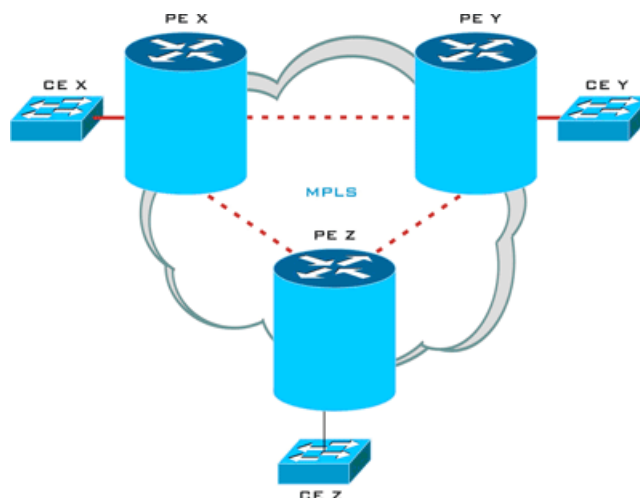


Multi-Point VPN (VPLS).

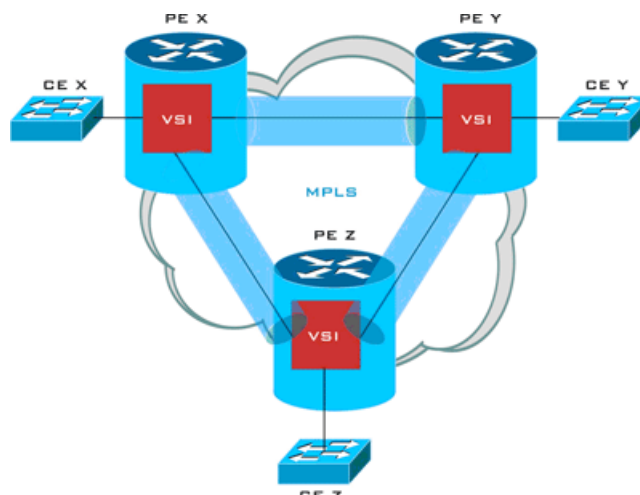
С целью преодоления ограничений point-to-point VPN разработана технология Virtual Private LAN Service (VPLS). VPLS – Layer 2 VPN технология, обеспечивающая многоточечные соединения (Multipoint Services) поверх пакетной сетевой инфраструктуры. VPLS дают возможность объединения распределенных локальных сетей в единую сеть.

Для потребителя сеть провайдера услуг выглядит как виртуальный Ethernet свич. При этом сеть оператора связи абсолютно прозрачна и не видна для сети заказчика.

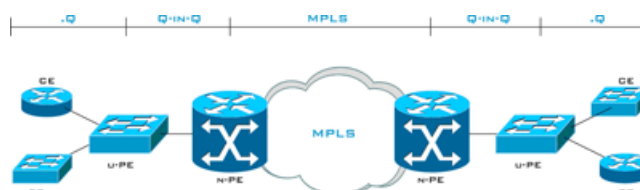
Логическая структура VPLS выглядит следующим образом.



Для каждого VPN на каждом PE выполняется Virtual Switching Instance (VSI), которая обеспечивает forwarding decision для каждой VPLS. Ethernet фреймы коммутируются между PE устройствами, используя VSI. В принципе VPLS расширяет модель АТом до многоточечных соединений, используя те же методы инкапсуляции.



Дальнейшим развитием масштабирования данной технологии является Hierarchical VPLS (H-VPLS). H-VPLS подразумевает декомпозицию PE устройства на два User-Facing PE (u-PE) и Network PE (n-PE).



Отличие VPLS от AToM в том, что AToM – p-t-p L2 сервис, а VPLS – multipoint.

В тоже время MPLS L3 VPN тоже multipoint, но ограничен IP трафиком. VPLS же L2 сервис и может поддерживать несколько высокоуровневых протоколов.

GMPLS.

В настоящее время, наряду со стандартной коммутацией, в качестве протокола маршрутизации и сигнализации предлагается использование протокола Generalized MPLS (GMPLS). На оптическом уровне данный протокол дает возможность маршрутизировать и передавать потоки данных, основываясь только на длине волны несущего светового сигнала. На сегодня это высшая степень интеграции пакетной технологии и оптической транспортной среды.

Заключение.

Краткое обобщающее содержание выше изложенного.

Упрощенно MPLS можно представить как добавление меток в пакеты и их дальнейшее использование при скоростной коммутации.

MPLS может использовать унаследованную ATM инфраструктуру, что позволяет проводить плавную модернизацию устаревшего оборудования.

MPLS QoS использует DiffServ модель и принципиально ничем от нее не отличается.

MPLS Traffic Engineering является возможностью гибкого и в том числе автоматического управления направлением прохождения трафика с учетом административных требований и реальных параметров сети.

MPLS Layer 3 VPN – технология объединения IP подсетей клиентов с полной изоляцией их друг от друга.

MPLS Layer 2 VPN позволяет объединять клиентские подсети на втором уровне. Может представлять собой виртуальный пачкорд (Point-to-point, AToM) или виртуальный свич (Multipoint, VPLS).

Общие выводы.

В настоящее время MPLS знаменует собой победу IP как универсального транспорта для всех видов приложений.

MPLS является ведущей технологией способной стать фундаментом для инфраструктуры мультисервисных сетей следующего поколения NGN, в рамках которых станет возможна передача любого трафика через единую телекоммуникационную инфраструктуру.

Частные выводы.

Несмотря на то, что при подготовке заметки использовались разноплановые материалы, несомненно сильное влияние оказала информация, предоставляемая фирмой cisco. Так что хотелось широты охвата, а получилось как всегда. Поэтому очень надеемся на вашу конструктивную критику и ждем замечаний и предложений.

Ссылки.

<http://www.cisco.com>

<http://www.rfc-editor.org/rfc/rfc2547.txt>

<http://www.rfc-editor.org/rfc/rfc2702.txt>

<http://www.rfc-editor.org/rfc/rfc2917.txt>

<http://www.rfc-editor.org/rfc/rfc3031.txt>

<http://www.rfc-editor.org/rfc/rfc3032.txt>

<http://www.rfc-editor.org/rfc/rfc3034.txt>

<http://www.rfc-editor.org/rfc/rfc3035.txt>

<http://www.rfc-editor.org/rfc/rfc3036.txt>

<http://www.rfc-editor.org/rfc/rfc3037.txt>

<http://www.cisco.com/en/..pr..29b.html>

<http://www.cisco.com/en/..pr..77b.html>

<http://www.ietf.org/internet-drafts/dr..16.txt>

<http://www.ietf.org/internet-drafts/dr..09.txt>

Анонс

- Четвертая часть, Основы технологии MPLS, и ее практическое применение (Edward Afontsev).
- Переделка ужастика;
- Антенна во льду;
- ТРК Одинцово - фотогалерея;
- Головная станция ТРК Одинцово;
- Грозозащиты и пинговалки, надеюсь на письма;
- Зарисовки узлов разных провайдеров. Вечная тема (много фотографий гарантировано);
- Традиционный пункт - ссылки на интересные места Сети. Присылайте письма - они очень нужны для обзоров. Обязательно сообщайте, нужна ли Ваша подпись, ссылка, или лучше обойтись без нее;
- В "ужастиках" - витая пара на балкон...