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

Кафедра СК и РИ

ДИПЛОМНАЯ РАБОТА

«Анализ применения туннельного эффекта технологии MPLS для построения каналов VPN»

Студентка
5 курс, гр. СК-92 **Л.В. Бородина**

Руководитель **А.Б. Гольдштейн**

Санкт-Петербург
2004

Введение. 3
Глава 1. Пути развития конвергентных сетей связи. 4
1.1. Современные подходы к организации сетей NGN. 4
1.1.1. Управление трафиком в мультисервисной сети. 8
1.2. Проблемы передачи разнотипного трафика. 9
1.2.1. Варианты обеспечения QoS. 12
1.3. Виртуальные частные сети VPN. 16
1.4. Введение в MPLS. 18
1.5. Актуальность темы дипломной работы. 20
Глава 2. Технология MPLS. 21
2.1.Общие принципы. 21
2.2. Основные понятия. 22
2.2.1. Метки. 22
2.2.2. Класс эквивалентности пересылки FEC. 26
2.2.3. Коммутируемый по меткам тракт LSP. 28
2.3. Принцип работы. 29
2.3.1.Замена меток. 33
2.4.Распределение меток. 35
2.4.1. Выбор маршрута. 36
2.5. Протокол рассылки меток. 38
2.6. Traffic Engineering. 40
2.6.1.Атрибуты TE-туннеля. 44
2.6.2. Поддержка TE-пути. 48
2.6.3.Протокол RSVP-TE. 50
2.7. Выводы. 56
Глава 3. Туннельный эффект для VPN. 59
3.1. Основы VPN. 59
3.2. Функции VPN по защите данных. 62
3.3. Технологии создания виртуальных частных сетей. 64
3.4. Применение туннелей для VPN. 71
3.5. Сравнительный анализ туннелей MPLS и обычных туннелей. 72
Глава 4. Функциональная модель фрагмента VPN на основе туннелей MPLS. 75
4.1. Базовый вариант создания VPN на основе туннелей MPLS. 75
4.1.1. Обмен маршрутной информацией. 76
4.1.2. Установление LSP-туннеля. 78
4.1.3. Поток данных. 79
4.2. Сценарий обмена сообщениями для установления TE-туннеля для VPN и передачи по нему трафика данных. 80
Заключение. 89
Литература. 90

Введение.

Возрастающий спрос клиентов на организацию виртуальных частных сетей повлек за собой появление различных технологий, предлагающих данный вид сервиса. В связи с протеканием процесса конвергенции эти решения должны соответствовать уровню требований, предъявляемых конвергентными сетями. Это должны быть надежные, безопасные частные сети, отвечающие требованиям по качеству обслуживания при передаче разнотипного трафика.

Существует несколько моделей качества обслуживания. Среди них хотелось бы выделить технологию многопротокольной коммутации по меткам MPLS. Эта технология обладает большой гибкостью в предоставлении новых услуг, масштабируемостью и рядом других достоинств. Совместно с протоколом RSVP-TE MPLS гарантирует предоставление необходимого уровня качества обслуживания каждому потоку, передаваемому по сети провайдера.

Построение виртуальных частных сетей на базе технологии MPLS обладает рядом существенных преимуществ по сравнению с иными подходами к данному вопросу, что позволяет назвать ее ведущей технологией организации сетей VPN.

Глава 1. Пути развития конвергентных сетей связи.

1.1. Современные подходы к организации сетей NGN.

До последнего времени сети передачи данных, голоса и видео строились независимо друг от друга, базировались на разных технологиях и инфраструктурах. Развитие IP-телефонии, мобильных сетей связи, продвижение на рынок услуг, для реализации которых требуются различные значения параметров качества обслуживания, - все это привело к необходимости создания новых технологий доступа, вследствие чего мы можем наблюдать протекание процесса конвергенции.

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. И хотя сегодня между отдельными видами коммутации видится больше различий, нежели сходства, уже завтра ситуация изменится.

Альтернативным вариантом построения отдельных сетей связи является создание единой мультисервисной сети общего пользования NGN, по которой предполагается передача трафика различного типа. Такое решение позволит отказаться от дублирующих друг друга сетей, а в перспективе позволит внедрять новые услуги, обеспечивая выполнение их специфических требований к скорости и качеству передачи.

Что же такое мультисервисная сеть?

Под мультисервисной сетью понимают телекоммуникационную структуру, позволяющую оказывать пользователям разнообразные услуги связи, различающиеся как по качественным, так и по количественным характеристикам. Вполне вероятно, мультисервисная сеть объединит в себе обычную телефонную сеть, сотовую связь, Интернет, IP-телефонию, кабельное телевидение, услуги

интеллектуальных сетей, доступ к информационным ресурсам, получение аудио- и видеопрограмм и многое другое. Неудивительно, что построение мультисервисных сетей привлекает к себе все большее внимание.

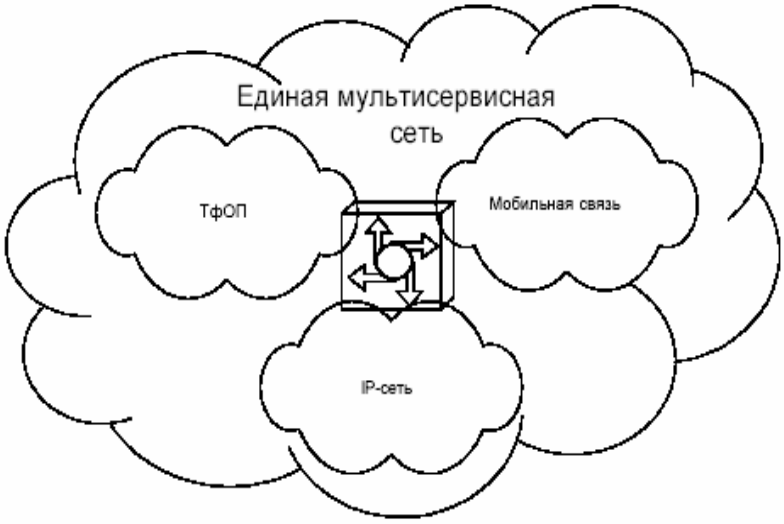


Рис. 1. Мультисервисная сеть связи.

Все преимущества, которые дает мультисервисная сеть можно подразделить на возможности для пользователя и возможности для оператора.

С точки зрения пользователя мультисервисная сеть дает такие преимущества:

- получить набор услуг электросвязи с помощью одного терминала, включенного в одну сеть.
- иметь единый договор с оператором на весь комплекс услуг электросвязи и, как следствие, экономию средств по сравнению с использованием нескольких разнородных служб электросвязи.

Оператору электросвязи сеть NGN позволит:

- упростить построение сети, благодаря чему исчезнет необходимость иметь несколько разных сетей для разных служб.

- повысить эффективность использования дорогостоящих средств и сооружений, что позволит снизить тарифы при сохранении рентабельности сети.
- расширить набор услуг, которые могут быть предоставлены пользователю
- повысит гибкость сети при внедрении новых услуг и служб.
- повысить конкурентоспособность сети и привлекательность ее для пользователей.

Основная задача сетей следующего поколения – передача любого типа информации от любого пользователя к любому другому пользователю, независимо от того, где пользователи расположены; при этом каждый тип информации предъявляет свои требования к полосе пропускания, времени доставки, допустимому уровню потерь и степени защищенности.

В последнее время наиболее стремительно растет трафик передачи данных. В связи с этим, процесс конвергенции рассматривается на базе средств пакетной передачи данных, а именно: на базе протокола IP.

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.

Из всех обозначенных направлений приоритетным на сегодняшний день считается направление по созданию единой транспортной инфраструктуры.

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.

1.1.1. Управление трафиком в мультисервисной сети.

При любом числе пользователей сети NGN требуется решение задач по управлению трафиком.

По своему замыслу данная сеть предполагает одновременное существование множества разнотипных потоков. Каждый из таких потоков требует безусловного соблюдения одних параметров передачи, и допускает некоторые уступки по другим. Поэтому, в периоды возникновения перегрузок сеть может для одного потока урезать полосу пропускания, для другого увеличить время доставки, а для третьего, например, пренебречь целостностью передаваемых данных.

Мультисервисная сеть должна обладать более сложной системой управления по сравнению с системами управления традиционными сетями. Она должна обеспечивать одновременное предоставление множества разнообразных сетевых услуг и передачу по сети разнотипного трафика.

Для эффективного управления трафиком необходимо располагать соответствующими аппаратными и программными средствами, позволяющими быстро и гибко предоставлять пользователю любую услугу.

В отношении процесса создания мультисервисной сети, то следует сказать что, пока, к сожалению, технологии, которая удовлетворяла бы запросам перспективной сети NGN, еще нет. Правда, уже существуют технологические решения, способные стать основой сетей NGN.

1.2. Проблемы передачи разнотипного трафика.

Мультисервисная сеть следующего поколения NGN предполагает одновременную передачу разнотипного трафика при гарантированном уровне качества обслуживания. При построении мультисервисных сетей не стоит забывать о том, что информационные потоки разных приложений требуют разных уровней обслуживания или типов качества. Задача обеспечения требуемого качества обслуживания значится одной из первоочередных в процессе проведения работ по созданию конвергентных сетей.

Как известно, сети IP не осуществляют какого-либо разделения потоков различных приложений при их транспортировке, как и не дают гарантий по их доставке.

Понятие качества обслуживания в IP-телефонии претерпело некоторые изменения. Дать определение понятию QoS можно следующим образом: качество обслуживания – это набор требований, предъявляемых к ресурсам сети при передаче потока данных. Качество обслуживания представляет собой набор технологий, которые позволяют приложениям запрашивать и получать необходимый уровень услуг с точки зрения пропускной способности, джиттера, а также общей задержки доставки данных. Для каждого конкретного случая качество обслуживания конкретизируется и определяется соответствующими параметрами.

На качество обслуживания в IP-сетях влияют четыре основных фактора:

- Задержка – время, которое требуется пакету для его передачи из одного пункта в другой.

Величина задержки может зависеть от доступной полосы пропускания, загрузки ресурсов сетевых устройств, расстояния между узлами. Полная временная задержка речевого трафика делится на две основные части: задержки на кодирование и декодирование в шлюзах, и задержки, вносимые сетью (в маршрутизаторах, линиях связи). Уменьшить величину задержки можно двумя способами: во-первых, за счет проектирования инфраструктуры сети таким образом, чтобы задержка в ней была минимальной: можно сократить число транзитных маршрутизаторов и соединить их между собой высокоскоростными линиями связи; а, во-вторых, за счет уменьшения времени обработки информационного трафика в шлюзе и/или на транспортном узле.

- Джиттер – вариация задержки.

Вариация задержки находится в прямой зависимости от загруженности каналов. Уменьшить величину джиттера возможно либо назначив высокий приоритет трафику, либо увеличив размер буфера.

- сброс пакетов.

Потеря пакетов происходит при перегрузке сетей или устройств и приводит к выпадению кусков информации в потоковых передачах, к разрыву соединений и т.п. Методы QoS позволяют ограничить полосу пропускания, которую могут использовать те или иные протоколы или соединения, таким образом, предотвращая или ограничивая перегрузку.

- контроль над использованием полосы пропускания.

Возможность контролировать трафик имеет большое значение, особенно в тех случаях, когда число сетевых ресурсов ограничено. Механизмы QoS позволяют присваивать более высокий приоритет

трафику критически важных приложений, оставляя для менее важных приложений оставшиеся канальные ресурсы.

При передаче сообщения по сети пакеты этого сообщения передаются независимо друг от друга, что в свою очередь может привести к значительному изменению задержки пакетов, вариации задержки, а это может оказать влияние на изменение параметров качества обслуживания.

Каждому типу трафика требуется свой, определенный уровень качества обслуживания. Например, при передаче голосового трафика в первую очередь необходима гарантия того, что пакеты будут доставлены пользователю и при этом значение задержки и вариации задержки не превысят максимально допустимое значение.

Большинство устройств, поддерживающих алгоритмы QoS, позволяют указать минимальную и максимальную полосы пропускания для конкретного протокола, а также минимальную и максимальную полосы пропускания для каждого сеанса связи. Кроме того, QoS позволяет назначить более высокий приоритет обслуживания для приложений отдельных пользователей.

Трафик всех приложений можно классифицировать по трем характеристикам:

- Относительная предсказуемость скорости передачи данных
- Чувствительность к задержкам
- Чувствительность к потерям и искажениям

Этим критериям сопоставляют три группы параметров, которые используются для определения и задания параметров требуемого качества обслуживания:

- во-первых, это параметры пропускной способности. К таким параметрам относятся средняя, максимальная (пиковая) и минимальная скорость передачи данных.

- во-вторых, параметры задержек, а именно: средняя и максимальная величина задержки, и среднее и максимальное значения вариации задержки.
- параметры надежности передачи, для определения которых используется процент потерянных пакетов и процент искаженных пакетов.

1.2.1. Варианты обеспечения QoS.

Для решения проблем обеспечения качества в IP сетях предлагаются различные способы решения.

Best Effort.

Данный вид обслуживания предусматривает обслуживание пакетов, передаваемых по сети, наилучшим образом из всех возможных с учетом наличия свободных ресурсов, что вызывает сетевые перегрузки и несправедливое распределение ресурсов сети. Как следствие, качество предоставляемых услуг непредсказуемо и зависит от загрузки сети.

***Интегрированное обслуживание* IntServ.**

Модель интегрированного обслуживания позволяет обеспечивать сквозное качество обслуживания, гарантируя необходимый уровень полосы пропускания, при условии, что все маршрутизаторы в сети поддерживают и реально учитывают механизмы IntServ.

В данной модели существует два класса обслуживания для трафика реального времени: гарантированного обслуживания и контролируемой загрузки сети. Первый класс гарантирует выделение заданной полосы пропускания и отсутствие дополнительной задержки из-за очередей пакетов.

Пакеты, отнесенные ко второму классу, передаются как традиционный IP-трафик, идущий по малозагруженной сети. Уровень обслуживания такого трафика остается неизменным при увеличении нагрузки в сети.

Трафик, не принадлежащий одному из данных классов IntServ, обрабатывается на основе оставшихся ресурсов.

Сигнальный протокол RSVP.

Протокол RSVP используется в качестве сигнального протокола в модели обслуживания IntServ.

Протокол резервирования ресурсов представляет собой механизм, с помощью которого приложения информируют сеть о своих требованиях, предъявляемых различными приложениями для пересылки информационного трафика с требуемым качеством. Таким образом, сеть может резервировать внутри себя ресурсы для того, чтобы обеспечить выполнение предъявляемых требований или отказать приложению.

Резервирование производится благодаря передаче сообщения Path, в котором указываются желательные характеристики качества обслуживания трафика, и сообщения Resv – запроса резервирования ресурсов. Значение QoS задается в спецификации flowspec сообщение протокола RSVP.

Следует отметить, что RSVP позволяет резервировать определенное значение полосы пропускания для существующего соединения, а не произвольное.

Инициатором резервирования всегда является получатель данных.

Протокол RSVP является односторонним. Стоит отметить и его способность автоматически адаптироваться к изменениям маршрутов и числу членов в группе.

Резервирование сетевых ресурсов протоколом RSVP выполняется только в случае выполнения двух условий: если маршрутизатор имеет необходимые для резервирования ресурсы и если запрос правомерен. Проверка выполнения этих условий проводится в каждом узле на пути следования запроса.

После резервирования инициатор начинает передачу информационного потока, и этот поток, на всем пути следования, обслуживается с заданным качеством. Резервирование производится как для уникастпротоколов, так и для мультикаст. Кроме того, резервирование в каждом маршрутизаторе на пути следования пакетов производится локально, т.е. независимо. По этой причине здесь не может идти речь о минимизации задержки, обеспечении надежности или безопасности, хотя в перспективе это может стать возможным.

Отмена резервирования реализуется либо по инициативе одного из пользователей, либо при срабатывании таймера, ограничивающего продолжительность резервирования ресурсов сети. При разрушении соединения ликвидируется и соответствующее резервирование.

Модель дифференцированного качества обслуживания DiffServ.

Дифференцированные сервисы не используют резервирования ресурсов в маршрутизаторах, и поэтому не дают каких-либо гарантий на предоставляемое качество обслуживания. В соответствии с этой моделью, поле, в котором переносится значение уровня качества обслуживания, получило название DS-байта. Шесть бит в этом поле используются для определения уровня качества обслуживания, а оставшиеся два находятся в резерве.

К настоящему времени определены два класса трафика модели дифференцированного обслуживания:

- срочная доставка
- гарантированная доставка

Протокол DiffServ подразумевает существование соглашения о качестве обслуживания SLA между провайдером и клиентом. По этому соглашению определяются критерии политики, и определяется тип трафика. Шесть бит, отводимых для кодирования уровня QoS, определяют, что в сети может существовать не более 32 потоков с

разным уровнем предоставляемого качества, что вместе с распределением трафика абонентов по очередям позволяет снизить требования к производительности. Модель классифицирует потоки в соответствии с определенными правилами, после чего однотипные потоки объединяются. Подобный механизм делает DiffServ более масштабируемым моделью по сравнению с IntServ. И хотя модель не дает стопроцентной гарантии на качество обслуживания, она и не требует организации предварительного соединения и резервирования ресурсов.

Поддержка QoS реализована в таких технологиях как ATM, FR и др., но в крупных сетях эти технологии не решают проблему обеспечения требуемого уровня QoS.

Технология MPLS с помощью определенных механизмов, о которых речь пойдет во второй главе, позволяет обеспечить необходимый уровень качества обслуживания информационного трафика.

Применение механизмов моделирования трафика в MPLS дает возможность расширить функции управления потоками передаваемых данных. К тому же, ее применение сводит к минимуму задержки в сети и величину джиттера.

Использование MPLS позволяет повысить производительность маршрутизаторов и пропускную способность сети в целом.

Технология совмещает в себе преимущества большинства предшествующих ей механизмов обеспечения QoS и интегрирует в себе некоторые, уже зарекомендовавшие себя технологии, например, RSVP. Кроме того, механизмы MPLS позволяют эффективно использовать ее с другими технологиями канального уровня.

Все это свидетельствует о том, что технология MPLS будет востребована при создании конвергентных сетей.

1.3. Виртуальные частные сети VPN.

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. Кроме того, существуют проблемы защиты информации, аутентификации и авторизации пользователей, предоставления доступа к ресурсам, обеспечение независимости адресных пространств.

Изначально, эти задачи решались путем организации собственной частной сети, что подразумевало прокладку выделенных каналов связи, установку маршрутизаторов и устройств доступа.

Преимущества частных сетей неоспоримы, это и независимость адресного пространства, и независимый выбор сетевой технологии, и высокий уровень безопасности. Но также неоспорим и тот факт, что с экономической точки зрения такую сеть может себе позволить далеко не каждое предприятие.

Что же такое VPN?

Под термином VPN понимают круг технологий, обеспечивающих безопасную и качественную связь в пределах контролируемой группы пользователей по открытой глобальной сети. Цель создания VPN сводится к максимальной степени обособления потоков данных одного предприятия от потоков данных всех других пользователей сети. Такое разделение должно быть обеспечено в отношении параметров пропускной способности потоков, а также, в отношении конфиденциальности передаваемых данных.

Проведенный анализ существующего спроса на предложения в области безопасности компьютерных сетей показал, что технологии построения виртуальных частных сетей VPN являются остро

востребованными и привлекают к себе все большее внимание специалистов.

Расширение глобальной сети Интернет, широкое распространение IP-приложений – все это позволяет сервис-провайдерам внедрять целый ряд новых услуг. В дальнейшем, сети VPN, возможно, станут основой для поддержки услуг, предлагаемых сетями нового поколения NGN.

На сегодняшний день, наряду с изменением типа передаваемого по общественным сетям трафика, меняется и тип информационных потоков, транспортируемых по каналам связи корпоративных сетей. В пределах сети предприятия передается трафик данных, потоки речевой информации, все большую популярность набирает передача видео, например, видеоконференция, передача данных видеонаблюдения и т.д. Для того, чтобы провайдер мог гарантировать определенное качество услуг QoS и обеспечивал безопасность трафика, ему необходимы средства, способные разделять между собой трафик различных приложений. Таким образом, сеть VPN должна уметь распознавать, к какому типу приложений относится трафик (голос, видеопотоки, электронная почта), а также уметь достаточно быстро отделять трафик одного приложения от трафика другого.

Как правило, виртуальные частные сети организуются на базе протокола IP, как наиболее распространенного, используемого для передачи разнородного трафика, в том числе и мультимедийного, критичного к задержкам. Но на базе этого маршрутизируемого протокола не всегда удаётся удовлетворить требование к задержке трафика и качеству обслуживания, т.к. маршрутизация пакетов осуществляется на более высоком – сетевом уровне, что требует больших затрат времени на обработку заголовков пакетов и процесс инкапсуляции/ деинкапсуляции, а функции QoS вообще не поддерживаются в явном виде. Решить эти проблемы позволит

применение протокола MPLS, который осуществляет быструю коммутацию пакетов, не прибегая к услугам сетевого уровня, и обеспечивает поддержку услуги QoS на требуемом уровне.

1.4. Введение в MPLS.

Многопротокольная коммутация меток MPLS – это стандарт, разработанный рабочей группой по созданию интегрированных услуг IETF. Это новая архитектура построения магистральных сетей, которая значительно расширяет имеющиеся перспективы масштабирования, повышает скорость обработки трафика и предоставляет огромные возможности для организации дополнительных услуг. Технология MPLS сочетает в себе возможности управления трафиком, присущие технологиям канального уровня, и масштабируемость и гибкость протоколов, характерные для сетевого уровня. Являясь результатом слияния механизмов разных компаний, она впитала в себя наиболее эффективные решения каждой.

MPLS соединила в себе надежность ATM, удобные, и мощные средства доставки и обеспечения гарантированного качества обслуживания IP-сетей, такая интеграция сетей позволяет получить дополнительную выгоду из совместного использования протоколов IP и ATM.

Главная особенность технологии MPLS – отделение процесса коммутации пакета от анализа IP-адреса в его заголовке, что позволяет осуществлять коммутацию пакетов значительно быстрее.

В соответствии с протоколом MPLS маршрутизаторы и коммутаторы присваивают на каждой точке входа в таблицу маршрутизации особую метку и сообщают эту метку соседним устройствам. Наличие таких меток позволяет маршрутизаторам и коммутаторам, поддерживающим технологию MPLS, определять

следующий шаг в маршруте пакета без выполнения процедуры поиска адреса.

На сегодняшний день существуют три основные области применения MPLS. Это моделирование трафика, поддержка классов обслуживания (CoS) и виртуальных частных сетей (VPN), которая на сегодняшний день весьма популярна.

Виртуальные частные сети.

Требования, предъявляемые к виртуальным сетям сегодня, условно можно подразделить на две группы: с одной стороны, это возможности, которые необходимы сервис-провайдеру для экономического предоставления услуг VPN клиентам, а с другой стороны, это функции безопасности, которые нужны корпоративным клиентам для защиты информации в общественной сети.

Как говорилось выше, VPN должны решить проблемы безопасности данных и поддержки неуникальных адресов частных сетей. MPLS предлагает простое решение этих проблем и позволяет провайдеру предоставлять услуги VPN, используя механизм туннелирования.

Использование MPLS для построения VPN позволяет сервис-провайдерам быстро и экономично создавать защищенные виртуальные частные сети любого размера в единой инфраструктуре.

Помимо построения сети предприятия, на базе технологии VPN можно также построить и сеть оператора IP-телефонии, имеющего свои представительства в разных странах. И VPN не просто объединит несколько небольших офисов, а позволит организовать единую сеть оператора IP-телефонии на всей территории земного шара. К тому же эта сеть сможет поддерживать множество дополнительных услуг взятых из VPN и реализовывать гарантированное качество обслуживания на основе MPLS.

1.5. Актуальность темы дипломной работы.

Технология VPN входит в группу важнейших технологий, которые предприятия собираются использовать в ближайшем будущем.

В свете все более возрастающего интереса к технологии, уже сегодня сервис-провайдеры разрабатывают планы предоставления услуг с добавленной ценностью поверх своих транспортных сетей VPN, расширяется рынок VPN-продуктов. Вместе с тем, важное место при организации VPN занимают информационная безопасность корпоративных сетей и применение криптографии для защиты информации при передаче по сети общего пользования.

Возможно, виртуальные частные сети станут основой для поддержки услуг, предоставляемых сетями нового поколения, поэтому задача выбора технологии построения VPN 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 технологии VPN MPLS, несомненно, есть будущее и рассмотрение организации такой сети довольно актуальный вопрос.

Глава 2. Технология MPLS.

2.1.Общие принципы.

Каждый пакет при использовании на сетевом уровне протокола, не предусматривающего создания виртуальных соединений, передается независимо на своем пути следования 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, что в свою очередь дает возможность решения части проблем, о которых говорилось ранее в главе 1.

В качестве технологии, обеспечивающей ускоренную передачу пакетов по сети, применяется технология MPLS.

MPLS (Multiprotocol Label Switching) – это технология многопротокольной коммутации на основе меток.

Данная технология была разработана комитетом IETF и является результатом объединения нескольких технологий, таких как IP Switching, Tag Switching, Aris и Cell Switch Router. Основная идея MPLS заключается в обеспечении возможности передачи IP-трафика по множеству, а не по одному маршруту, определенному по протоколу BGP или OSPF. Благодаря такому подходу к передаче трафика появилась возможность избежать проблем, связанных с недостаточной пропускной способностью каналов связи, что позволяет операторам внедрять различные классы и уровни обслуживания.

«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 транспонировать информацию множества других протоколов высших уровней модели

OSI. Напомню, что на физическом уровне обеспечивается двухсторонняя передача битов с определенной достоверностью; на втором, канальном уровне, обеспечивается формирование в тракте передачи этих бит надежного логического звена связи, по которому обеспечивается двухсторонний обмен информационными блоками, при этом, заданная достоверность передачи гарантируется путем обнаружения и исправления ошибок; а на третьем уровне реализуются функции, обеспечивающие передачу информационных блоков по сети от отправителя к получателю через несколько узлов, выбирая подходящий маршрут передачи, который образуется из звеньев второго уровня. Информационный блок каждого уровня содержит заголовок и информационное поле, а каждый блок протокола вышестоящего уровня помещается в информационное поле блока протокола, соседнего нижележащего уровня. Таким образом, 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 эквивалентности пересылки
- LSP – коммутируемый по меткам тракт

Рассмотрим каждый из них подробно.

2.2.1. Метки.

Метка - это идентификатор фиксированной длины, определяющий класс эквивалентности 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, которая вставляется между заголовками канального и сетевого уровня. Являясь протокольно независимой, она может использоваться для инкапсуляции пакетов любого протокола сетевого уровня. Это может быть метка идентификаторов виртуального канала и виртуального пути (VCI/VPI) или метка идентификатора соединения канального уровня (DLCI).

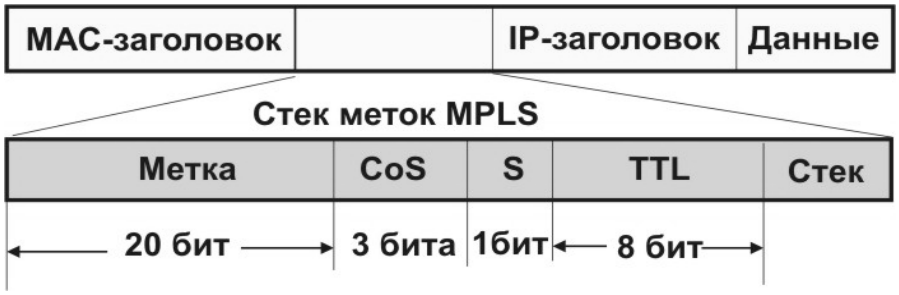


Рисунок 2.

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

Информация об уровне качества обслуживания в сети MPLS передается в поле CoS, занимающем следующие три бита в поле метки. Это поле необходимо для предоставления дифференцированных услуг в сети MPLS. Для сквозного обеспечения услуг IP QoS на границе MPLS-сети можно скопировать поле IP-приоритета в поле CoS. Технология MPLS использует функции IP QoS

для реализации различных уровней обслуживания трафика, передающегося по сети. В MPLS информация об QoS передается в поле CoS, в то время как в IP уровень качества обслуживания определяется значением заголовка IP-пакета.

Поддержка QoS реализуется за счет применения одного из двух механизмов:

- трафик, передаваемый по определенному LSP-туннелю, помещается в очередь выходного интерфейса LSR в зависимости от его приоритета.
- для каждой пары пограничных маршрутизаторов устанавливается несколько путей, по которым передаются потоки с различным приоритетом.

Последний бит третьего байта используется для указания окончания стека меток.

Четвертый байт в формате поля метки занимает параметр TTL (Time to Live), который указывает время, в течение которого пакет должен существовать в сети, что обеспечивает некий уровень защищенности сети от образования петель и ограничивает область распространения пакета.

Характерным свойством меток является их уникальность. Уникальность меток заключается в следующем: маршрутизатор LSR имеет право осуществить привязку метки к FEC только при условии, что он может однозначно определить к стеку меток какого маршрутизатора она относится.

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. Поскольку дерево ветвится многократно, в каком-то другом LSR, находящемся ближе к корню, происходит слияние нескольких объединенных потоков, и в стеке появляется еще одна метка.

Метки в стеке располагаются по принципу «последний пришел – первый вышел». Каждый маршрутизатор работает только с первой (верхней) меткой в стеке пока она не удаляется. Остальные метки стека передаются прозрачно до удаления вышестоящей. В дальнейшем, эти метки анализируются и обрабатываются аналогично верхней.

Число меток стека определяют его глубину. Считается, что стек меток имеет глубину m, если метка, находящаяся на дне стека размещена на первом уровне, метка над ней – на втором, а верхняя метка имеет уровень m. Пакет, не содержащий в себе метку, имеет глубину стека, равную нулю. LSP-туннель, по которому передаются пакеты, имеющие глубину стека m, называют LSP уровня m.

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. Определение протокола третьего уровня производится на основе последней метки стека и содержимого самого заголовка. Таким образом, метка, заносимая в стек первой должна быть уникальной для каждого протокола сетевого уровня. Кроме того, к заменяющей ее метке в процессе передачи предъявляются такие же требования. В противном случае выходной LER не сможет определить используемый в данном пакете протокол сетевого уровня.

Для создания меток используются разные методы:

- метод на основе топологии. Для задания меток 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 эквивалентности пересылки FEC.

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

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.

При традиционной IP-маршрутизации конкретный маршрутизатор тоже может считать, что два пакета принадлежат одному и тому же условному классу эквивалентности, если в его таблицах маршрутизации используется некий адресный префикс, идентифицирующий направление, в котором предполагаемые маршруты транспортировки этих двух пакетов совпадают наиболее долго. По мере продвижения пакета по сети каждый следующий маршрутизатор анализирует его заголовок и приписывает этот пакет к такому из собственных, принадлежащих только этому маршрутизатору классов эквивалентности, который соответствует тому же направлению.

В отличие от традиционной маршрутизации, при использовании многопротокольной коммутации на основе меток 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.

Таким образом, подводя итог вышесказанного, можно дать следующее определение FEC. Класс эквивалентности пересылки FEC – это форма представления группы пакетов с одинаковыми требованиями к их передаче, т. е. все пакеты такой группы обрабатываются одинаково на пути их следования к пункту назначения.

Класс FEC представляет собой набор FEC-элементов, каждый из которых идентифицируется определенной меткой. На сегодняшний день существует всего два FEC-элемента: Address Prefix и Host Address.

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.

Метод пересылки пакетов на основе пар «FEC – метка», принятый в MPLS, имеет ряд преимуществ перед методами, основанными на анализе заголовка блоков сетевого уровня. В частности, пересылку по методу MPLS могут выполнять маршрутизаторы, которые способны читать и заменять метки, но при этом либо вообще не способны анализировать заголовки блоков сетевого уровня, либо не способны делать это достаточно быстро.

2.2.3. Коммутируемый по меткам тракт LSP.

Коммутируемый по меткам тракт – это последовательность MPLS-маршрутизаторов.

Набор пакетов, передаваемый по LSP, относится к одному FEC, и каждый маршрутизатор LSR в LSP-туннеле назначает для него свою метку. LSP-туннель создается внутри LSP-тракта. Следует отметить, что зачастую начало и конец туннеля не совпадают с началом и концом LSP-тракта. Как правило, туннель короче. Для каждого туннеля подсчитывается число пропущенных пакетов и байт. Иногда поток данных может быть настолько велик, что для него создается несколько LSP-туннелей между отправителем и получателем.

В одном LSP может быть создано несколько LSP-туннелей с различными точками приема и передачи, а в каждом туннеле могут быть созданы LSP-туннели другого уровня. В этом проявляется иерархичность структуры MPLS.

Возможны два варианта создания туннелей: 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-туннель 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.

2.3. Принцип работы.

В основе MPLS лежит принцип обмена меток. Любому передаваемому IP-пакету 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, присваивается определенный класс эквивалентности пересылки FEC (Forwarding Equivalence Class). Класс FEC характеризует группу пакетов с одинаковыми требованиями к передаче, такие пакеты на всем пути следования до пункта назначения будут обрабатываться одинаково. Отмечу, что анализ заголовка IP-пакета и назначение FEC производится только один раз на входе в сеть.

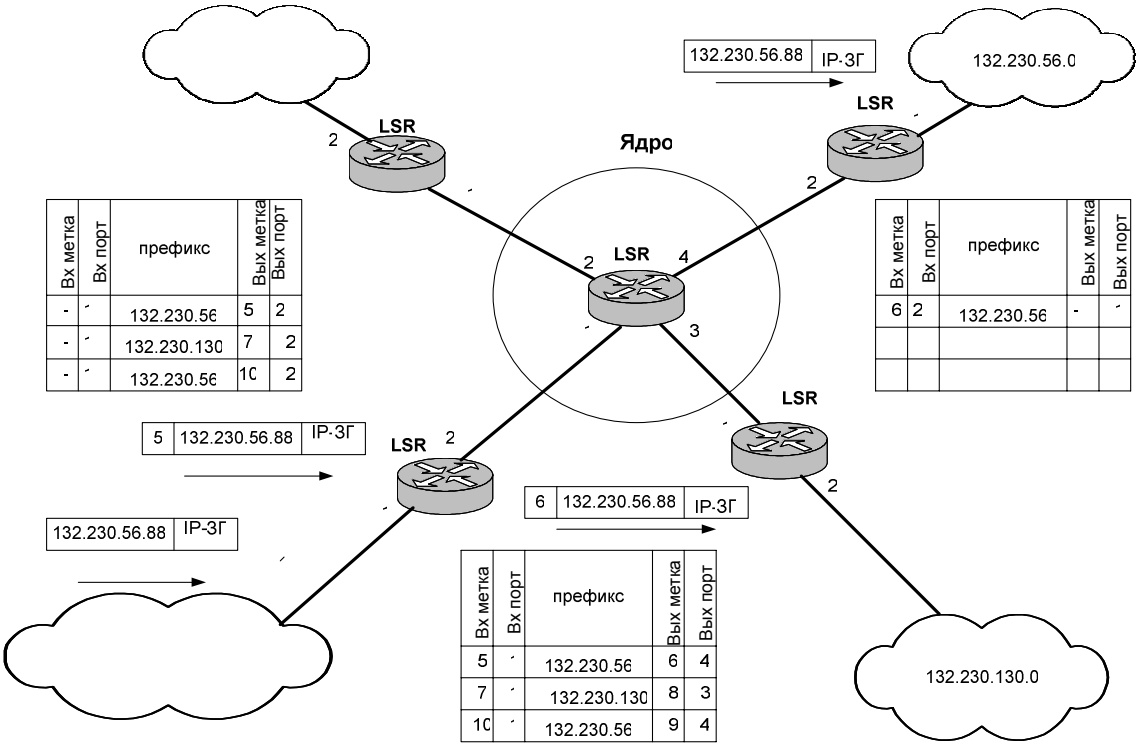


Рис 3. сеть MPLS.

По своей сути FEC представляет набор FEC-элементов, он идентифицируется определенной меткой, представляющей собой код фиксированной длины. Метка каждый раз меняется, т.е. она имеет 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. Устройство коммутации по меткам, как правило, заменяет содержащуюся в пакете метку, некоторой новой меткой перед ее пересылкой на следующий участок маршрута, вследствие чего алгоритм пересылки называют перестановкой меток (label swapping). Для принятия решения о том, куда пересылать пакеты, используется алгоритм точного совпадения меток. При этом определение направления пересылки меток осуществляется маршрутизаторами с помощью использования стандартных протоколов управления IP-сетью.

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 поддерживает маршрутизаторы 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 получения 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. База LIB позволяет упростить процесс продвижения пакетов и повысить масштабируемость сети благодаря сопоставлению нескольких входящих меток к одному и тому же блоку информации об исходящей метке, за счет чего реализуется новый тип маршрутизации.

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 меток в узлах на пути следования потока от отправителя к получателю. По таким трактам в сети MPLS реализуется передача данных. Следует отметить, что пакеты, принадлежащие одному FEC, передаются по одному LSP. 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. После выбора оптимального маршрута маршрутизаторы обмениваются метками. Метки в LSP раздаются с помощью протокола распределения меток LDP или с помощью протокола RSVP, или же инкапсулируются в протоколы маршрутизации BGP и OSPF. Каждый пакет инкапсулирует и переносит метки во время своего следования от отправителя к получателю.

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.

2.3.1.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.

Следует отметить, что при осуществлении коммутации пакетов по туннелю, LSR, занося свою метку в стек, должен руководствоваться тем, чтобы данная метка соответствовала FEC, с которым соотнесен трафик.

Объединение меток.

Для реализации процесса коммутации 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. Соответственно, если LSR не способен объединять метки, то они должны быть переадресованы с различными выходными метками. При объединении входящих меток число выходных меток на один FEC равно единице, а если маршрутизатор не может объединять метки, то число выходных меток соответствует числу узлов в сети.

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

Назначение меток для объединяющих и необъединяющих маршрутизаторов производится следующим образом. Если вышестоящий LSR поддерживает объединение меток, то он назначает одну метку на FEC. В ином случае, маршрутизатор назначает несколько меток на один FEC. При этом, метки посылаются только по запросу LSR, так как заранее не известно, сколько нужно меток. Если и нижестоящий маршрутизатор не поддерживает объединение меток, то,

при получении запроса от вышестоящего LSR, он подает запрос следующему нижестоящему маршрутизатору.

2.4.Распределение меток.

Тракт LSP между двумя маршрутизаторами LSR является однонаправленным.

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 вначале 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 два способа 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 верхний, так и нижний LSR. Эти режимы называются, соответственно, unsolicited downstream и downstream ondemand.

Предполагается, что некоторые реализации MPLS будут поддерживать только определенный метод реализации назначения меток, а некоторые будут работать в двух режимах. В любом конкретном случае LSR должны согласовывать режим работы.

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

Консервативный режим распределения меток.

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.

Либеральный режим распределения меток.

В данном режиме верхний LSR принимает решение о привязке метки к FEC как от смежных, так и от несмежных LSR.

Неоспоримым достоинством свободного режима привязки меток является его быстрая адаптация к маршрутным изменениям сети, но за это приходится расплачиваться необходимостью работы с большим диапазоном меток. Консервативный же режим, в свою очередь, требует от LSR поддержки много меньшего числа меток.

2.4.1. 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. Для того чтобы реализовать переадресацию в MPLS согласно динамически определяемому маршруту каждый LSR должен установить в своей базе LIB соответствие между одной или несколькими входящими и исходящими метками и, используя протокол рассылки меток, проинформировать маршрутизаторы о назначенных им привязках «метка-FEC».

При динамической маршрутизации существует разные варианты привязки метки к FEC. Они выполняются как нижним, так и верхним маршрутизаторами.

На сегодняшний день именно этот режим маршрутизации применяется в IP-сетях.

При явной маршрутизации путь, по которому будет должен следовать трафик, задается отправителем. Явная маршрутизация дает возможность проводить политику маршрутизации и управление трафиком. Данный тип маршрутизации может быть инициирован входным или выходным маршрутизаторами. Путь, определенный силами явной маршрутизации, запоминается полностью, то есть, запоминаются все маршрутизаторы, через которые будет передаваться информационный поток. 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 маршрутизации.

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

2.5. Протокол рассылки меток.

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. Остановимся на них подробнее.

Протокол 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 LSR.

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. После установления сессии инициатор раздачи меток может послать сообщение с запросом на получение метки Label Request, в котором описывается FEC передаваемого потока. На данный запрос возможны два варианта ответа. 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.

Важной функцией протокола LDP является функция обнаружение петель. Для этой цели протоколом LDP предусмотрено наличие двух полей Path Vector и Hop Count в сообщениях Label Request и Label Mapping.

В поле Path Vector содержится список идентификаторов тех маршрутизаторов, через которые прошло данное сообщение. При передаче пакета по сети каждый LSR маршрутизатор анализирует данное поле и, в случае обнаружения собственного идентификатора принимает решение о возникновении петли.

Поле Hop Count содержит счетчик пройденных сообщением маршрутизаторов. Если значение счетчика становится равным максимальному значению, то считается, что при передаче пакета образовалась петля.

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. Traffic Engineering.

Вернемся к проблеме единого трафика и качества обслуживания в IP-сетях, которая уже была затронута в первой главе анной работы.

Под термином Traffic Engineering понимают методы и механизмы 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.

При традиционной маршрутизации IP-трафик маршрутизируется посредством его передачи от одной точки назначения к другой и следует до пункта назначения по пути, имеющем наименьшую суммарную метрику сетевого уровня. Этот путь может не быть оптимальным, так как он зависит от информации о статической метрике канала. В данном случае, при выборе пути не учитываются свободные сетевые ресурсы, текущая загрузка каналов, а также требования к обслуживанию трафика. Таким образом, если кратчайший путь уже перегружен, то пакеты все равно будут посылаться по этому пути, вследствие чего будет наблюдаться картина загруженности одних каналов связи и простоя других. Следует заметить, что при наличии в сети нескольких равноценных альтернативных маршрутов, трафик делится между ними, и нагрузка на маршрутизаторы и каналы связи распределяется более сбалансировано. Но, если маршруты не являются полностью равноценными, распределение трафика между ними не происходит.

Технология управления трафиком – это мощный механизм эффективного использования ресурсов сети. При рассмотрении TE в более широком масштабе можно дать ему следующее определение: TE - глобальная оптимизация сети за счет изменения всех возможных параметров: количества маршрутизаторов, их производительности, топологии связей между ними, скоростей каналов передачи трафика, приоритетов обслуживания и др.

Технология управления трафиком включает в себя различные временные масштабы:

- реальный масштаб времени. При этом параметры изменяются с периодом в несколько секунд или микросекунд. Этот тип обеспечивает

QoS в маршрутизаторах, которые используют различные дисциплины обслуживания очередей и оперируют каждым отдельным пакетом.

- оперативное управление параметрами. В этом случае период составляет несколько часов или дней. Здесь реализуются методы выбора путей передачи информационного трафика через сеть, при этом путь меняется только в случае продолжительного изменение интенсивности потоков.

- планирование сети, подразумевающее изменение параметров один раз в несколько месяцев или лет. Параметрами в данном случае выступают структурные характеристики сети: количество маршрутизаторов, их тип, топология, типы каналов связи.

В качестве основы для моделирования трафика можно взять технологию MPLS. Данная технология позволяет сетевым администраторам указывать точный физический маршрут для маркировки пакетов, а также выбирать маршруты, соответствующие специфическим требованиям передачи.

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.

Управление трафиком в MPLS основано на следующих механизмах:

- на применение туннелей LSP, формирующихся на основе протокола RSVP-TE.
- на протоколах маршрутизации внутреннего шлюза, которые базируются на расширенных протоколах определения состояния канала.
- на алгоритме вычисления пути, который определяет пути LSP.
- на механизмах доступа к ресурсам сети.

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 через маршруты с коммутацией по меткам.

Задачи TE включают в себя технологию, научные принципы определения оптимального пути, моделирование, описание и управление трафиком. Для поддержания задач TE технология MPLS предлагает использовать протокол LDP с учетом ограничивающих ресурсов – CR-LDP или модифицированный протокол резервирования ресурсов RSVP - RSVP-TE.

Получить полную картину о сети MPLS позволяет применение расширенных протоколов маршрутизации: OSPF и IS-IS, которые лавинообразно распространяют информацию для каждого маршрутизатора, содержащую полную информацию о топологии сети, метрике сети по всем каналам, с целью обеспечения вычисления кратчайшего пути до адресата.

В объявлениях данных протоколов содержится информация о маршрутизаторах, связи между ними и в целом о сети. Управление трафиком реализуется благодаря тому, что в данные протоколы включены дополнительные типы сообщений, в которых по сети распространяется информация об изначальной и доступной пропускной способности каждого канала. Благодаря данной информации маршрутизатор LSR, в соответствии с предъявляемыми требованиями к качеству обслуживания, определяет путь передачи трафика.

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.

2.6.1.Атрибуты TE-туннеля.

TE-туннель имеет определенные атрибуты, описывающие требования транка трафика, от которых зависит выбор политики администратора.

Полоса пропускания. Данный атрибут определяет сквозную полосу пропускания, необходимую для TE-туннеля. Ее выбор основан на требованиях класса трафика, который передается по TE-туннелю.

Приоритет установки и удержания. Эти приоритеты используются при управлении доступом. Приоритет установки определяет приоритет ресурса.

Когда ресурсы находятся в состоянии конфликта, новый туннель с высоким приоритетом получения ресурса может вне очереди занять свободный ресурс. Вытесняя при этом все установленные туннели в пути, приоритет удержания которых меньше приоритета получения ресурса нового туннеля. Установленный TE-туннель с наивысшим приоритетом удержания не может быть вытеснен.

Родственность класса ресурса. Атрибут представляет возможность ограничивать выбор пути административным включением в сеть определенных каналов или исключением их из сети.

Порядок выбора пути. Определяет порядок, в котором пограничный маршрутизатор выбирает явные пути для ТЕ-туннелей.

В атрибуте устойчивость определяется желаемое поведение системы в случае прекращения существования текущего пути ТЕ-туннеля. Это происходит из-за сбоев сети или вытеснения туннеля.

Адаптируемость. Данный атрибут определяет, нужно ли повторно оптимизировать существующие ТЕ-туннели в случае, если появится лучший путь.

Атрибуты ресурсов канала. Такие атрибуты описывают все каналы. В них содержится информация о свободных ресурсах и о политиках использования канала для вычисления пути.

Доступная полоса пропускания. В атрибуте указывается ширина свободной полосы пропускания для каждого приоритета получения ресурса.

Класс ресурса. На атрибуте класса ресурса основывается решение о включении канала в процессе вычисления пути или об исключении канала из него. Атрибуты класса могут использоваться для:

- реализации одинаковых политик для набора ресурсов. Которые необязательно находятся в одной и той же топологической области.
- спецификации относительного предпочтения для набора ресурсов, связанных с положением маршрута, по которому транспортируется поток данных.
- ограничение положения каналов передачи данных для заданного субнабора ресурсов.

- реализации политики ограничения локальности трафика. То есть, политики, которая ищет способы размещения трафика в пределах оговоренных топологических областей сети.

Атрибуты, связанные с каналами передачи данных и ресурсами сети, а также параметры, связанные с маршрутизацией, в совокупности представляют собой набор управляющих переменных, которые могут быть модифицированы в результате либо действий администратора, либо автоматических агентов, для того, чтобы привести сеть в требуемое состояние.

При определении явно задаваемого пути необходимо учитывать ограниченные возможности канала и требования TE-туннеля.

В первую очередь, рассматриваются атрибуты TE-туннеля, задаваемые вышестоящим маршрутизатором, создающим этот туннель; ресурсы каналов всей сети и информация о ее топологии, которая распространяется протоколом внутреннего шлюза.

Минимальным требованиям (по полосе пропускания и т.д.) могут отвечать сразу несколько маршрутов, выбор определенного маршрута производится на последующих этапах.

На следующем шаге производится выбор каналов. Критериями выбора в данном случае являются, пропускная способность канала и ресурс, который может быть предоставлен каналом. При этом выбирается маршрут с наименьшим числом переходов.

Далее, при помощи алгоритма SPF определяется явный путь TE-туннеля.

Технология MPLS поддерживает два типа явных путей: строгий (strict) и свободный (loose). Строгий явный путь определяет все промежуточные узлы следования трафика. Свободный – задает только часть промежуточных узлов, а выбор остальных предоставляет самим промежуточным узлам.

Наряду с последовательностью маршрутизаторов в сообщениях RSVP-TE указывается резервируемая пропускная способность. Каждый LSR, получив такое сообщение, вычитает запрашиваемую пропускную способность из пула свободной пропускной способности соответствующего интерфейса, а затем объявляет остаток в сообщениях протокола маршрутизации.

Первостепенной задачей управления трафиком является минимизация перегрузок, носящих долгосрочный характер и влияющих на поведение сети с целом.

Перегрузки в сети могут быть вызваны в силу двух причин: во-первых, перегрузки возникают при несоответствии находящихся в наличии ресурсов сети поступающей нагрузке. В этом случае проблема перегрузок может быть решена путем расширения ресурсов сети, применением стандартных средств управления перегрузками, или сочетанием этих методов. Во-вторых, перегрузки возникают при неэффективном распределении информационных потоков по сетевым ресурсам. Решением в данной ситуации является применение технологии TE.

Управление трафиком в сети MPLS позволяет:

- Исключить необходимость ручной конфигурации сетевых устройств, для задания определенных маршрутов.
- Производить оценку полосы пропускания канала и значения трафика при прокладке маршрута через опорную сеть.
- При отказе узла производить коррекцию топологии опорной сети благодаря наличию механизмов динамической адаптации.

Рассматривая принцип маршрутизации в MPLS в сравнение с традиционной маршрутизацией по отношению к технологии MPLS можно выделить следующие преимущества:

- внутренние маршрутизаторы сети MPLS – простые, так как их функция сводится к осуществлению коммутации.

- при традиционной маршрутизации маршрутизатор может рассматривать только информацию, находящуюся в заголовке IP-пакета, тогда как граничный маршрутизатор MPLS может использовать для этой цели и другую информацию, вплоть до зависимости от портов, по которым поступают пакеты.
- сопоставление пакетов с FEC может зависеть и от самого маршрутизатора, на который поступает трафик.
- маршрутизации пакетов в MPLS предоставляет пользователю гарантии минимальной задержки пакетов и максимальной пропускной способности.

Управление доступом к каналу.

Система управления доступом решает, какому из TE-туннелей следует предоставить ресурсы. Она предполагает наличие следующих функций:

- определение наличия ресурсов. Система определяет, есть ли свободные ресурсы.
- уничтожение ресурса. Система должна уничтожить существующие туннели, когда новые туннели с высоким приоритетом получения ресурса вытесняют существующие туннели с низким приоритетом удержания ресурса.
- введение локального учета использования ресурсов. Подразумевает контроль над использованием ресурсов сети.
- инициирование обновления информации о маршрутах протокола внутреннего шлюза. Система инициирует процесс лавинообразного распространения обновления информации о маршрутах протокола внутреннего шлюза, когда из статистики локального учета использования ресурсов следует, что количество доступных ресурсов может опуститься ниже сконфигурированного порогового значения.

2.6.2. Поддержка TE-пути.

Поддержка TE-пути включает выполнение таких функций, как повторная оптимизация пути и его восстановлении. Эти операции выполняются после установки TE-туннеля. Повторная оптимизация пути описывает желаемое поведение маршрутизатора в случае появления после установки TE-туннеля его потенциально лучшего преемника. Во время повторной оптимизации пути маршрутизатор должен попытаться найти какую-либо возможность для того, чтобы заново оптимизировать существующий TE-путь.

Восстановление пути описывает метод восстановления TE-туннеля в случае, если текущий путь перестал функционировать, используя для этого атрибут устойчивости.

Протокол CR-LDP.

CR-LDP – это протокол LDP с учетом ограничивающих условий. Протокол представляет собой расширение базового протокола LDP и в отличие от протокола LDP, способного следовать только таблицам маршрутизации, поддерживает явную маршрутизацию с учетом CoS.

При использовании протокола CR-LDP в качестве протокола распространения меток, запрос на получение метки следует по явно заданному маршруту. В этом случае нет необходимости использовать таблицы маршрутизации, сообщение передается по маршруту, заданному в специальном поле ERO сообщения Path.

Протокол CR-LDP не поддерживает динамического вычисления явно задаваемых маршрутов, поэтому сведения о динамическом резервировании пропускной способности должны включаться в широковещательную информацию протоколов OSPF и IS-IS или в объявления о состоянии каналов. Благодаря этой информации протокол CR-LDP занимает и резервирует пропускную способность. Величина доступной пропускной способности изменяется в соответствии с запросами, и ее новое значение рассылается остальным

маршрутизаторам с помощью протоколов OSPF или IS-IS, после чего вычисляется новый маршрут для прокладки LSP.

2.6.3.Протокол RSVP-TE.

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 введены дополнительные возможности: функция явной маршрутизации и метод привязки меток к RSVP-потокам.

Основная цель применения протокола RSVP в MPLS заключается в том, чтобы маршрутизаторы LSR, которые выполняют классификацию пакетов путем анализа их меток, а не IP-заголовков, могли распознавать пакеты, принадлежащие потокам, для которых было сделано резервирование ресурсов. В этом случае, совокупность пакетов, для которых было сделано резервирование ресурсов, рассматривается как еще один класс FEC.

Протокол RSVP-TE – это расширение существующего протокола RSVP. Протокол использует сигнальные сообщения протокола RSVP, добавляя определенные расширения для поддержки механизмов управления трафиком. Для управления трафиком применяются туннели, построенные на базе MPLS, а для передачи данных по явному пути используются локальные метки. Суть маршрутизации на основе резервирования ресурсов заключается в том, что в отличие от протоколов маршрутизации, продвигающих пакеты на основе топологии сети (OSPF, IS-IS) в данном случае пакеты передаются с учетом класса трафика; требований, предъявляемых к обслуживанию и с учетом ресурсов сети. Соответственно, для реализации маршрутизации на основе резервирования необходимо определить

класс трафика, предъявляемые требования и способ задания явного маршрута

Применение протокола RSVP-TE дает следующие возможности в отношении туннелей LSP.

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

В протоколе RSVP достаточно просто осуществить привязки меток к потокам с резервированием, по крайней мере, в случае использования уникастных адресов.

Для привязки метки к потоку с резервированием ресурсов сообщение Resv расширили дополнительным объектом Label, который переносится внутри сообщения Resv. Таким образом, RSVP становится инструментом для распределения меток MPLS. Когда LSR желает передать сообщение Resv для нового потока RSVP, LSR назначает метку из своего пула свободных меток, создает запись в своей таблице LIB, делая назначенную метку входящей меткой, и затем передает сообщение Resv, содержащее эту метку в объекте LABEL. Следует отметить, что, поскольку сообщения Resv идут от получателя к отправителю, это разновидность назначения меток снизу.

При получении сообщения Resv, содержащего метку потока, маршрутизатор записывает ее в своей базе LIB как исходящую, назначает для данной исходящей метки входящую и пересылает ее вышестоящему LSR. Таким образом, по пути распространения сообщения создается тракт LSP. Поскольку в сообщениях Resv указываются метки, каждый LSR может легко связать соответствующие ресурсы QoS с трактом LSP.

Протокол RSVP, расширенный объектом LABEL, может создать тракт LSP только вдоль маршрута, вычисленного схемой традиционной маршрутизации пакетов IP. Это вызвано тем, что при использовании обычного протокола RSVP путь, по которому идет сообщение Path, управляется парадигмой пересылки на основе пункта назначения, а маршрут, по которому идет сообщение Path, задает путь LSP. Когда маршрутизатор должен переслать сообщение Path, он для определения следующего маршрутизатора, к которому он должен переслать сообщение, использует имеющуюся у него таблицу маршрутизации, которая формируется с помощью таких протоколов, как IS-IS, OSPF, RIP или BGP, и адрес получателя, содержащийся в заголовке IP-пакета. При этом отсутствует способность «управлять» сообщением Path, отправляя его вдоль конкретного, явно заданного маршрута

Для возможности задания явного маршрута в протокол RSVP-TE ввели еще один объект – Explicit Route Object (ERO). ERO содержит последовательность маршрутизаторов, представляющую собой явно заданный маршрут и включается в сообщении Path. В ответ на это сообщение по данному маршруту передается сообщение Resv, благодаря чему резервируются ресурсы сети, и устанавливается путь LSP. Заметим, что ERO состоит из конкретно заданных абстрактных узлов. Каждый такой узел представляет один или несколько маршрутизаторов, при этом внутренняя топология группы

маршрутизаторов может быть непрозрачной для маршрутизатора, который вычисляет явно заданный маршрут. Примером такого абстрактного узла может быть совокупность маршрутизаторов, принадлежащих конкретной автономной системе или набор маршрутизаторов, адреса которых попадают под конкретный адресный префикс. Сточки зрения кодирования, объект ERO представляет собой последовательность триплетов формата TLV, в котором каждый триплет описывает конкретный абстрактный узел.

Поскольку трафик, проходящий по LSP определяется меткой, присвоенной на входном маршрутизаторе, то данный путь можно считать своеобразным туннелем, находящемся под уровнем IP-маршрутизации, причём трафик идущий по нему непрозрачен для промежуточных узлов. Таким образом, появилось понятие LSP-туннеля.

Для поддержания функций LSP-туннеля в RSVP-TE введены дополнительные объекты RSVP SESSION, SENDER_TEMPLATE и FILTER_SPEC, называемые LSP_TUNNEL_IPv4 и LSP_TUNNEL_IPv6. Функционально эти объекты идентичны, а отличаются только форматом адреса, с которым работают, поэтому их обобщенно называют LSP_TUNNEL.

Стоит также отметить появление в протоколе RSVP-TE объектов RECORD_ROUTE и SESSION_ATTRIBUTE. Объект RECORD_ROUTE входит в состав сообщения Path. Цель его использования - предоставление пользователю информации о маршруте, по которому проходит LSP-туннель, а также в запросе на получение уведомления при изменении пути LSP.

Объект SESSION_ATTRIBUTE также входит в состав сообщения Path. Данный объект несет в себе информацию о приоритете данного сеанса установления тракта LSP по сравнению с другими сеансами.

Кроме того, он указывает на необходимость записи меток при записи информации о маршрутах.

После установления LSP-тракта устанавливается LSP-туннель. Следует отметить, что если трафик доставляется без гарантий, то нет необходимости в резервировании ресурсов. Как и в протоколе RSVP в протоколе RSVP-TE резервирование ресурсов сети реализуется передачей в сообщении Resv полей Tspec и Rsepc.

Одним из основных требований к управлению трафиком является возможность ремаршрутизации TE-туннелей согласно определенным условиям, задаваемым администратором сети. В общем, проводить разделение трафика, а также оказывать другие неблагоприятные воздействия на сеть нежелательно. Поэтому, создание нового LSP-туннеля и перенесение в него трафика производится до разрушения старого LSP. Недостатком такой реализации является возможность соперничества между старым и новым туннелями за ресурсы, что может привести к отказу в установлении нового туннеля. В RSVP-TE данная проблема решается за счет разделения ресурсов между старым и новым LSP.

Еще одним характерным свойством сети MPLS является быстрая перемаршрутизация – механизм, служащий для минимизации потерь пакетов в случае сбоев и отказов. Суть данного термина сводится к выделению защитного туннеля для переключения трафика в случае отказа канала или узла.

Выделяют три типа перемаршрутизации:

- защита канала. Вариант предполагает, что при обрыве канала производится переход на резервный туннель, который используется до тех пор, пока не будет рассчитан новый маршрут через туннель.

- защита узла. Это второй тип быстрой перемаршрутизации, применяющийся в ситуации, когда при передаче трафика дает сбой какой-либо маршрутизатор, что подразумевает необходимость

защищать туннель до его перехода, следующего за защищенным каналом.

- защита маршрута подразумевает создание множества туннелей от начальной до конечной точки, при этом все они проходят по разным маршрутам. Из представленных вариантов перемаршрутизации - то наиболее ресурсоемкая, наиболее медленная и наименее масштабируемая защита.

Заканчивая краткое рассмотрение протокола RSVP-TE, следует отметить главные расширения этого протокола:

- поддержку резервирования меток.

Протокол RSVP-TE должен поддерживать резервирование меток и их установку для использования RSVP при сигнализации LSP-туннеля. В отличие от обычного RSVP- протокола, протокол RSVP-TE использует RSVP с целью резервирования меток для потоков без резервирования полосы пропускания. Для этого определен новый тип объекта Flow Spec. Кроме того, протокол RSVP-TE также резервирует метки для потоков.

- поддержку маршрутизации от источника.

В LSP-туннелях используется явная маршрутизация от источника, которая реализуется в протоколе RSVP-TE путем добавления нового объекта – ERO.

- поддержка RSVP-TE - узлов.

В отличие от протокола RSVP, в котором сообщения PATH и RESV создаются приложениями на конечных узлах, в протоколе RSVP-TE данные сообщения инициируются верхними маршрутизаторами.

- поддержка идентификации туннеля, созданного на базе LSP-пути.

Для передачи идентификатора туннеля используются новые типы объектов Filter Spec и Sender Template.

- поддержка нового алгоритма удаления резервирования.

Для гарантированного удаления TE – туннеля дополнительно ввели новое сообщение Tear Confirm.

2.7. Выводы.

В заключение рассмотрения MPLS, хотелось бы выделить ряд преимуществ данной технологии в сравнении с другими технологиями базовой сети IP и IP/ATM. Среди них:

- повышение масштабируемости сети.
- быстрая коммутация на основе меток.
- разделение транспортного и управляющего уровней, что позволяет значительно облегчить введение новых протоколов маршрутизации и упростить, ускорить и снизить вероятность ошибки при проектировании оборудования.
- обеспечение высокой гибкости в предоставлении новых услуг, при относительной простоте настройки.
- доставка трафика с гарантированным уровнем качества QoS.
- MPLS позволяет уменьшить себестоимость и улучшить качество базовых услуг.
- возможность управления трафиком (Traffic Engineering). Поддержка функций управления трафиком дает возможность манипулировать прохождением данных по сети таким образом, чтобы можно было реализовать новые виды услуг.
- при построении VPN на базе MPLS отпадает необходимость в дополнительном шифровании информации и других мерах защиты доступа.
- по сети MPLS могут передаваться любые данные, так как содержимое пакета остается неизменным на протяжении всего пути, заменяются лишь метки.
- обеспечивает рабочие характеристики сетей 2 уровня

- обеспечивает связанность и сетевые услуги сетей 3 уровня
- при определении пути передачи трафика в MPLS рассматривается множество параметров, не отвечающие заявленным требованиям маршруты исключаются из рассмотрения.
- круглосуточная поддержка работы критически важных приложений.
- MPLS реализует механизмы, позволяющие назначать более высокий приоритет чувствительным к пропускной способности сети типам трафика, например, видео потокам.

Перечисленные достоинства делают MPLS весьма многообещающей технологией. 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. Использование MPLS в корпоративных сетях с большим трафиком, несомненно, более оправдано, чем в небольших LAN, так как изоляция трафика в локальных сетях не является проблемой для большинства пользователей, а требования к защите реализуются, как правило, на уровне приложений, что позволяет довольно просто отделить одного пользователя от другого. А обеспечение QoS экономически более выгодно реализовать увеличением мощности коммутаторов. В локальной сети применение MPLS для отделения неинформационного трафика от трафика данных.

Внедрение MPLS не должно вызвать какие-либо дополнительные затруднения в сравнении с другими протоколами, базирующимися на

IP. Естественно, необходимо учитывать то обстоятельство, что маршрутизаторы сети MPLS должны поддерживать данную технологию, это является обязательным условием для открытия LSP-тракта.

Глава 3. Туннельный эффект для VPN.

3.1. 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 финансовых 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.

3.2. 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 предоставление абонентам различных 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.

3.3. Технологии создания виртуальных частных сетей.

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).

На рисунке 4 представлен общий вариант построения виртуальной частной сети на базе общедоступной сети провайдера. Сеть каждого клиента состоит из территориально распределенных

офисов, которые связаны между туннелями, проложенными через сеть провайдера.

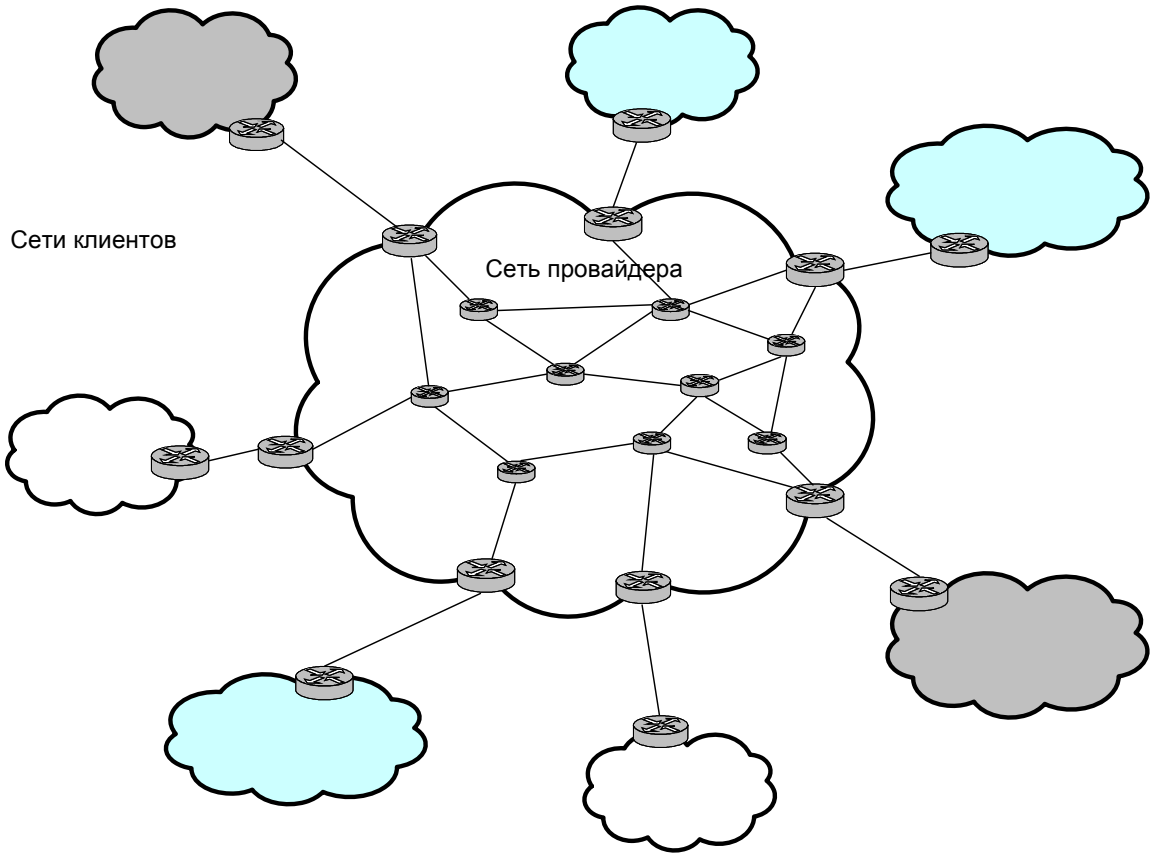


Рис 4. Виртуальная частная сеть.

IPSec VPN.

Internet Protocol Security относится к наиболее распространенным и популярным технологиям VPN. Стандарт IPSec обеспечивает высокую степень гибкости, позволяя выбирать нужный режим защиты, а также позволяет использовать различные алгоритмы аутентификации и шифрования данных. Режим инкапсуляции пакетов позволяет изолировать адресные пространства клиента и провайдера за счет применения двух IP адресов: внешнего и внутреннего.

IPSec, как правило, применяется для создания VPN, поддерживаемых провайдером, - туннели в них строятся на базе устройств клиента, но конфигурируются они удаленно и управляются провайдером.

Технология IPSec позволяет решать следующие задачи по установлению и поддержанию защищенного канала:

- аутентификацию пользователей или компьютеров при инициализации канала.
- шифрование и аутентификацию передаваемых данных между конечными точками канала.
- автоматическое снабжение точек секретными ключами, необходимыми для работы протоколов аутентификации и шифрования данных.

Недостатком данной технологии является тот факт, что из всех свойств виртуальной сети технология IPSec реализует только защищенность и изолированность адресного пространства. Пропускную способность и другие параметры QoS она не поддерживает. Кроме того, минусом IPSec является и его ориентированность исключительно на IP-протокол.

VPN на основе туннелирования через IP.

Сюда входят все технологии, для образования VPN которые используют туннели через IP-сети. Применение туннеля позволяет изолировать адресное пространство клиента, что в свою очередь дает клиенту возможность переносить незашифрованный трафик (L2TP) или шифровать его (PPTP).

Протокол PPTP поддерживает управление потоками данных и многопротокольное туннелирование на базе протокола IP. Удаленным пользователям протокол позволяет получать доступ к корпоративной сети, подключаясь по телефонной линии к местному поставщику услуг Интернет вместо прямого подключения к сети компании. PPTP

обеспечивает соединение с нужным сервером, создавая для каждого удаленного клиента виртуальную сеть. Протокол решает многие проблемы сетевых администраторов, вынужденных обеспечивать поддержку множества удаленных пользователей, но желающих избежать создания и обслуживания относительно дорогой сети на выделенных каналах.

Спецификации L2TP разрабатывает IETF. Он ориентирован на поддержку многопротокольного туннелирования, но кроме этого, обеспечивает совместимость всех L2TP продуктов.

К недостаткам протоколов PPTP и L2TP можно отнести отсутствие встроенных алгоритмов шифрования.

***MPLS VPN*.**

Технология MPLS в настоящее время является одной из наиболее перспективных технологий создания VPN.

Сеть MPLS VPN делится на две области: IP-сети клиентов и внутренняя (магистральная) сеть провайдера, которая служит для объединения клиентских сетей.

В общем случае у каждого клиента может быть несколько территориально обособленных сетей IP, 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 MPLS и образуют виртуальную частную сеть этого клиента. Обмен маршрутной информацией в пределах сайта осуществляется по одному из внутренних протоколов маршрутизации IGP.

Структура MPLS VPN предполагает наличие трех основных компонентов сети:

- Customer Enge Router, CE – пограничный маршрутизатор клиента.
- Provider Router, P - внутренний маршрутизатор магистральной сети провайдера.
- Provider Enge Router, PE - пограничный маршрутизатор сети провайдера.

Пограничные маршрутизаторы клиента служат для подключения сайта клиента к магистральной сети провайдера. Эти маршрутизаторы принадлежат сети клиента и ничего не знают о существовании VPN. К пограничным маршрутизаторам сети провайдера через маршрутизаторы CE сайты клиентов и внутренние маршрутизаторы сети провайдера. Взаимодействие маршрутизаторов CE и PE реализуется на основе стандартных протоколов стека TCP/IP.

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 удалось добиться преобразованием IP-адреса в VPN-IP-адрес и использованием протокола MP-BGP для работы с этими адресами. Считается, что CE-маршрутизатор относится к одному сайту, но 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.

Маршрутизаторы CE не обязаны поддерживать технологию многопротокольной коммутации, поддержка MPLS нужна только для внутренних интерфейсов PE маршрутизаторов и, конечно, для всех интерфейсов маршрутизаторов P.

По функциональному построению более сложными являются пограничные маршрутизаторы сети провайдера. На них возлагается

функция поддержки VPN, а именно: разграничение маршрутов и данных, поступающих от разных клиентов. Кроме того, эти маршрутизаторы служат оконечными точками путей LSP между сайтами заказчика.

Каждый PE-маршрутизатор должен поддерживать столько таблиц маршрутизации, сколько сайтов пользователей к нему подсоединено, то есть на одном физическом маршрутизаторе организуется несколько виртуальных. Причем 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.

Под каждый новый сайт клиента PE создает отдельную ассоциированную таблицу маршрутизации.

Каждой ассоциированной таблице маршрутизации в маршрутизаторе PE присваивается один или несколько атрибутов RT, которые определяют набор сайтов, входящих в конкретную VPN. Помимо этого, маршрут может быть ассоциирован с атрибутом VPN of Origin, однозначно идентифицирующим группу сайтов и соответствующий маршрут, объявленный одним из маршрутизаторов, находящихся в этих сайтах; и с атрибутом Site of Origin, идентифицирующим сайт, от которого маршрутизатор PE получил информацию о данном маршруте.

Через маршрутизаторы PE проходит невидимая граница между зоной клиентских сайтов и зоной ядра провайдера. По одну сторону располагаются интерфейсы, через которые PE взаимодействует с маршрутизаторами P, а по другую - интерфейсы, к которым подключаются сайты клиентов. С одной стороны на PE поступают

объявления о маршрутах магистральной сети, с другой стороны - объявления о маршрутах в сетях клиентов.

Ограничение области распространения маршрутной информации пределами отдельных VPN изолирует адресные пространства каждой VPN, позволяя применять в ее пределах как публичные адреса Интернет, так и частные (private) адреса. Всем адресам адресного пространства одной VPN добавляется префикс, называемый различителем маршрутов (Route Distinguisher, RD), который уникально идентифицирует эту VPN. В результате на маршрутизаторе PE все адреса, относящиеся к разным VPN, обязательно будут отличаться друг от друга, даже если они имеют совпадающую часть - адрес IP.

Обмен маршрутной информацией между сайтами каждой отдельной VPN выполняется под управлением протокола MP-BGP (Multiprotocol BGP).

MPLS не обеспечивает безопасность за счет шифрования и аутентификации, как это делает IPSec, но допускает применение данных технологий как дополнительных мер защиты. Провайдер MPLS может предлагать клиентам услуги гарантированного качества обслуживания при использовании методов Traffic Engineering или DiffServ.

Виртуальные сети VPN MPLS ориентированы на построение защищенной корпоративной сети клиента на базе частной сетевой инфраструктуры одной компании. Данный вариант организации сочетает в себе преимущества применения протокола IP с безопасностью частных сетей и предоставляемым качеством обслуживания, которые дает технология MPLS.

Сети MPLS VPN больше всего подходят для создания корпоративного пространства для электронной коммерции, обеспечивающего единую сетевую среду для подразделений

корпорации и организацию экстрасетей. Они также могут стать основой для электронной коммерческой деятельности предприятия.

3.4. Применение туннелей для VPN.

Протоколы защищенного канала, как правило, используют в своей работе механизм туннелирования. С помощью данной методики пакеты данных транслируются через общедоступную сеть как по обычному двухточечному соединению. Между каждой парой «отправитель–получатель данных» устанавливается своеобразный туннель – безопасное логическое соединение, позволяющее инкапсулировать данные одного протокола в пакеты другого.

Процесс туннелирования (или инкапсуляции) сводится к тому, что пакет протокола более низкого уровня помещается в поле данных пакета протокола такого же или более высокого уровня. Этот механизм используется для безопасности передачи данных через публичные сети путем упаковки пакетов во внешнюю оболочку. Туннель создается между двумя пограничными устройствами, которые размещаются в точках входа в сеть.

Технология туннелирования позволяет зашифровать исходный пакет целиком, вместе с заголовком, а не только его поле данных. Такой зашифрованный пакет помещается в другой пакет с открытым заголовком. Этот заголовок используют для транспортировки данных на участке общей сети. В граничной точке защищенного канала извлекается зашифрованный заголовок, который будет использоваться для дальнейшей передачи пакета.

Как правило, туннель создается только на участке сети общего пользования, где существует угроза нарушения конфиденциальности и целостности данных.

Помимо защиты передаваемой информации механизм туннелирования используют для обеспечения целостности и

аутентичности. При этом защита потока реализуется более полно. Туннелирование применяется также и для согласования разных транспортных технологий, если данные одного протокола транспортного уровня необходимо передать через транзитную сеть с другим транспортным протоколом.

Следует отметить, что процесс туннелирования не зависит от того, с какой целью он применяется.

Сам по себе механизм туннелирования не защищает данные от несанкционированного доступа или от искажений, он лишь создает предпосылки для защиты всех полей исходного пакета. Для обеспечения секретности передаваемых данных, пакеты на транспортном уровне шифруются и передаются по транзитной сети.

3.5. Сравнительный анализ туннелей MPLS и обычных туннелей.

Туннели MPLS позволяют передавать данные любого протокола вышестоящего уровня (например, IP, IPX, кадры Frame Relay,ячейки ATM), так как содержимое пакетов вдоль всего пути следования пакета остается неизменным, меняются только метки. В отличие от них, туннели IPSec поддерживают передачу данных только протокола IP, а протоколы PPTP и L2TP позволяют обмениваться данными по протоколам IP, IPX или Net BEUI.

Безопасность передачи данных в MPLS обеспечивается за счёт определённой сетевой политики, запрещающей принимать пакеты, снабжённые метками, и маршрутную информацию VPN-IP от непроверенных источников. Она может быть повышена использованием стандартных средств аутентификации и/или шифрования (например, шифрование IPSec).

Для безопасной передачи данных в протокол IP Security включены определенные процедуры шифрования IP-пакетов,

аутентификации, обеспечения защиты и целостности данных при транспортировке, вследствие чего, туннели IPSec обеспечивают надежную доставку информационного трафика.

Протокол L2TP поддерживает процедуры аутентификации, туннелирования информационного потока, а PPTP помимо данных функций снабжен и функциями шифрования.

Применение меток MPLS позволяет реализовать ускоренное продвижение пакетов по сети провайдера. Транспорт MPLS не считывает заголовки транспортируемых пакетов, поэтому используемая в этих пакетах адресация может носить частный характер. Содержимое пакетов не считывается и при передаче IP-пакетов по протоколам IPSec, PPTP, L2TP. Однако, в отличие от MPLS традиционные протоколы туннелирования для транспортировки IP-пакетов используют традиционную IP-маршрутизацию.

При выборе пути следования пакета в MPLS учитываются различные параметры, оказывающие влияние на выбор маршрута. Совместная работа технологии многопротокольной коммутации и механизмов Traffic Engineering позволяет для каждого туннеля LSP предоставить требуемый уровень качества обслуживания за счет процедуры резервирования ресурсов на каждом маршрутизаторе вдоль пути следования пакета. Помимо этого, появляется возможность отслеживать действительный маршрут, проходящий через сформированный туннель, возможность диагностики и административного контроля туннелей LSP.

Различные туннели, в соответствии с необходимым уровнем QoS между двумя точками поддерживает и протокол L2TP.

Технология VPN IPSec не поддерживает параметров качества обслуживания установленного соединения, а протокол PPTP поддерживает один единственный туннель между двумя точками.

Нельзя не отметить и тот факт, что весь трафик при использовании традиционных IP-туннелей следует до адресата вдоль одного и того и того же пути. Технология MPLS позволяет контролировать потоки, передаваемые по множеству всех имеющихся путей до адресата.

С точки зрения многоадресной рассылки стоит отметить, что ни одна из рассматриваемых технологий ее не поддерживает, но относительно MPLS-TE она находится в разработке.

MPLS VPN может быть создана для поддержки критически важных приложений на круглосуточной основе. В этом случае провайдер услуг определяет фиксированный путь на срок контракта с пользователем. В случаях сбоя или отсутствия пропускной способности приоритет отдается более важным потокам (с более высоким приоритетом).

Одна из функций MPLS - объединение виртуальных каналов, когда несколько туннелей MPLS объединяются для создания единого туннеля. Такая структура распространяет VPN на базе MPLS в сети оператора на сеть внутри офиса и прямо до сервера или клиента. При подобном расширении VPN оператору может быть предоставлена ответственность по управлению для обеспечения непрерывного контроля за CoS из конца в конец.

Глава 4. Функциональная модель фрагмента VPN на основе туннелей MPLS.

В предыдущих главах было дано общее понятие виртуальных частных сетей, теперь перейдем к рассмотрению функциональной модели участка виртуальной частной сети, построенной на основе технологии MPLS.

4.1. Базовый вариант создания VPN на основе туннелей MPLS.

На рисунке 5 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.

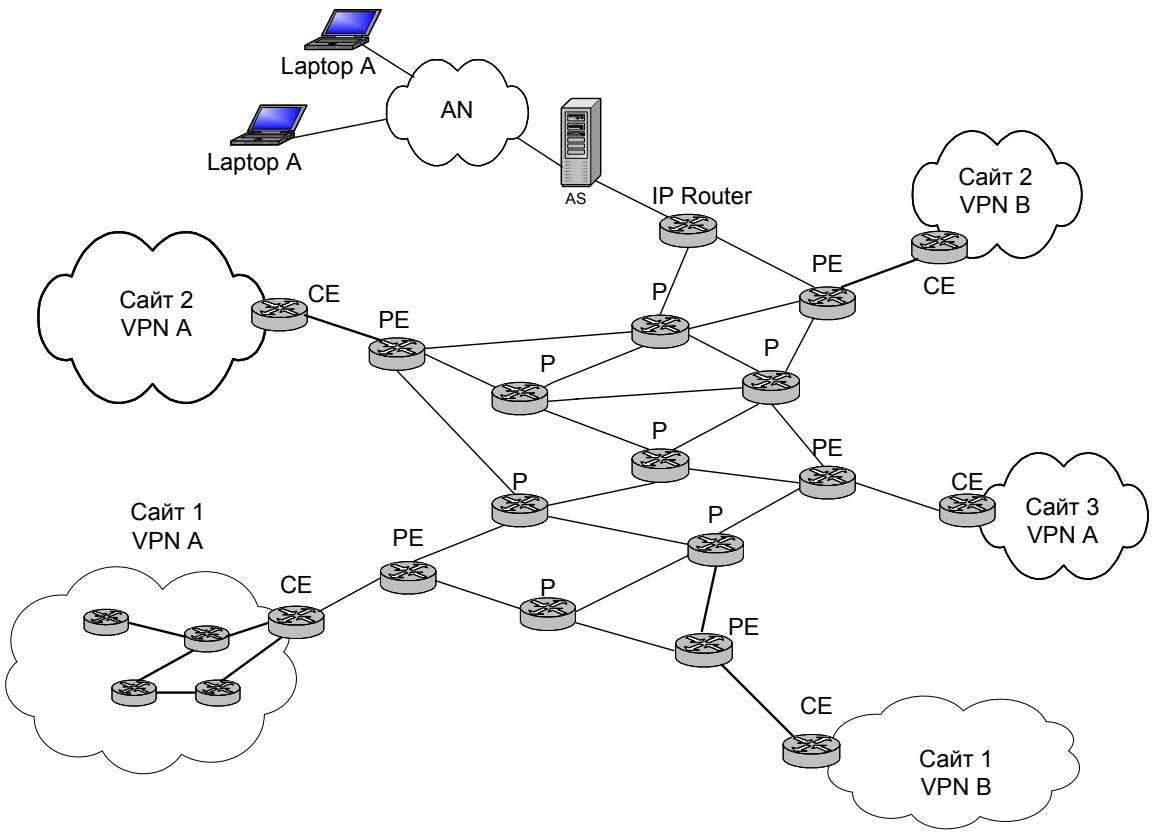


Рис 5. Виртуальная частная сеть на базе технологии MPLS.

4.1.1. 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. 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, о которых упоминалось выше. В принципе, маршрутизатор PE может объявлять любой маршрут, содержащийся в его таблице маршрутизации, ассоциированной с сайтом, содержащим рассматриваемый CE. Но есть одно ограничение: маршрут, имеющий атрибут Site of Origin, никогда не должен объявляться CE-маршрутизатором, принадлежащим сайту, идентифицируемому этим атрибутом.

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 системы ASBR, а затем этот маршрутизатор должен будет передавать маршрутные объявления ASBR, находящемуся в другой автономной зоне по протоколу EBGP.

4.1.2. 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 или CR-LDP.

При этом, если путь прокладывается при помощи протокола LDP, то обслуживаться он будет согласно модели Best Effort (с максимально возможным качеством). 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.

4.1.3. 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.

4.2. Сценарий обмена сообщениями для установления TE-туннеля для VPN и передачи по нему трафика данных.

Рассмотрим сценарий обмена сообщениями на примере конкретной сети.

Как уже говорилось выше, управляющий поток подразделяется на два потока:

- поток обмена маршрутной информацией между маршрутизаторами PE и CE и между маршрутизаторами PE.
- управляющий поток установления LSP-пути.

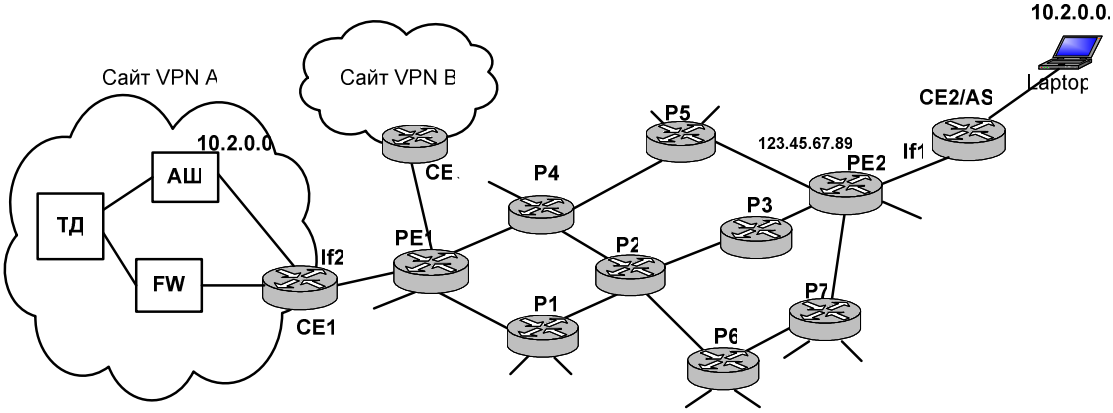


Рисунок 6 Структура виртуальной частной сети.

Управляющий поток обмена маршрутными объявлениями.

Маршрутизатор CE2 объявляет префиксы маршрута связанному с ним маршрутизатору пограничной сети провайдера PE2. Это объявление содержит его IP-адрес удаленного пользователя, входящего в виртуальную частную сеть VPNA и адрес внешнего интерфейса маршрутизатора CE2 (if1), маршрут транслируется при помощи протокола внутренней маршрутизации IGP (например, OSPF или IS-IS).

Net = 10.2.0.0.

Next Hop = CE2

PE2 проверяет соответствие этого маршрута локально сконфигурированным правилам импорта и, если маршрут

удовлетворяет данным правилам, вносит его в соответствующую таблицу VRF.

Следует уточнить, что маршрутное объявление по протоколу MP-BGP посылается только тем маршрутизаторам PE, которые прописаны в конфигурационных параметрах маршрутизатора-отправителя в качестве соседей.

Перед тем, как направить маршрутное объявление выходному маршрутизатору PE1, PE2 транслирует его в формат VPN-IP для чего он выполняет следующие действия:

- к адресу добавляет различитель маршрутов RD.
- изменяет поле Next Hop, записывая в него адрес своего внешнего интерфейса.
- назначает метку VPN, указывающую на виртуальную частную сеть VPNA и на интерфейс маршрутизатора PE2, к которому подключен сайт.
- назначает атрибуты RT, Site of Origin, VPN of Origin

Таким образом, маршрутное объявление по протоколу MP-BGP, будет иметь следующий вид:

VPN-IP = 123.45.67.89:1:10.2.0.0

Next Hop = 123.45.67.89

Lvpn=7

RT=A.

Когда выходной маршрутизатор PE1 получает маршрут VPN-IPv4, он проверяет атрибут RT, содержащийся в маршруте на совпадение с политикой импорта всех своих VFR, в данном случае VRF1A и VRF1B. Значение атрибута route-target равно A, поэтому маршрут добавляется (после преобразования в формат IPv4 путем удаления различителя маршрутов RD) только в таблицу VRF2A, так как для нее определена политика импорта A. Таблица VRF2B остается

в неизменном виде, так как ее политика импорта говорит о том, что в нее должны помещаться только маршруты с атрибутом route-target B.

В данном примере маршрутизаторы CE1 и PE1 находятся в разных автономных зонах, поэтому обмен маршрутными объявлениями между данными маршрутизаторами осуществляется при помощи протокола EBGP.

После того, как маршрутизатор PE1 передаст маршрутное объявление маршрутизатору CE1, таблица маршрутизации CE1 будет содержать следующую информацию:

Network = 10.2.0.0.

Next Hop = PE1

Interface = if 2

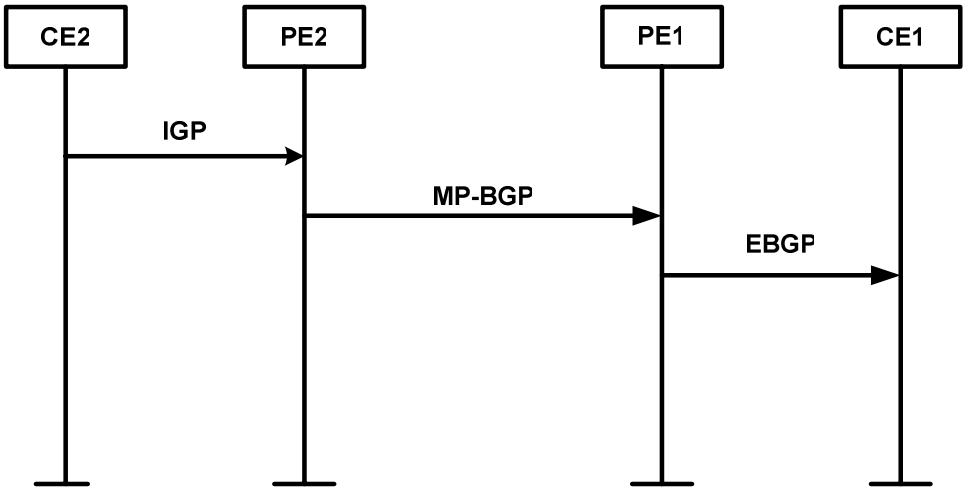


Рисунок 7 Обмен маршрутной информацией.

Процесс управления установлением туннелей LSP.

Перед созданием LSP-TE-туннеля в сети MPLS работает протокол LDP, благодаря которому создается топологическая карта

сети, распространяются атрибуты ресурсов и устанавливаются обычные LSP-туннели.

Администратор сети провайдера собирает статистику по этим туннелям, после чего, в соответствии с договоренностью об уровне предоставляемого качества обслуживания, он принимает решение о создании TE-туннелей с различным уровнем качества обслуживания.

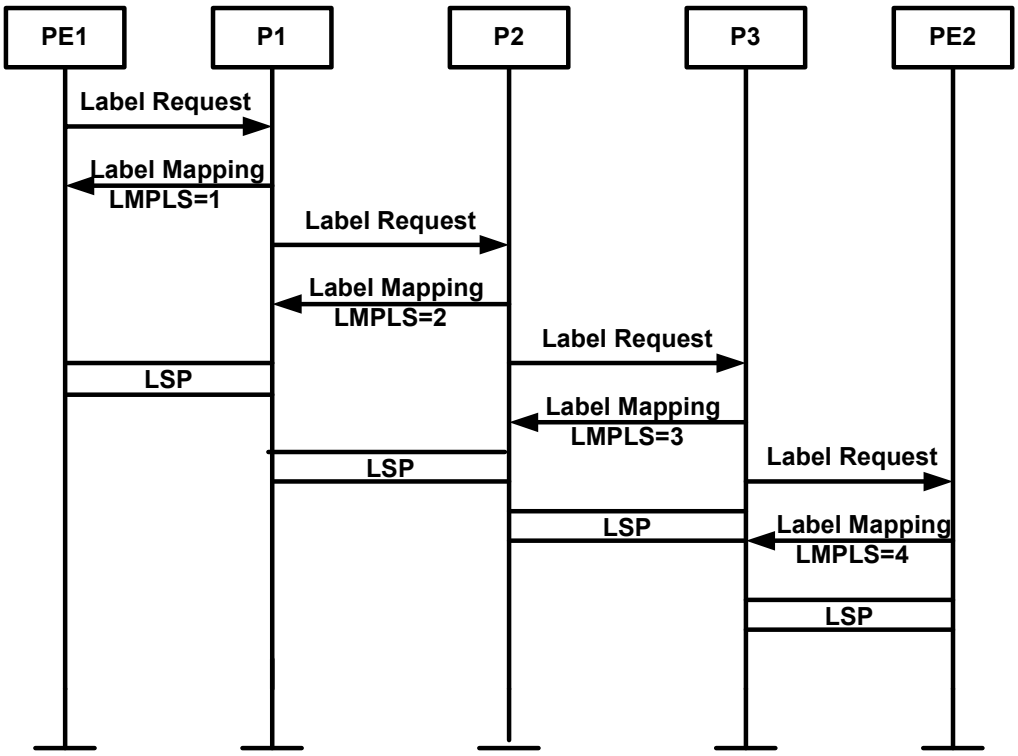


Рисунок 8. Установление коммутируемого по меткам тракта.

Установление TE-туннелей.

Для установления TE-туннеля администратор магистральной сети на основе статистических данных о сети и туннелях LSP определяет маршрут, который удовлетворит затребованному уровню QoS и формирует этот путь путем ввода объекта ERO в сообщение Path, в котором прописывает явный маршрут. В данном случае ERO содержит следующую запись: P3, P2, P1, PE1.

Сообщение Path несет в себе объекты: Label Request, Session, Sender Template, Time Values, Sender Tspec.

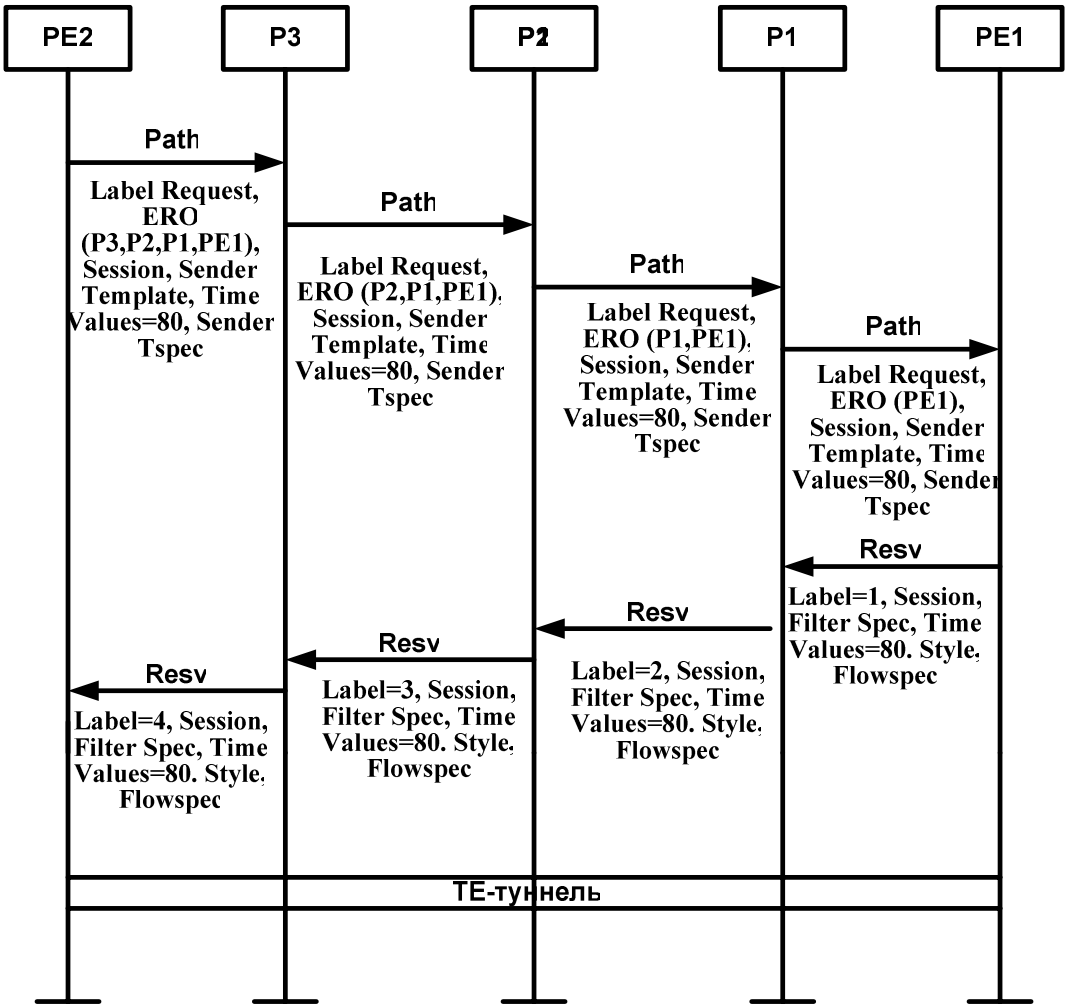


Рисунок 9. Установление TE-туннеля.

Каждый маршрутизатор, получивший сообщение Path, пересылает его на следующий маршрутизатор в соответствии с записью в объекте ERO и фиксирует у себя адрес маршрутизатора, от которого это сообщение было получено. Пройдя, таким образом, через маршрутизаторы P3, P2, P1 сообщение Path поступает на маршрутизатор PE1. Этот маршрутизатор, приняв данное сообщение, определяет наличие требуемых ресурсов и правомерность запроса и, если запрос правомерен и требуемые ресурсы имеются, PE1 резервирует их для данного туннеля, после чего передает сообщение

Resv, запроса резервирования ресурсов, маршрутизатору P1. Сообщение Resv, содержащее объекты: Label, Session, Filter Spec, Time Values. Style, Flowspec, следует в направлении, обратном направлению распространения сообщения Path, т.е., проходит через маршрутизаторы P1, P2, P3 и PE2. При этом, на каждом из этих маршрутизаторов производится резервирование ресурсов.

Таким образом организуется TE-туннель, для которого на всех маршрутизаторах, через которые этот туннель проходит, зарезервированы определенные ресурсы для обеспечения требуемого качества обслуживания.

Продвижение трафика данных.

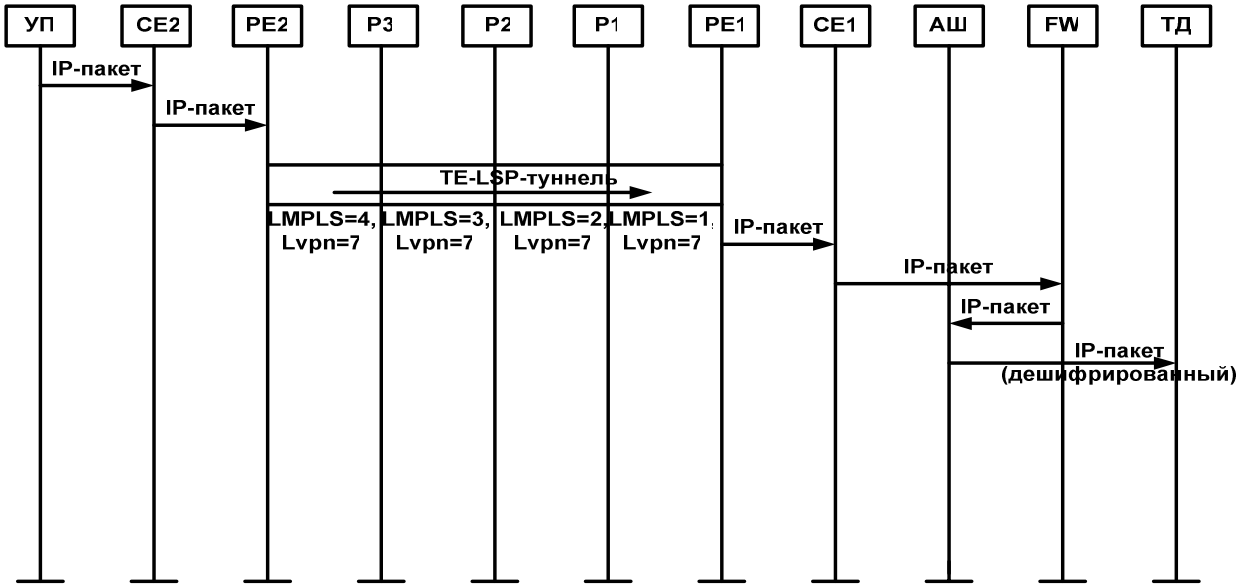


Рисунок 10. Передача информационного трафика

Рассмотрим процесс передачи трафика данных от удаленного пользователя в точку доступа, находящуюся на сайте, принадлежащем VPNA через магистральную сеть провайдера MPLS-TE.

Удаленный пользователь посылает IP-пакет.

В первую очередь этот пакет попадает на сервер доступа (AS), реализованный на маршрутизаторе CE2. Сервер доступа проводит аутентификацию и авторизацию пользователя, после чего, по таблице маршрутизации CE2 определяется дальнейший путь следования пакета и посылает его на маршрутизатор PE2.

При поступлении IP-пакета PE2 обращается к таблице VRFA и назначает этому пакету метку виртуальной частной сети Lvpn=7. Далее маршрутизатор обращается к таблице LIB, в которой в соответствии с требуемым уровнем качества обслуживания (ToS) выбирается TE-туннель и назначается метка MPLS.

Продвижение пакета по сети провайдера происходит на основании метки верхнего уровня, роль которой отводится метке LMPLS. Каждый раз, когда пакет проходит очередной маршрутизатор P вдоль туннеля, метка LMPLS анализируется и заменяется новым значением. И только после достижения конечной точки TE-туннеля, маршрутизатора PE1, из стека извлекается метка Lvpn=7.

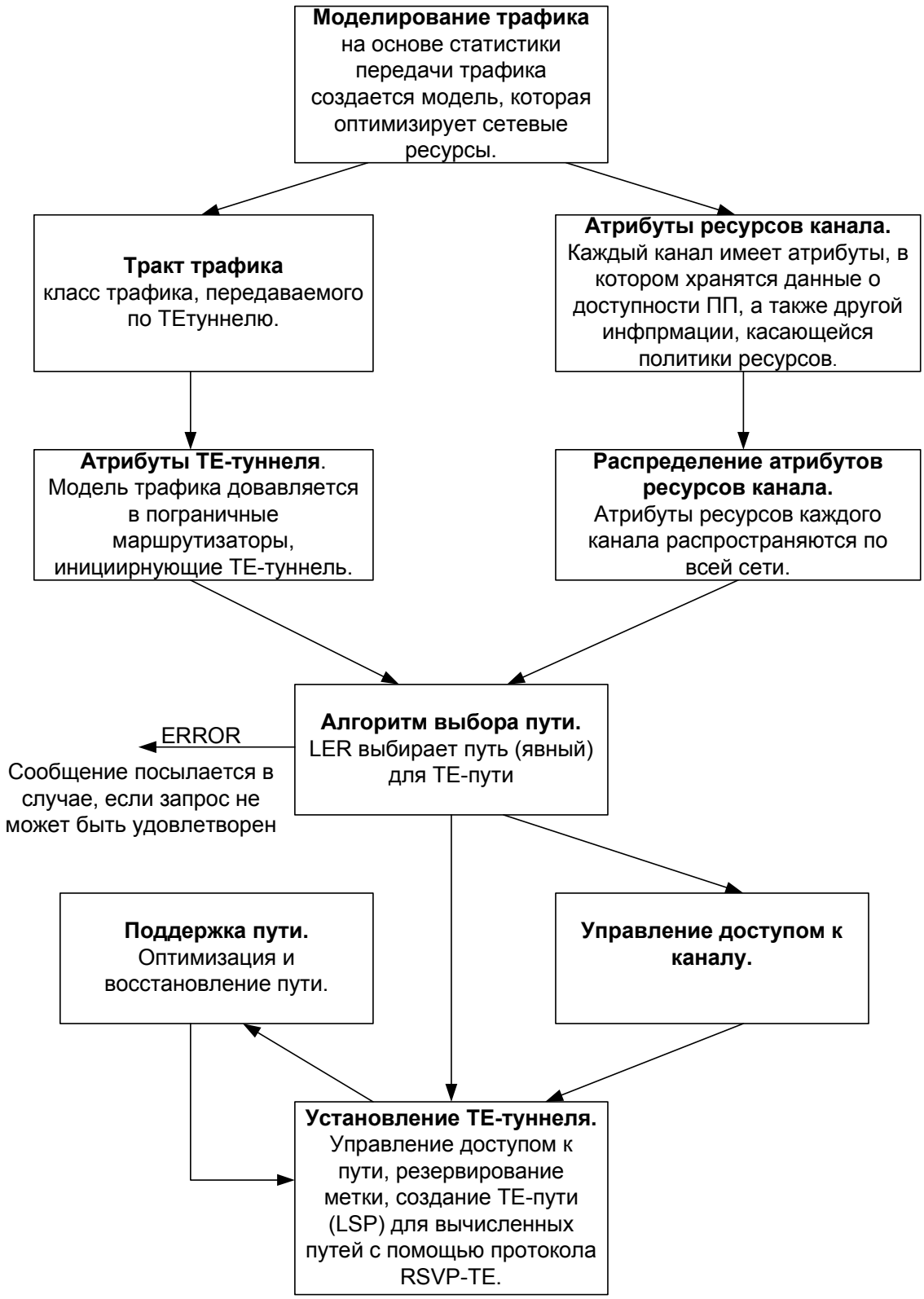
Дальнейшее продвижение пакета основывается на этой метке. В зависимости от ее значения пакет направляется на тот или иной выходной интерфейс маршрутизатора PE1: маршрутизатор PE1 обращается к таблице VRF VPNA, связанной с данным интерфейсом и извлекает запись о маршруте к пункту назначения.

Последующее продвижение пакета к маршрутизатору CE1 осуществляется при помощи стандартного протокола IP.

Когда стандартный IP-пакет поступает на маршрутизатор CE1 по таблице маршрутизации осуществляется поиск маршрута и пакет поступает на FW. Брандмауэр проводит фильтрацию трафика, поступающего от провайдера. После фильтрации пакета он дешифрируется и поступает на ТД.

4.3. Диаграмма установления ТЕ-туннеля.

На рисунке 11 представлен алгоритм установления ТЕ-туннеля.



Заключение.

В дипломной работе, посвященной разработке функциональной модели участка VPN на основе туннелей MPLS были рассмотрены современные технологии построения виртуальных частных сетей, проведен сравнительный анализ туннелей, построенных на базе технологии многопротокольной коммутации на основе меток с туннелями на базе таких технологий как IPSec, L2TP, PPTP.

В результате проведенного анализа можно сделать вывод о том, что технология VPN MPLS на сегодняшний день является ведущей технологией построения виртуальных частных сетей. Она обладает широкой масштабируемостью, гибкостью, 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 и механизмов Traffic Engeenering позволяет предоставить для каждого информационного потока безопасный туннель с гарантированным уровнем качества обслуживания, что имеет большое значение в свете перехода к мультисервисным сетям.

Использование разработанной в данной работе функциональной модели участка VPN MPLS и алгоритма установления TE-туннеля позволяет продолжить более детальное рассмотрение данного варианта организации виртуальных частных сетей.

Литература.

1. Гольдштейн А.Б. Построение виртуальных частных сетей (VPN) на базе технологии MPLS//54 Научно-техническая конференция профессорско-преподавательского состава, научных сотрудников и аспирантов. 28 января – 1 февраля 2002 года/Материалы. СПбГУТ.-СПб, 2002. – с.18.
2. Гольдштейн А.Б. Построение виртуальных частных сетей VPN на базе технологии MPLS//57-я Научная сессия, посвященная Дню радио. 15-16 мая 2002 г., Москва. Труды. Том 1/М.: МТУСИ, 2002. – с.54 – 56.
3. Гольдштейн А.Б.. Проблемы перехода к мультисервисным сетям// Вестник связи. -М., 2002. №12.-с.26-32.
4. Гольдштейн А.Б. Разработка модели MPLS /57 Научно-техническая конференция студентов, аспирантов и молодых специалистов 19-23 мая 2003. СПбГУТ.-СПб, 2003.
5. Goldstein A., Yanovsky G. Traffic Engineering in MPLS Tunnels// International Conference on "Next Generation Teletraffic and Wired/Wireless Advanced Networking (NEW2AN'04)". February 02-06, 2004.
6. Гольдштейн А.Б. Аналитическая модель для расчета механизма туннелирования в MPLS/56-я научно-техническая конференция профессорско-преподавательского состава, научных сотрудников и аспирантов/СПбГУТ. -СПб., 2004.-с.5.
7. Гольдштейн А.Б. Механизм эффективного туннелирования в сети MPLS// Вестник связи. –М ., 2004. №2. – с. 48-54.
8. Гольдштейн А.Б. Исследование методов расчета механизма туннелирования в MPLS /58 Научно-техническая конференция студентов, аспирантов и молодых специалистов. 17-21 мая 2004. СПбГУТ.-СПб, 2004.
9. Гольдштейн Б.С., Пинчук А.В., Суховицкий А.Л. IP телефония// М.: Радио и связь, 2003.
10. Олифер В., Олифер Н. Новые технологии и оборудование// СПб: БХВ – Санкт-Петербург, 2000.
11. Остерлох Х. Маршрутизация в IP-сетях// М.: DiaSoft, 2002.
12. Шринивас Вагешна Качество обслуживания в сетях IP. // М.: Вильямс, 2003.
13. www.loniis.ru
14. www.cisco.com
15. www.networld.ru
16. ccc.ru
17. www.comptek.ru
18. www.poplar.ru

19. www.osp.ru
20. www.book.itep.ru

ОТЗЫВ

на дипломную работу студентки
факультета СС, СК и ВТ
СПбГУТ им. проф. М.А. Бонч-Бруевича

Бородиной Людмилы Владимировны.

тема работы: ***"Анализ применения туннельного эффекта технологии MPLS для построения каналов VPN".`***

Возрастающий спрос на организацию виртуальных частных сетей приводит к необходимости поиска технологий построения сетей VPN, гарантирующих конфиденциальность и безопасность ресурсов корпоративных сетей, а также, обеспечивающих обмен информацией между территориально распределенными филиалами предприятий с необходимым уровнем качества обслуживания. В данной дипломной работе проведен анализ применения туннелей MPLS для построения каналов VPN, а также разработана функциональная модель участка VPN на основе туннелей MPLS.

Отличительной особенностью работы следует считать последовательное прохождение всех этапов выполнения технического задания. Дипломница, опираясь на широкую информационную базу, провела сравнительный анализ туннелей IP и туннелей MPLS, провела анализ туннельного эффекта MPLS для построения каналов VPN, разработала функциональную модель участка VPN MPLS.

Представленный материал свидетельствует о том, что на этапах работы Бородина Людмила Владимировна умело и грамотно применила большое количество специальной литературы. Данный подход позволил ей решить поставленные задачи на высоком уровне и продемонстрировать качество специальной подготовки.

Пояснительная записка выполнена аккуратно, в ней учтены основные требования к составу и структуре дипломной работы. Требования технического задания выполнены полностью.

В целом дипломная работа отвечает всем предъявленным требованиям и заслуживает отличной оценки, а Бородина Людмила Владимировна достойна присвоения квалификации инженера по специальности «Сети связи и системы коммутации».

Начальник сектора ЛОНИИС ***Гольдштейн А. Б.***