

**МИНИСТЕРСТВО ПО РАЗВИТИЮ ИНФОРМАЦИОННЫХ
ТЕХНОЛОГИЙ И КОММУНИКАЦИЙ РЕСПУБЛИКИ УЗБЕКИСТАН**

**НУКУССКИЙ ФИЛИАЛ ТАШКЕНТСКОГО УНИВЕРСИТЕТА
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
ИМЕНИ МУХАММАДА АЛ-ХОРАЗМИЙ**

Кафедра «Информационные технологии»

направление Компьютерный инжиниринг («Компьютерный инжиниринг»)

Допуск к защите
Заведующий кафедрой
Турениязова А.

«____» _____ 2018 г.

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

на тему

«Принципы работы транспортных сетей MPLS»

Выполнил:

Калмуратов Н.

Научный руководитель:

Шарапова И.

НУКУС - 2019 г.

Содержание

Введение	
1. ОБЗОР ПОСТАВЛЕННОЙ ЗАДАЧИ И ПУТИ ЕЕ РЕШЕНИЯ.	
1.1. Сравнительная оценка возможностей технологии MPLS....	5
1.2. Проблемы качества обслуживания (QoS) на магистральных участках сетей, стоящие перед современными операторами связи...	12
1.3. Обеспечение совместимости технологии MPLS с другими технологиями современными операторами связи.....	15
2. ОСНОВНЫЕ ПРИНЦИПЫ РАБОТЫ И ТЕХНОЛОГИЯ MPLS.	
2.1. Введение в технологию MPLS.....	16
2.2. Принципы работы MPLS.....	18
2.3. Принцип коммутации.....	20
2.4. Элементы архитектуры.....	22
2.5. Выбор маршрута.....	26
2.6. Управление трафиком в технологии MPLS.....	30
2.7. Будущее технологии MPLS.....	38
3. ПРОЕКТИРОВАНИЕ ТЕХНОЛОГИИ MPLS НА ВИРТУАЛЬНОЙ МАШИНЕ.	
3.1. Принципы маршрутизации.....	40
3.2. Обзор OSPF.....	43
3.3. Настройка технологии OSPF на виртуальной машине.....	49
Заключение.....	5
Список литературы.....	59

Введение

Значительные неиспользуемые резервы для роста объемов и расширения сферы услуг сохраняются сегодня в строительстве, на транспорте, в финансово-банковской и информационно-коммуникационной сферах, медицинском и коммунально-бытовом обслуживании населения и особенно в сельской местности. По уровню развития сферы услуг, количеству и качеству предоставляемых услуг мы еще серьезно отстаем от экономически развитых стран[1].

В целях формирования национальной системы информатизации, массового внедрения и использования во всех сферах экономики и жизни общества современных информационных технологий, средств компьютерной техники и телекоммуникаций, наиболее полного удовлетворения растущих информационных потребностей граждан, создания благоприятных условий для вхождения в мировое информационное сообщество и расширения доступа к мировым информационным ресурсам[2].

Широкое распространение Интернета, использование IP-ориентированных приложений и технологии передачи голоса и видео по сетям данных способствовали мощному развитию мультисервисных операторских IP-сетей. Предоставление только услуги канала связи первого и второго уровней (выделенные линии, frame relay, АТМ (Asynchronous Transfer Mode) и др.) существенно ограничивает набор услуг провайдера в условиях высококонкурентного рынка телекоммуникаций. Сегодня услуги различных IP-сервисов являются своего рода стандартом, причем ведущие операторы кроме доступа в Интернет уже обеспечивают функции пакетной телефонии, телевещания и видео по запросу, виртуальных частных сетей.

Архитектура MPLS, наиболее эффективная для передачи IP-трафика и работы в среде IP-ориентированных приложений, разрабатывалась и

позиционируется для построения высокоскоростных магистральных сетей, обеспечивает экономичность и безопасность организации VPN соединений. Гибкие и высоко масштабируемые сети MPLS реализуют мощные функции управления IP-трафиком и позволяют передавать его на высокой скорости и в большем объеме.

MPLS является масштабируемым и независимым от каких-либо протоколов механизмом передачи данных. В сети, основанной на MPLS, пакетам данных присваиваются метки. Решение о дальнейшей передаче пакета данных другому узлу сети осуществляется только на основании значения присвоенной метки без необходимости изучения самого пакета данных. За счет этого возможно создание сквозного виртуального канала, независимого от среды передачи и использующего любой протокол передачи данных. MPLS позволяет достаточно легко создавать виртуальные каналы между узлами сети. Технология позволяет инкапсулировать различные протоколы передачи данных.

Целью данной выпускную квалификационную работы является создание сети MPLS, основных принципов работы технологии MPLS (Multi Protocol Label Switching – быстрая коммутация пакетов в многопротокольных сетях, основанная на использовании меток).

Задачей данной выпускную квалификационную работы является, создание сети MPLS призванного помочь оператору в анализе наиболее оптимальной конфигурации своей сети, улучшении её отдельных участков и необходимого для построения сети на основе технологии MPLS. Работа предназначена также для организации процесса обучения специалистов основам сбора статистических данных при работе в сетях MPLS с их последующим анализом.

1. ОБЗОР ПОСТАВЛЕННОЙ ЗАДАЧИ И ПУТИ ЕЕ РЕШЕНИЯ

1.1. Сравнительная оценка возможностей технологии MPLS

Характеристики современного трафика магистральных сетей.

Многопротокольная коммутация информационных потоков в соответствии с метками (Multiprotocol Label Switching, MPLS) рассматривается как перспективная, хотя и не единственная основа для конвергенции услуг и построения мульти сервисных сетей следующего поколения (NGN), в которых станет возможна передача разнородного трафика через интегрированную телекоммуникационную инфраструктуру вместо нескольких различных сетей.

Принятие MPLS в качестве унифицирующей, замещающей технологии должно привести к значительному упрощению сетевых инфраструктур и управления ими. Внедрение MPLS позволяет повысить уровень сервиса, предоставлять востребованные услуги на базе IP (с гарантированным уровнем качества) и услуги конвергентных сетей для корпоративных клиентов, включая создание виртуальных частных сетей (VPN) и передачу голоса поверх IP (VoIP).

Инфраструктура MPLS VPN дает возможность соединять узлы по схеме «любой с любым» независимо от технологии доступа (Frame Relay, выделенная линия, DSL или Ethernet), повышает производительность, масштабируемость IP и надежность маршрутизации в приложениях Triple Play (голос, данные, видео).

С MPLS хорошо сочетается Ethernet — благодаря такой комбинации открывается возможность экономичного предоставления целого комплекса услуг и внедрения широкополосных приложений в городских сетях и сетях доступа. На основе проведенного сравнительного анализа приведены достоинства и недостатки технологии передачи данных[4].

Достоинства и недостатки технологий MPLS

Достоинства:

Отделение выбранного маршрута от анализа IP-адреса (дает возможность предоставлять широкий спектр дополнительных сервисов при сохранении масштабируемости):

- ✓ Ускоренная коммутация (сокращает время поисков в таблицах);
- ✓ Гибкая поддержка QoS интегрируемых сервисов VPN;
- ✓ Эффективное использование явного маршрута;
- ✓ Разделение функциональности между ядром и граничной области сети;
- ✓ Высокую эффективность использования полосы пропускания (малый размер заголовка пакетов);
- ✓ Эффективность при перегрузках и отказах элементов.

Недостатки:

- ✓ В MPLS нет понятия безопасности в отличие от ATM, где безопасность определяется на логическом уровне;
- ✓ Приоритетом MPLS является быстрота продвижения пакета, а не QoS;
- ✓ Не всегда совместима с оборудованием разного производства.

Сравнительный анализ показывает, что технология MPLS позволяет поддерживать качество обслуживания (QoS) и безопасность на уровне ATM, сохраняя гибкость и масштабируемость присущие технологии IP. Появления технологии MPLS определяет направление интеграции IP маршрутизации и ATM коммутации в общую IP / MPLS сеть. Таким образом технология MPLS становится единой технологической платформой для создания и развития современных инфокоммуникационных сетей[25].

Работа по созданию сетей следующего поколения (NGN) на основе технологии MPLS. В настоящее время большинство операторов связи делают ставки на использование технологии MPLS в качестве базовой

технологии передачи трафика в своих сетях не только по вышеозначенным причинам, но также и с точки зрения создания основы для построения в ближайшем будущем сетей следующего поколения (Next Generation Networks, NGN). Современные требования к сетям связи следующего поколения заключаются в возможности оптимальной передачи голосового трафика, трафика данных, создания и предоставления новых сервисов, снижения расходов на капитальное строительство и операционных издержек по сравнению с существующими сетями связи.

В настоящее время развернуто значительное количество традиционных сетей связи, поэтому при строительстве сети NGN целесообразно учитывать возможности существующего оборудования для организации эволюционного перехода к сетям связи следующего поколения.

В общем случае, сеть связи состоит из трех уровней:

✓ Уровень приложений. Отвечает за предоставление конечному пользователю информационных услуг и от того, насколько эти услуги будут ему интересны, зависит дальнейшее развитие сети. Серверы, обеспечивающие предоставление услуг, могут находиться как внутри, так и за пределами самой сети (различные серверы).

✓ Уровень управления сервисами. Отвечает за маршрутизацию вызовов, обработку сигнализации и непосредственное управление потоками.

✓ Транспортный уровень. Отвечает за передачу информации конечному пользователю и состоит из высокоскоростного ядра пакетной сети (например, сети MPLS) и уровня доступа, который обеспечивает непосредственное подключение конечных пользователей к сети[15].

Построение виртуальных частных сетей (VPN) на основе технологии MPLS. Сегодня сеть Интернет выросла до огромных размеров, превратившись в фактически неиссякаемый источник информации почти обо всех, абсолютно разных, областях нашей жизни. Кроме того, это быстрый и надежный способ общения. Но, к сожалению, достоинства сети Интернет

являются и ее недостатками. Так, открытость сети для подключения новых компьютеров и возможность доступа к информации, передаваемой в сетевых пакетах, делают данные пользователей Интернет незащищенными. Это может быть неприятно, даже если речь идет об общении с другом, но, когда стоит вопрос о передаче конфиденциальной информации, такое «прослушивание» просто недопустимо. Особую актуальность это приобрело в последнее время вследствие развития электронной коммерции, более частого использования оплаты услуг через сеть Интернет, интенсивного общения между людьми в различных частях сети[18].

Новейшей концепцией в этой области является концепция виртуальных частных сетей (VPN, рис.1). Основная идея ее такова: сетью объявляется некоторый набор компьютеров, которые не обязательно должны находиться в одном месте, а в качестве каналов передачи данных используются уже существующие (отсюда и слово «виртуальные») каналы Интернет. При этом информация передается в зашифрованном виде (отсюда слово «частные»). Схематически это может быть реализовано следующим образом: на каждом из компьютеров будущей сети устанавливается программа-клиент. Целью программ-клиентов является как минимум выполнение функций защиты и шифрования информации. Какой-либо выделенный компьютер становится сервером, откуда возможно управление сетью и наблюдение за ее работой. В зависимости от сложности программ пользователям сети становятся доступны различные наборы дополнительных сервисов, таких как защищенная почта, защищенная передача электронных подписей и многое другое.

Данные сети имеют целый ряд преимуществ. Например, нет необходимости построения каких-либо новых сетей и прокладки новых каналов связи, что существенно экономит средства компании, поскольку существующие каналы сети Интернет являются весьма дешевым средством передачи данных.

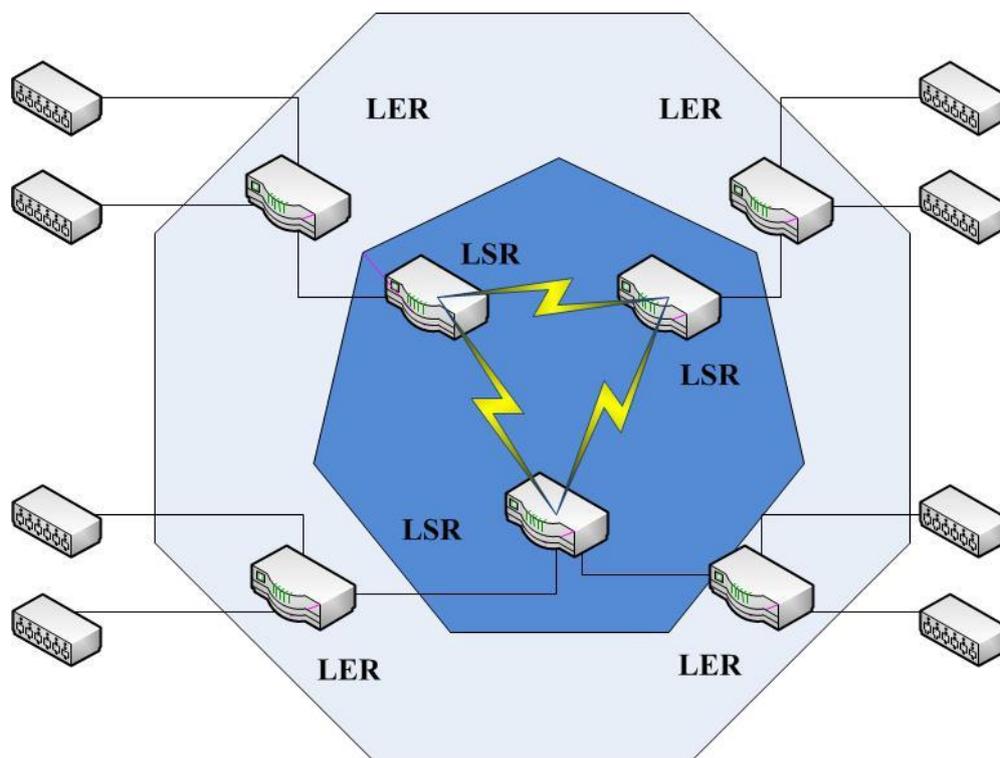


Рис. 1. Топология сети MPLS VPN

Одной из наиболее распространенных технологий построения виртуальных частных сетей является технология MPLS. Существенными отличительными свойствами виртуальной частной сети, построенной на основе технологии MPLS, являются:

- ✓ Независимый выбор сетевых технологий: выбор ограничивается только возможностями производителей оборудования.
- ✓ Независимая система адресации. В частных сетях нет ограничений на выбор адресов: они могут быть любыми.
- ✓ Предсказуемая производительность. Собственные каналы связи гарантируют заранее известную пропускную способность между узлами предприятия (для глобальных соединений) или коммуникационными устройствами (для локальных соединений).
- ✓ Максимально возможная безопасность. Отсутствие связей с внешним миром ограждает от атак извне и существенно снижает вероятность "прослушивания" трафика по пути следования.

На сегодняшний день, помимо вышеперечисленных свойств, заказчики сетевых решений требуют от современных операторов обеспечения мультисервисности, то есть предоставления наибольшего числа услуг из всех возможных в рамках единой сети[7].

Мультисервисный доступ в сетях MPLS. Концепция мультисервисности заключается в следующем (рис. 2): сокращается до минимума количество устройств, обеспечивающих разнотипные услуги (телефония, видеоконференции, телевидение, информационное обеспечение и др.). Данные устройства помещаются в «черный ящик», содержащий различного вида коммутаторы и другие аппаратные средства обработки трафика (например, пограничные коммутаторы LER сети MPLS, модули VoIP и т.д.).

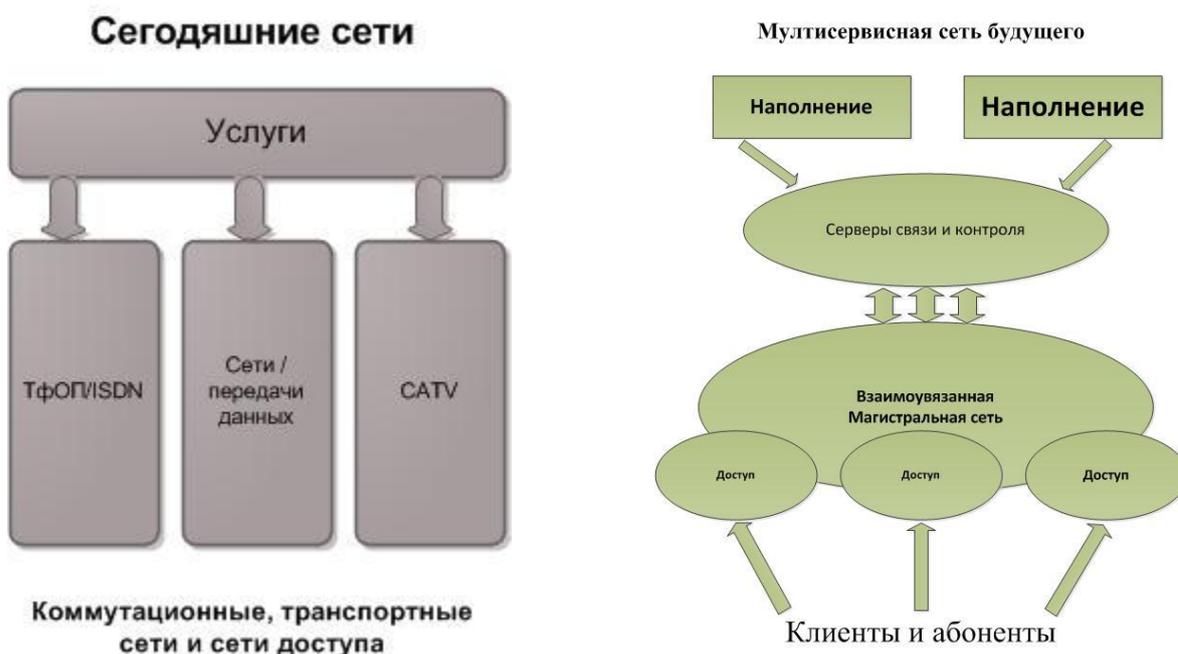


Рис. 2. Сравнение сегодняшних сетей и мульти сервисных сетей будущего

Благодаря поддержке технологий ATM, Frame Relay, MPLS, маршрутизации IP, мульти сервисные функции современных магистральных и пограничных коммутаторов помогают консолидировать сети разного типа и сокращать затраты на предоставление услуг посредством достаточно небольшого набора телекоммуникационных устройств. Одной из важных черт мульти сервисных сетей IP нового поколения является поддержка качества (Quality of Service, QoS), без чего невозможно внедрение услуг «голос по IP» и «видео по запросу». Аналитики ожидают увеличения расходов на технологии нового поколения, позволяющие объединять потоки голоса и данных в одной сети.

Традиционные операторы связи видят, что интенсивное развитие Интернет - технологий приводит к резкому возрастанию объема данных, передаваемых по сетям. Попытки удовлетворить растущий спрос приводят к переходу на мульти сервисные сетевые платформы и конвергенции трафика разных типов (данных, голоса и видео) в рамках единой пакетной инфраструктуры. Обладающая вышеперечисленными возможностями транспортная сеть на базе технологии MPLS, в полной мере соответствует предъявляемым сетевыми операторами требованиям по организации на ее основе широкого спектра новейших услуг, как для корпораций, так и для частных лиц, предоставляет средства управления передачей трафика и многое другое.

Большой процент роста трафика данных в сочетании с глобальной децентрализацией рынка связи вызвал к жизни два явления:

✓ Перед традиционными сервис - провайдерами стоит задача внедрения инфраструктуры передачи данных при сохранении огромных инвестиций, сделанных ранее в традиционные технологии коммутации и передачи голоса. Этим провайдерами становится все труднее передавать возрастающие объемы данных по малоэффективным сетям с коммутацией каналов. Чтобы выжить в конкурентной борьбе, традиционным операторам связи приходится

либо снижать тарифы, разрабатывать планы перехода на технологию IP, закупать и разворачивать новые IP-сети, либо быстро создавать и предлагать абонентам новые дифференцированные услуги с тем, чтобы крепче привязать заказчиков к старым технологиям связи. Технология MPLS позволяет организовать работу в магистральной сети с использованием элементов других транспортных технологий. Постепенное внедрение решает проблему одновременной замены дорогостоящего сетевого оборудования и, вместе с тем, предоставляет возможность создания на основе сетей MPLS качественно о концептуально новых услуг.

✓ Новые конкурентные сервис - провайдеры имеют уникальную возможность выйти на рынок с новыми более эффективными (и менее дорогими) сетями, такими как, например MPLS сети, позволяющими передавать большие объёмы данных по тарифам, которые намного меньше традиционных.

По мере того, как IP-технологии получают возможность беспрепятственной передачи голоса, данных и видео, различия между сетями теряют свое значение. В конечном итоге сеть становится стандартным продуктом. Для конкурентоспособной борьбы в Интернет – экономике крайне важно будет предлагать новые услуги, выгодно отличающие компанию от конкурентов. Те, кто будет следовать за другими, и повторять чужие подходы, а также владельцы базовых сетей местной и дальней связи и сетей передачи данных потеряют доходы и станут менее конкурентоспособными[6].

1.2. Проблемы качества обслуживания (QoS) на магистральных участках сетей, стоящие перед современными операторами связи

Качество обслуживания QoS связано с необходимостью сети предоставить клиенту требуемый ему уровень услуг в условиях работы

поверх сетей с самыми разнообразными технологиями, включая Frame Relay, ATM, Ethernet, сети 802.1 и маршрутизируемые IP- сети. Все перечисленные технологии в той или иной мере используют механизмы качества обслуживания, но обеспечение QoS не является их основной характеристикой. На определенном этапе развития телекоммуникаций (несколько лет назад) операторы обнаружили тенденцию к увеличению числа клиентов (в основном крупных корпоративных), требующих от провайдеров качественно новый уровень обслуживания при передаче разнородного трафика. Разработчики сетевых технологий пришли к выводу о необходимости создания технологии, которая объединит в себе механизмы качества обслуживания, задействованные в работе предыдущих транспортных технологий, и добавит собственные принципиально новые разработки в этой области. Именно поэтому технология MPLS формировалась главным образом как технология, призванная обеспечить гарантированные параметры качества обслуживания QoS.

Качество обслуживания QoS представляет собой собрание технологий, которые позволяют приложениям запрашивать и получать предсказуемый уровень услуг с точки зрения пропускной способности, временного разброса задержки ответа, а также общей задержки доставки данных. В частности, качество обслуживания QoS подразумевает улучшение параметров или достижение большей предсказуемости предоставляемых услуг.

Это достигается следующими методами:

- ✓ Возможностью конфигурирования сетевого трафика.
- ✓ Сокращением вероятности потери пакетов/кадров.
- ✓ Поддержкой определенной полосы пропускания.
- ✓ Исключением или управляемостью сетевых перегрузок.
- ✓ Установкой количественных характеристик трафика по пути через сеть.

Решение проблем перегрузок в сетях – одна из основных задач всех технологий с использованием механизмов качества обслуживания QoS (для

краткости будем называть их QoS-технологиями). Управление перегрузкой может осуществляться путем изменения порядка, в котором посылаются пакеты согласно приписанного им приоритету. QoS- управление перегрузкой имеет четыре модификации протоколов управления очередями, каждый из которых позволяет организовать разное число очередей.

Качество обслуживания QoS предполагает следующее:

✓ Управление входными очередями: когда пакет/кадр приходит на вход порта, он может быть отнесен к одной из нескольких очередей, ассоциированных с портом, прежде чем он будет направлен на один из выходных портов. Обычно, несколько очередей используются тогда, когда различные информационные потоки требуют различных уровней услуг или минимизации задержки.

✓ Классификация: процесс классификации включает просмотр различных полей в заголовке, чтобы обеспечить определенный уровень услуг при коммутации пакетов.

✓ Политика: осуществление политики является процессом анализа пакета/кадра, чтобы определить, не будет ли превышен заданный уровень трафика за определенный интервал времени. Если пакет/кадр создает ситуацию, при которой трафик превысит заданный уровень, он будет отброшен или значение CoS (Class of Service, класс обслуживания) может быть понижено.

✓ Перепись: процесс переписи предоставляет возможность переключателю модифицировать класс обслуживания CoS в заголовке или ToS (Type of Service, вид обслуживания) в IPv4-заголовке[14].

1.3. Обеспечение совместимости технологии MPLS с другими технологиями современными операторами связи

У технологии MPLS есть одно важное преимущество, которое не так бесспорно, но подчеркивается всеми операторами, сделавшими ставку на коммутацию по меткам, - это несравненная простота приведения к единому знаменателю абсолютно всех технологий, используемых на участке доступа.

Краткая характеристика взаимодействия технологий ATM и MPLS. Технология MPLS позволяет совместить преимущества по производительности и управлению трафиком коммутирующих устройств второго уровня модели ЭМВОС с преимуществами масштабируемости и гибкости маршрутизирующих устройств третьего уровня модели ЭМВОС в одном устройстве. Вообще говоря, такой подход применим к сетям, использующим любую технологию второго уровня модели ЭМВОС, но наибольший выигрыш можно получить, применяя технологию MPLS к ATM-сетям, совмещая маршрутизацию IP-пакетов с коммутацией ATM-ячеек.

Привлекательность технологии MPLS в отношении производительности настолько велика, что ведущие производители были вынуждены принципиально модернизировать коммутаторы ATM, чтобы отодвинуть на некоторое время переход операторов, использующих технологию ATM на магистральных участках своих сетей, на технологию MPLS. В результате на рынке появилось новое поколение коммутаторов ATM с очень высокой общей производительностью: то 1,2 до 480 Гбит/с[5].

2. ОСНОВНЫЕ ПРИНЦИПЫ РАБОТЫ И ТЕХНОЛОГИЯ MPLS.

2.1. Введение в технологию MPLS.

MPLS (multiprotocol label switching — многопротокольная коммутация по меткам) — механизм в высокопроизводительной телекоммуникационной сети, осуществляющий передачу данных от одного узла сети к другому с помощью меток.

MPLS является масштабируемым и независимым от каких-либо протоколов механизмом передачи данных. В сети, основанной на MPLS, пакетам данных присваиваются метки. Решение о дальнейшей передаче пакета данных другому узлу сети осуществляется только на основании значения присвоенной метки без необходимости изучения самого пакета данных. За счет этого возможно создание сквозного виртуального канала, независимого от среды передачи и использующего любой протокол передачи данных.

История. В 1996 г. группа инженеров из Ipsilon Networks разработала «Протокол управления потоком» (Flow Management Protocol).

Основанная на этом протоколе технология «Коммутации IP-пакетов» (IP Switching), работающая только поверх упрощенной сети ATM, не получила коммерческого успеха. Cisco Systems разработала похожую технологию «коммутации на основе тегов» (Tag Switching), не ограниченную передачей поверх сети ATM.

Данная технология, впоследствии переименованная в «коммутацию на основе меток» (Label Switching), была закрытой разработкой Cisco. Позднее она была передана в Специальную комиссию интернет-разработок (IETF) для открытой стандартизации.

Преимущества технологии

MPLS позволяет достаточно легко создавать виртуальные каналы между узлами сети. Технология позволяет инкапсулировать различные протоколы передачи данных.

Основным преимуществом MPLS является независимость от особенностей технологий канального уровня, таких как ATM, Frame Relay, SONET/SDH или Ethernet, и отсутствия необходимости поддержания нескольких сетей второго уровня, необходимых для передачи различного рода трафика. По виду коммутации MPLS относится к сетям с коммутацией пакетов.

Технология MPLS была разработана для организации единого протокола передачи данных как для приложений с коммутацией каналов, так и приложений с коммутацией пакетов (подразумеваются приложения с датаграммной передачей пакетов). MPLS может быть использован для передачи различного вида трафика, включая IP-пакеты, ячейки ATM, фреймы SONET/SDH и кадры Ethernet.

В частности, MPLS обходится без коммутации ячеек и набора сигнальных протоколов, характерных для ATM. При разработке MPLS пришло понимание того, что на уровне ядра современной сети нет необходимости в ячейках ATM маленького фиксированного размера, поскольку современные оптические сети обладают такой большой скоростью передачи данных, что даже пакет данных максимальной длины в 1500 байт испытывает незначительную задержку в очередях буферов коммутационного оборудования (необходимость сокращения таких задержек, например, для обеспечения заданного качества голосового трафика, повлияла на выбор ячеек малого размера, характерных для ATM).

Несмотря на то, что переход на MPLS дает преимущества управления потоками данных (улучшение надежности и повышение производительности

как коммутация может быть выполнена непосредственно на коммутационной фабрике вместо центрального процессора.

Маршрутизаторы, расположенные на входе или выходе MPLS-сети называются LER (*Label Edge Router*— граничный маршрутизатор меток). LER на входе в MPLS-сеть добавляют метку MPLS к пакету данных, а LER на выходе из MPLS-сети удаляет метку MPLS из пакета данных. Маршрутизаторы, выполняющие маршрутизацию пакетов данных, основываясь только на значении метки, называются LSR (*Label Switching Router* — коммутирующий метки маршрутизатор). В некоторых случаях пакет данных, поступивший на порт LER, уже может содержать метку, тогда новый LER добавляет вторую метку в пакет данных.

Метки между LER и LSR распределяются с помощью LDP (*Label Distribution Protocol* — протокол распределения меток).

Виртуальные каналы (туннели), называемые LSP (*Label Switch Path* — пути коммутации меток), устанавливаются провайдерами для решения различных задач, например, для организации VPN или для передачи трафика через MPLS-сеть по указанному туннелю. Во многом LSP ничем не отличается от PVC в сетях ATM или Frame Relay за исключением того, что LSP не зависят от особенностей технологий канального уровня.

При описании виртуальных частных сетей, основанных на технологии MPLS, расположенные на входе или выходе сети LER обычно называются PE-маршрутизаторы (*Provider Edge* — маршрутизаторы на границе сети провайдера), а узлы, работающие как транзитные маршрутизаторы, называются P-маршрутизаторы (*Provider* — маршрутизаторы провайдера).[19]

2.3. Принцип коммутации

В основе технологии MPLS лежит принцип обмена меток. Любой передаваемый пакет ассоциируется с тем или иным классом сетевого уровня (Forwarding Equivalence Class, FEC), каждый из которых идентифицируется определенной меткой. Значение метки уникально лишь для участка пути между соседними узлами сети MPLS, которые называются также маршрутизаторами, коммутирующими по меткам (Label Switching Router, LSR). Метка передается в составе любого пакета, причем способ ее привязки к пакету зависит от используемой технологии канального уровня.[4]

Маршрутизатор LSR получает топологическую информацию о сети, участвуя в работе алгоритма маршрутизации — OSPF (поиск кратчайшего пути), BGP (Border Gateway Protocol – протокол граничных маршрутизаторов) и др. Затем он начинает взаимодействовать с соседними маршрутизаторами, распределяя метки, которые в дальнейшем будут применяться для коммутации. Обмен метками может производиться с помощью как специального протокола распределения меток (Label Distribution Protocol, LDP), так и модифицированных версий других протоколов сигнализации в сети (например, незначительно видоизмененных протоколов маршрутизации, резервирования ресурсов RSVP и др.)[4].

Распределение меток между маршрутизаторами LSR приводит к установлению внутри домена MPLS путей с коммутацией по меткам (Label Switching Path, LSP). Каждый маршрутизатор LSR содержит таблицу, которая ставит в соответствие паре «входной интерфейс, входная метка» тройку «префикс адреса получателя, выходной интерфейс, выходная метка».

Получая пакет, маршрутизатор LSR по номеру интерфейса, на который пришел пакет, и по значению привязанной к пакету метки определяет для него выходной интерфейс. (Значение префикса применяется лишь для построения таблицы и в самом процессе коммутации не используется.)

Старое значение метки заменяется новым, содержащимся в поле «выходная метка» таблицы, и пакет отправляется к следующему устройству на пути маршрутизатора LSP[3].

Вся операция требует лишь одноразовой идентификации значений полей в одной строке таблицы. Это занимает гораздо меньше времени, чем сравнение IP-адреса отправителя с наиболее длинным адресным префиксом в таблице маршрутизации, которое используется при традиционной маршрутизации.

Сеть MPLS делится на две функционально различные области — ядро и граничную область. Ядро образуют устройства, минимальным требованием к которым является поддержка технологии MPLS и участие в процессе маршрутизации трафика для того протокола, который коммутируется с помощью технологии MPLS[2].

Маршрутизаторы ядра занимаются только коммутацией. Все функции классификации пакетов по различным классам FEC, а также реализацию таких дополнительных сервисов, как фильтрация, явная маршрутизация, выравнивание нагрузки и управление трафиком, берут на себя граничные маршрутизаторы LSR.

В результате интенсивные вычисления приходятся на граничную область, а высокопроизводительная коммутация выполняется в ядре, что позволяет оптимизировать конфигурацию устройств MPLS-сети в зависимости от их местоположения.

Таким образом, главная особенность технологии MPLS — отделение процесса коммутации пакета от анализа IP-адресов в его заголовке, что открывает ряд привлекательных возможностей. Очевидным следствием описанного подхода является тот факт, что очередной сегмент LSP может не совпадать с очередным сегментом маршрута, который был бы выбран при традиционной маршрутизации[8].

2.4. Элементы архитектуры

Метки и способы маркировки. Метка — это короткий идентификатор фиксированной длины, который определяет класс FEC. По значению метки пакета определяется его принадлежность к определенному классу на каждом из участков коммутируемого маршрута.

Как уже отмечалось, метка должна быть уникальной лишь в пределах соединения между каждой парой логически соседних маршрутизаторов LSR. Поэтому одно и то же ее значение может использоваться маршрутизатором LSR для связи с различными соседними маршрутизаторами, если только имеется возможность определить, от какого из них пришел пакет с данной меткой. Другими словами, в соединениях «точка—точка» допускается применять один набор меток на интерфейс, а для сетей с множественным доступом необходим один набор меток на модуль или все устройство. В реальных условиях угроза исчерпания пространства меток очень маловероятна[11].

Перед включением в состав пакета метка определенным образом кодируется. В случае использования протокола IP она помещается в специальный «тонкий» заголовок пакета, инкапсулирующего IP. В других ситуациях метка записывается в заголовок протокола канального уровня или кодируется в виде определенного значения VPI/VCI (в сети ATM). Для пакетов протокола IPv6 метку можно разместить в поле идентификатора потока[16].

Стек меток. Кодирование стека меток. В рамках архитектуры MPLS вместе с пакетом разрешено передавать не одну метку, а целый их стек. Операции добавления/изъятия метки определены как операции на стеке (push/pop). Результат коммутации задает лишь верхняя метка стека, нижние же передаются прозрачно до операции изъятия верхней. Такой подход позволяет создавать иерархию потоков в сети MPLS и организовывать

туннельные передачи. Стек состоит из произвольного числа элементов, каждый из которых имеет длину 32 бита: 20 бит составляют собственно метку, 8 отводятся под счетчик времени жизни пакета, один указывает на нижний предел стека, а три не используются. Метка может принимать любое значение, кроме нескольких зарезервированных[21].

Стек меток представляет собой последовательность записей. Каждая запись в стек имеет длину 4 октета. Формат такой записи показан на рис.3. Запись стека меток размещается после заголовка канального уровня, и перед заголовком сетевого уровня (например, между Ethernet и IP-заголовками). Верх стека записывается первым, а дно - последним. Сетевой заголовок следует сразу вслед за записью стека меток с битом S=1.

Каждая запись стека меток содержит в себе следующие поля:

- ✓ Дно стека (S). Этот бит устанавливается равным 1 для последней записи в стеке меток (т.е., для дна стека), и нулю для всех прочих записей.
- ✓ Время жизни (TTL). Это 8-битовое поле служит для представления значения времени жизни пакета.
- ✓ Экспериментальное поле. Это 3-битовое поле зарезервировано для экспериментальных целей (QoS).
- ✓ Значение метки. Это 20-битовое поле несет в себе код метки. Когда получен помеченный пакет, анализируется значение метки на вершине стека. В результате этого анализа определяется:
 - a) следующий шаг, куда должен быть переадресован пакет;
 - b) операция, которая должна быть выполнена со стеком меток до переадресации; эта операция может быть заменой метки на вершине стека, или удаление записи из стека, или замещение верхней позиции в стеке и занесение туда затем одной или более новых записей.

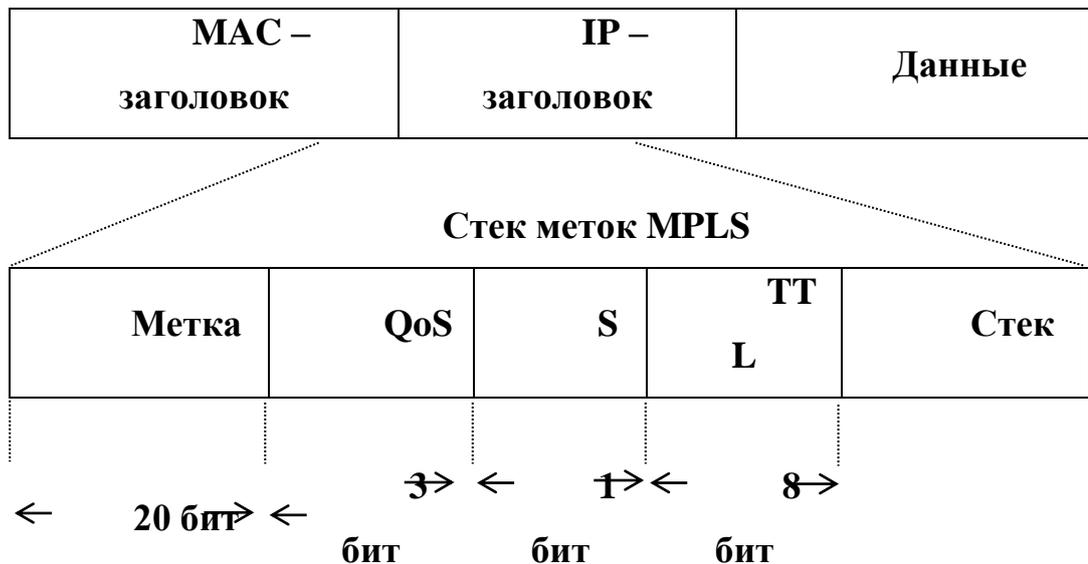


Рис.3 Формат записи стека меток

Поле Time To Live (TTL). При традиционной IP-переадресации, каждый пакет имеет в заголовке значение поля "Time To Live" (TTL). Когда бы пакет ни проходил через маршрутизатор, его TTL уменьшается на 1. Если TTL достигает 0, прежде чем пакет достигнет места назначения, он отбрасывается[26].

Это обеспечивает некоторый уровень защиты против петлевых маршрутов, которые могут существовать из-за ошибок в конфигурации, или по причине ошибки или медленной сходимости алгоритма маршрутизации. TTL иногда используется для других функций, таких как определение зоны действия мульти кастинга, и поддержка команды "traceroute". Это означает, что имеется две проблемы, связанные с TTL, которые технология MPLS должна решить:

- ✓ TTL как способ подавления зацикливания;
- ✓ TTL как метод реализации других функций, таких как ограничение области распространения пакета.

Определение протокола сетевого уровня. Когда последняя метка удалена из стека (стек становится пустым), дальнейшая обработка пакета

осуществляется на основе его заголовка сетевого уровня. Маршрутизатор LSR, который извлекает последнюю метку из стека, должен быть способен работать с протоколом сетевого уровня. Однако, стек меток не содержит поля, идентифицирующего протокол сетевого уровня. Это означает, что идентичность сетевого протокола должна определяться по значению кода метки, извлеченной со дна стека, возможно, вместе с самим содержимым заголовка сетевого уровня.

Следовательно, когда в сетевой пакет заносится первая метка, она должна быть уникальной для конкретного сетевого уровня или для набора сетевых протоколов. Кроме того, когда бы в процессе передачи метка ни была заменена другой, новая метка также должна отвечать тем же критериям. Если эти условия не выполнены, маршрутизатор LSR, который удаляет последнюю метку из пакета, не сможет идентифицировать сетевой протокол.

Строгое соблюдение этих условий не обязательно приведет немедленно к тому, что узлы будут распознавать сетевой протокол. В обычных условиях, это необязательно, но в ситуациях ошибок это оказывается крайне желательным. Например, если промежуточный маршрутизатор LSR определяет, что помеченный пакет не может быть доставлен, может быть желательно для данного маршрутизатора LSR сформировать сообщение об ошибке, которое является специфическим для пакетов сетевого уровня.

Единственные средства, которыми располагает промежуточный маршрутизатор LSR для идентификации сетевого уровня, является анализ верха стека и заголовка сетевого уровня[29].

Если пакет не может быть переадресован по какой-то причине, либо если его протокол сетевого уровня не может быть идентифицирован, либо не существует протоколно зависимых правил для обработки случаев ошибок, тогда пакет должен быть без комментариев отброшен[27].

Компоненты коммутируемого маршрута. Коммутируемый путь (LSP) одного уровня состоит из последовательного набора участков,

коммутация на которых происходит с помощью метки данного уровня (рис. 4).

Например, путь LSP нулевого уровня проходит через устройства LER 0, LSR 0, LSR 2, LSR 3 и LER 1. При этом LER 0 и LER 1 являются, соответственно, входным (ingress) и выходным (egress) маршрутизаторами для пути нулевого уровня. LSR 0 и LSR 2 играют ту же роль для пути LSP первого уровня; первый из них производит операцию добавления метки в стек, а второй — ее изъятия. С точки зрения трафика нулевого уровня, путь LSP первого уровня является прозрачным туннелем. В любом сегменте пути LSP можно выделить верхний и нижний маршрутизаторы LSR по отношению к трафику. Например, для сегмента «LSR 3 — LER 1» третий (LSR3) маршрутизатор будет верхним, а первый (LER1) — нижним[27].

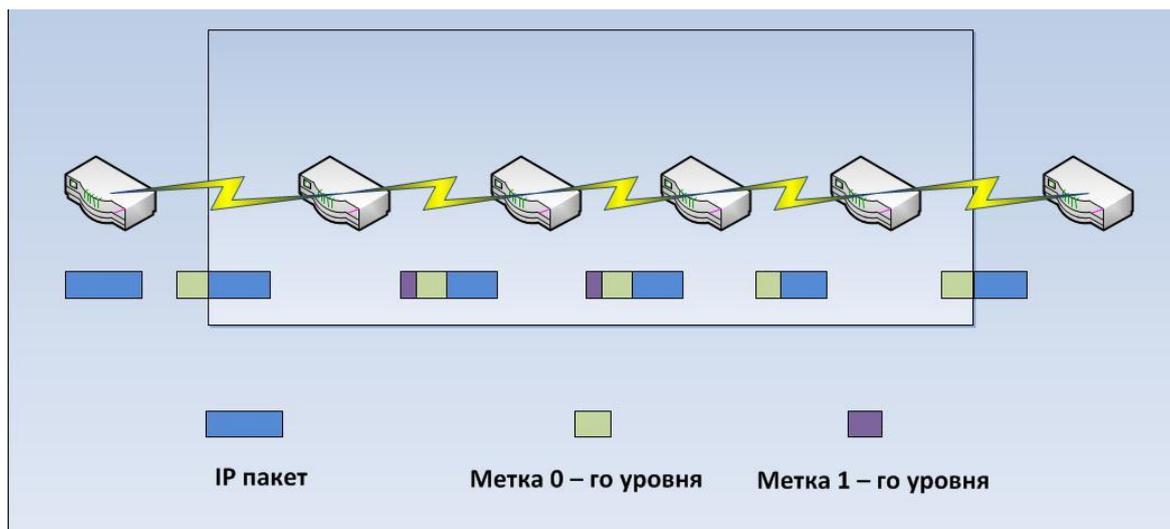


Рис. 4 Компоненты коммутируемого соединения

2.5. Выбор маршрута

Выбор маршрута сопряжен с методом, используемым при выборе пути LSP для определенного класса FEC. Предлагаемая архитектура MPLS

поддерживает две опции выбора маршрута: маршрутизация шаг-за-шагом и явная маршрутизация[10].

Построение коммутируемого маршрута. Рассмотрим, как в MPLS-сети автоматически создается путь LSP в простейшем случае — с помощью протокола LDP. Архитектура MPLS не требует обязательного применения протокола LDP, однако, в отличие от других возможных вариантов, он наиболее близок к окончательной стандартизации.

Сначала посредством многоадресной рассылки сообщений UDP коммутирующие маршрутизаторы определяют свое «соседство» (adjacency) в рамках протокола LDP. Кроме близости на канальном уровне, протокол LDP может устанавливать связь между «логически соседними» маршрутизаторами LSR, не принадлежащими к одному каналу. Это необходимо для реализации туннельной передачи. После того как соседство установлено, протокол LDP открывает транспортное соединение между участниками сеанса поверх протокола TCP. По этому соединению передаются запросы на установку привязки и сама информация о привязке. Кроме того, участники сеанса периодически проверяют работоспособность друг друга, отправляя тестовые сообщения (keepalive message)[17].

Рассмотрим на примере, как происходит заполнение таблиц меток по протоколу LDP (рис. 5). Предположим, что выбран упорядоченный режим распределения меток LSP со спонтанным распространением сведений о привязке[15]

Исходными данными для выбора путей являются, во-первых, характеристики передающей сети - топология, а также производительность составляющих ее маршрутизаторов и каналов связи, а во-вторых, сведения о нагрузке сети, т. е. о потоках трафика, которые она должна передать между своими пограничными маршрутизаторами. Каждый поток характеризуется точкой входа в сеть, точкой выхода из нее и некоторыми параметрами трафика. Так как при выборе путей мы стремимся обеспечить равномерную

загрузку маршрутизаторов и каналов связи, то для каждого потока, как минимум, нужно учитывать его среднюю интенсивность. Для более тонкой оптимизации трафика в сети можно привлекать и более детальное описание каждого потока: например, величину возможной пульсации трафика или требования к качеству обслуживания - чувствительность к задержкам, вариации задержек и допустимый процент потерь пакетов. Однако, поскольку оценить такого рода параметры трафика более сложно, чем среднюю интенсивность, а их влияние на функционирование сети менее значительно, чтобы найти оптимальное распределение путей прохождения потоков через сеть, учитываются только параметры их средней интенсивности[10].

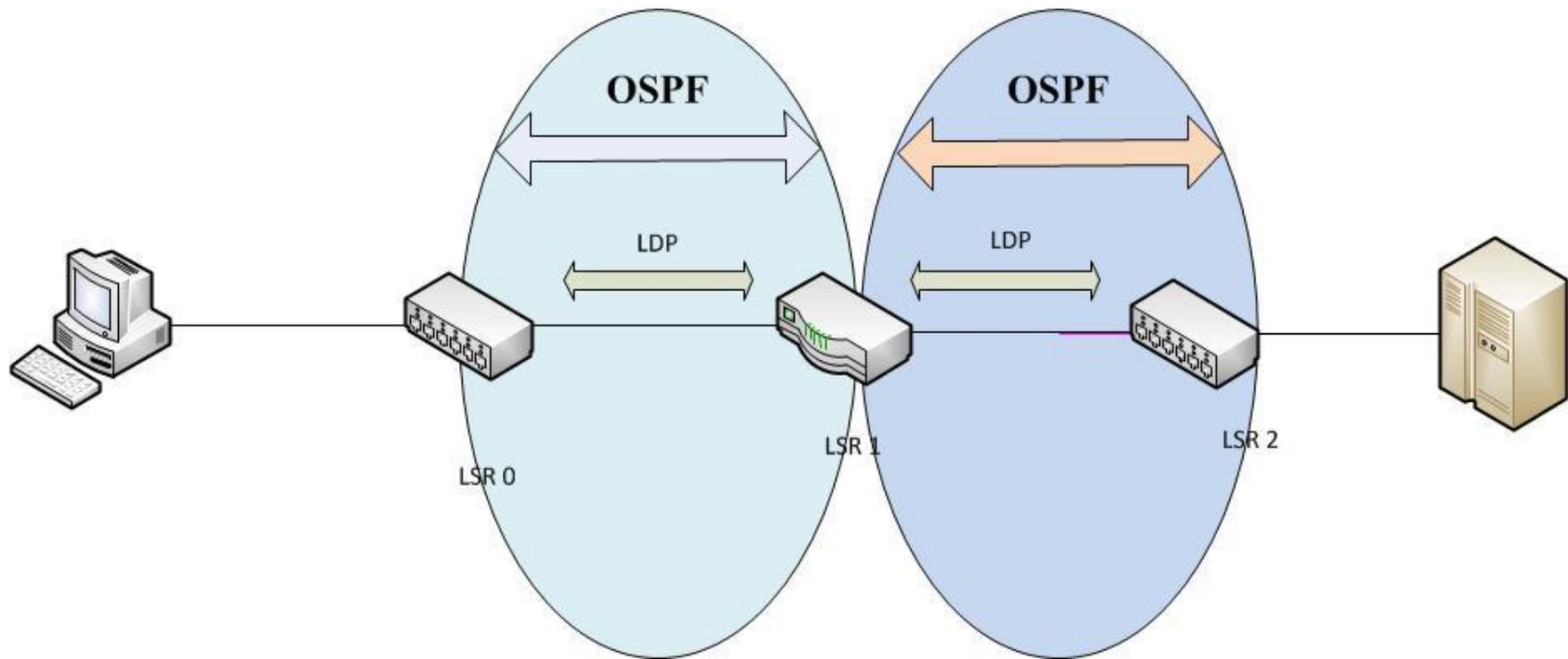


Рис. 5 Построение коммутируемого пути по протоколу LDP

2.6. Управление трафиком в технологии MPLS

Одним из мощных, но не применяемых ранее в сетях IP методов влияния на эффективное использование ресурсов сети является технология Traffic Engineering (TE), или в дословном переводе "инжиниринг трафика. В узком смысле, наиболее соответствующем названию, под TE понимаются методы и механизмы достижения сбалансированности загрузки всех ресурсов сети за счет рационального выбора путей прохождения трафика через сеть.

Задача TE состоит в определении маршрутов потоков трафика через сеть, т. е. для каждого потока требуется указать точную последовательность промежуточных маршрутизаторов и их интерфейсов на пути между входной и выходной точкой потока. При этом все ресурсы сети должны быть загружены как можно более сбалансировано. Это условие можно формализовать разными способами. Например, максимальный коэффициент использования ресурса по всем ресурсам сети должен быть минимален, чтобы трафику был нанесен как можно меньший ущерб. Именно так формулируется задача TE в RFC 2702 "Requirements for Traffic Engineering Over MPLS" ("Требования для управления трафиком в сетях MPLS") [13].

Технология MPLS поступает иначе - она обрабатывает для выбора путей топологическую информацию, собираемую протоколами маршрутизации стека TCP/IP, при этом пути всегда устанавливаются заранее, до передачи трафика. Так как маршрутизаторы IP являются в то же время и коммутаторами MPLS, то в результате имеется единый общий вариант топологии сети для уровня IP и уровня MPLS - а не два варианта, как при использовании самостоятельного слоя коммутаторов ATM под маршрутизаторами IP [16].

Методики, используемые для управления трафиком в сетях MPLS. Методики, используемые в сетях MPLS для управления трафиком, базируются на следующих факторах:

✓ Явные пути с коммутацией меток могут быть легко сформированы сетевым администратором или посредством стандартных протоколов.

✓ Эффективная поддержка механизма LSP. Управление трафиком реализуется за счет механизма так называемых «явно заданных маршрутов» (то есть за счет механизмов LSP, признанных приоритетными), минуя процесс автоматического создания. Механизм LSP с явно заданным маршрутом позволяют избегать перегруженных областей при прохождении трафика по сети, согласно требованиям качества обслуживания QoS, из соображений безопасности или в зависимости от других критериев.

✓ Каналы передачи данных могут быть смоделированы и поставлены в соответствие путям LSP.

✓ Набор атрибутов могут быть ассоциирован с каналами передачи данных, которые регулируют их рабочие характеристики.

✓ Набор атрибутов может быть ассоциирован с ресурсами, которые ограничивают положение путей LSP и каналов передачи данных.

✓ Технология MPLS позволяет как агрегацию, так и дисагрегацию трафика, в то время как классическая переадресация на основе IP-адреса места назначения допускает только агрегацию.

✓ Относительно легко интегрировать "маршрутизацию на основе ограничений" в рамках MPLS-сетей.

✓ Ограничения механизмов управления протокола IGP, так как они, базируясь на алгоритмах кратчайшего пути, вносят заметный вклад в проблемы перегрузки в автономных системах сетей.

Кроме того, через механизм коммутации меток технология MPLS позволяет наложить на современную модель маршрутизации сети Интернет квазиканальную коммутацию[13]

2.7. Будущее технологии MPLS

В настоящее время существуют два основных способа создания магистральных IP-сетей: с помощью IP-маршрутизаторов, соединенных каналами «точка—точка», либо на базе сети ATM, поверх которой работают IP-маршрутизаторы. Применение технологии MPLS оказывается выгодным в обоих случаях. В сети ATM оно дает возможность одновременно предоставлять клиентам как стандартные сервисы ATM, так и широкий спектр услуг IP-сетей вместе с дополнительными услугами. Такой подход существенно расширяет пакет услуг провайдера, заметно повышая его конкурентоспособность. Тандем технологий IP и ATM, соединенных посредством технологии MPLS, способствует еще большему распространению этих технологий и создает основу для построения крупномасштабных сетей с интеграцией сервисов[26]

Анализируя выводы, сделанные в результате исследований, произведенных, можно утверждать, что обоснованные в первой главе задачи, стоящие перед операторами MPLS сетей, актуальны и поиск решений в данной среде является важным на сегодняшний день вопросом. Таким образом, опираясь на теоретические разработки западных и отечественных специалистов в области транспортных сетевых технологий, было решено использовать материалы исследований второй главы для разработки программного обеспечения для сбора статистических данных о конфигурации и параметрах работы проектируемого участка сети MPLS.

Безусловно, сегодня технология MPLS даст ATM много очков вперед, а ситуация принципиально отличается от той, которая складывалась в период проведения прошлогодней конференции.

Во-первых, технология MPLS приобрела, наконец, устойчивость и более широкую поддержку производителей.

Во-вторых, все большее число операторов поговаривают о будущем внедрении MPLS.

В-третьих, когда стало ясно, что базой для создания будущих приложений является технология IP, все увидели, что лучшие годы ATM остались в прошлом[22].

Если говорить о том, что еще предстоит сделать, то особое внимание следует уделить взаимодействию сетей ATM и MPLS. Это нужно для того, чтобы операторы могли разворачивать архитектуру MPLS в ядре сети, оставляя оборудование ATM на ее конечных узлах[19].

Рабочие группы ATM Forum и IETF уже предложили ряд решений, позволяющих ATM функционировать поверх MPLS, и активно отстаивали свою позицию перед органами стандартизации ITU. На последнем заседании ITU, прошедшем в Японии, было принято компромиссное решение, которое предусматривает признание четырех встроенных режимов ATM-MPLS-ATM. Теперь процесс интеграции технологий может двигаться дальше[12].

Вне зависимости от того, насколько хороша эта технология, MPLS не сумеет одолеть ATM за один день — хотя бы потому, что для перехода на новую основу нужны слишком большие капиталовложения. Можно с уверенностью утверждать, что пройдет еще немало времени, прежде чем MPLS окончательно встанет на ноги, особенно в условиях нынешнего неблагоприятного экономического климата[20].

3. ПРОЕКТИРОВАНИЕ ТЕХНОЛОГИИ MPLS НА ВИРТУАЛЬНОЙ МАШИНЕ

В этой главе рассматриваются протокол динамической маршрутизации протокол маршрутизации OSPF, которыми пользуются маршрутизаторы для общения друг с другом.

Маршрутизация - это одна из наиболее важных функций IP. Датаграммы, которые должны быть с маршрутизированы, могут генерироваться как локальным хостом, так и каким-либо удаленным хостом. В последнем случае наш хост должен быть сконфигурирован как маршрутизатор, иначе дата граммы, получаемые через сетевые интерфейсы и не предназначенные нашему хосту, будут молча удалены.

3.1. Принципы маршрутизации

Прежде чем начать обсуждение IP маршрутизации, необходимо понять, что именно ядро обновляет в таблице маршрутизации. Информация, содержащаяся в таблице маршрутизации, необходима IP уровню для принятия решения о маршрутизации.

1. Поиск совпадающего адреса хоста.
2. Поиск совпадающего адреса сети.
3. Поиск пункта по умолчанию. (Пункт по умолчанию обычно указывается в таблице маршрутизации как сеть с идентификатором сети равным нулю.). Совпавший адрес хоста используется всегда перед совпавшим адресом сети.

Маршрутизация, осуществляемая IP - процесс поиска в таблице маршрутизации, определение интерфейса, куда будет послан пакет,

называется механизмом маршрутизации. С другой стороны, политика маршрутизации устанавливает правила, по которым решается, какой маршрут будет внесен в таблицу маршрутизации. IP осуществляет механизм маршрутизации, тогда как маршрутизирующий демон обычно определяет политику маршрутизации.

Динамическая маршрутизация

Динамическая маршрутизация — вид маршрутизации, при котором таблица маршрутизации редактируется программно. В случае UNIX-систем *демонами маршрутизации*; в других системах — служебными программами, которые называются иначе, но фактически играют ту же роль.

Демоны маршрутизации обмениваются между собой информацией, которая позволяет им заполнить таблицу маршрутизации наиболее оптимальными маршрутами. Протоколы, с помощью которых производится обмен информацией между демонами, называется *протоколами динамической маршрутизации*.

Динамическая маршрутизация используется для общения маршрутизаторов друг с другом. Маршрутизаторы передают друг другу информацию о том, какие сети в настоящее время подключены к каждому из них. Маршрутизаторы общаются, используя протоколы маршрутизации. Пользовательский процесс, посредством которого маршрутизаторы могут общаться с соседними маршрутизаторами, называется демоном маршрутизации (*routing daemon*).

Динамическая маршрутизация не меняет способы, с помощью которых ядро осуществляет маршрутизацию на IP уровне. Мы назвали это механизмом маршрутизации (*routing mechanism*). Ядро точно так же просматривает свою таблицу маршрутизации, отыскивая маршруты к хостам, маршруты к сетям и маршруты по умолчанию. Меняется только способ

помещения информации в таблицу маршрутизации - вместо запуска команды route или использования загрузочных файлов маршруты добавляются и удаляются динамически демоном маршрутизации, который работает постоянно.

Как было отмечено ранее, демон маршрутизации отвечает за политику маршрутизации (routing policy) , выбирая, какие маршруты необходимо поместить в таблицу маршрутизации. Если демон обнаружил несколько маршрутов к пункту назначения, он выбирает (каким-либо образом), какой маршрут лучше, и именно этот маршрут (единственный) добавляет в таблицу маршрутизации. Если демон определил, что канал исчез (возможно по причине выхода из строя маршрутизатора или телефонной линии), он может удалить соответствующие маршруты или добавить альтернативные маршруты, чтобы обойти возникшую неисправность.

В Internet, на сегодняшний день, используется множество различных протоколов маршрутизации. Internet организован как сообщество автономных систем (AS - autonomous systems), каждая из которых обычно администрируется независимо от остальных. Например, сеть, построенная в университетском городке, обычно считается автономной системой. Магистраль (backbone)NSFNET с точки зрения Internet это автономная система, потому что все маршрутизаторы на магистрали находятся под единым административным контролем.

Для каждой автономной системы выбирается собственный протокол маршрутизации, с помощью которого осуществляется взаимодействие между маршрутизаторами в этой автономной системе. Такой протокол называется протоколом внутренних маршрутизаторов (IGP - interior gateway protocol) или протоколом внутри доменной маршрутизации (intradomain routing protocol). Наиболее популярный IGP - это протокол обмена информацией о маршрутизации (RIP - Routing Information Protocol). Более новый IGP это

протокол Open Shortest Path First (OSPF). Он был разработан как замена для RIP.

Новые требования к маршрутизаторам Router Requirements RFC определяют, что маршрутизатор, который реализует любые динамические протоколы маршрутизации, должен поддерживать OSPF и RIP, а также может поддерживать другие IGP.

Существуют протоколы маршрутизации, которые называются протоколами внешних маршрутизаторов (EGP - exterior gateway protocols) или протоколами меж доменной маршрутизации (interdomain routing protocols). Они предназначены для общения между маршрутизаторами, находящимися в разных автономных системах. Исторически (и к большому сожалению) предшественником всех EGP был протокол с тем же самым именем: EGP. Более новый EGP - протокол пограничных маршрутизаторов (BGP - Border Gateway Protocol) в настоящее время используется между магистралью NSFNET и некоторыми региональными сетями, которые подключены к магистрали. Планируется, что BGP заменит собой EGP.

3.2. Обзор OSPF

- Создает отношения соседства за счет обмена пакетами приветствия
- Распространяет объявления состояния канала, а не обновления таблицы маршрутизации
 - Канал: интерфейс маршрутизатора
 - Состояние: описание интерфейса и его отношений с соседними маршрутизаторами
- Рассылает объявления состояния канала всем маршрутизаторам OSPF в области, не только маршрутизаторам с прямым подключением
- Сводит вместе все объявления состояния канала, созданные маршрутизаторами OSPF, чтобы создать базу данных состояний канала OSPF

- Использует алгоритм SPF для вычисления кратчайшего пути к каждому месту назначения и помещает этот путь в таблицу маршрутизации

OSPF основан на алгоритме состояния канала. Канал можно представить как интерфейс маршрутизатора. Состояние канала — это описание интерфейса и его отношений с соседними маршрутизаторами. Описание интерфейса должно содержать, такие параметры, как IP адресация, маску, тип сети, к которой подключен интерфейс, маршрутизаторы, подключенные к этой сети и т. п. Набор всех состояний каналов формирует базу данных состояний каналов.

Маршрутизатор Cisco отправляет пакеты объявления состояния канала (LSA), чтобы объявить о своем состоянии, через регулярные интервалы (30 минут) или немедленно при изменении состояния маршрутизатора. В объявлениях состояния канала OSPF содержатся данные о подключенных интерфейсах, используемых метриках и других параметрах. Накопив данные о состоянии каналов, маршрутизаторы OSPF Cisco используют алгоритм SPF для расчета кратчайшего пути к каждому из узлов.

Топологическая база данных (база данных состояния каналов) содержит общее представление сетей с точки зрения маршрутизаторов. Топологическая база данных содержит набор объявлений состояния канала, полученных от всех маршрутизаторов в области. Поскольку маршрутизаторы в одной области используют одинаковые данные, их топологические базы данных идентичны.

Примечание Протокол OSPF может работать в иерархии. Самая крупная сущность иерархии — автономная система (набор сетей под общим управлением и с общей стратегией маршрутизации). Автономную систему можно разделить на несколько областей, которые представляют собой группы смежных сетей и подключенных к ним узлов.

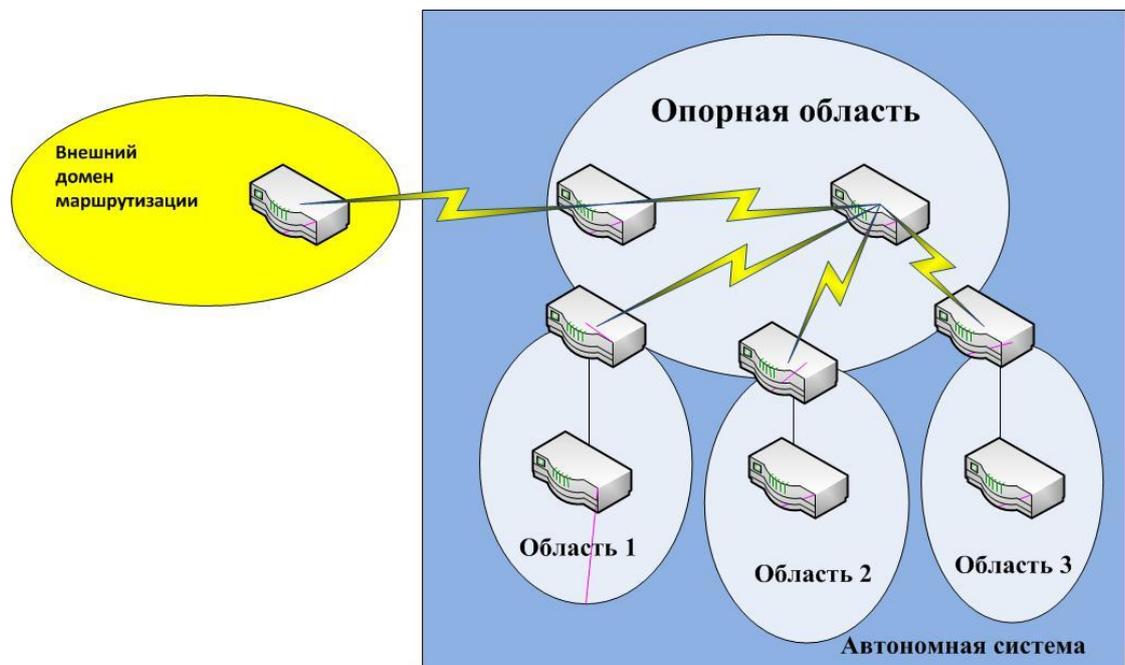


Рис. 6 Пример иерархии OSPF Cisco

- Уменьшает записи таблиц маршрутизации
- Изолирует влияние изменений топологии внутри одной области

OSPF использует двухуровневую иерархию сети. Эта иерархия содержит два основных элемента.

- Область. Область — это группа смежных сетей. Области представляют собой логические разделы автономной системы.

- Автономная система. Автономная система — это совокупность сетей с общим управлением и с общей стратегией маршрутизации. Автономные системы, также известные как домены, можно логически разделить на несколько областей.

В каждой автономной системе необходимо задать непрерывную магистральную (Backbone) область. Все немагистральные области соединяются через магистральную область. Магистральная область является транзитной, поскольку все остальные области взаимодействуют через нее. В сети OSPF немагистральные области могут быть настроены в качестве тупиковых (Stub), полностью тупиковых (totally stubby) или не так уж

тупиковых (notso stubby NSSA), чтобы уменьшить размеры баз данных состояния канала и таблиц маршрутизации.

Маршрутизаторы, работающие в двухуровневой сетевой иерархии, могут выполнять разные роли и функции в среде OSPF. Ниже приводятся примеры этих ролей (см. рисунок).

- Маршрутизатор В является магистральным маршрутизатором. Магистральный маршрутизатор обеспечивает соединение областей.

- Маршрутизаторы С, D и E — пограничные маршрутизаторы области (Area Border Router ABR). ABR подключаются к нескольким областям, ведут отдельную базу данных состояний канала для каждой области, к которой они подключены, и маршрутизируют трафик, направленный в другие области или прибывающий из них.

- Маршрутизаторы F, G и H — немагистральные, внутренние маршрутизаторы. Немагистральные внутренние маршрутизаторы имеют данные о топологии областей, в которых они находятся, и ведут одинаковые базы данных состояния каналов для этих областей.

- В зависимости от конфигурации немагистральной области OSPF (тупиковой области, полностью тупиковой области или NSSA) маршрутизатор ABR объявляет маршрут по умолчанию внутреннему немагистральному маршрутизатору. Внутренний немагистральный маршрутизатор использует маршрут по умолчанию для пересылки всего межобластного или меж доменного трафика к маршрутизатору ABR.

- Маршрутизатор А является пограничным маршрутизатором автономной системы (Autonomous System Border Router ASBR) и служит для соединения с внешним доменом маршрутизации или автономной системой.

- Маршрутизатор I принадлежит другому домену маршрутизации или автономной системе.

Формирование соседских отношений между соседними узлами OSPF

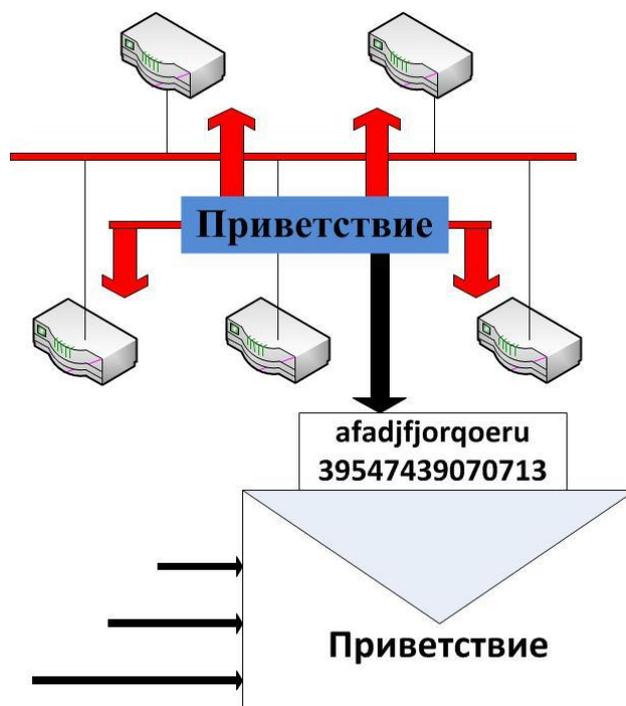


Рис. 7 Соседские отношения: пакет приветствия Hello

Соседние маршрутизаторы OSPF должны опознать друг друга в сети перед тем, как смогут обмениваться информацией, так как маршрутизация OSPF зависит от состояния канала между двумя маршрутизаторами. Этот процесс реализуется с помощью протокола приветствия (Hello). Протокол приветствия создает и поддерживает соседские отношения, обеспечивая двунаправленное соединение между коммутаторами. Двунаправленное соединение имеет место, когда маршрутизатор находит себя в пакете приветствия, полученном от соседнего узла.

Каждый интерфейс в среде OSPF периодически отправляет пакеты приветствия по адресу многоадресной рассылки 224.0.0.5. Пакет приветствия содержит следующие сведения.

- Идентификатор маршрутизатора (Router ID).

- Интервалы приветствия и простоя (Hello and dead intervals).
- Соседи (Neighbors). В поле соседей перечисляются соседние маршрутизаторы, с которыми установлено двусторонне соединение.
- Идентификатор области (Area ID). Для успешного взаимодействия маршрутизаторы должны находиться в одном сегменте и их интерфейсы должны принадлежать к одной области OSPF в этом сегменте.
- Приоритет маршрутизатора (Router priority).
- IP-адреса DR и BDR. IP-адреса маршрутизаторов DR и BDR в сети (если они известны).
- Пароль аутентификации (Authentication password).
- Флаг тупиковой области (Stub area flag). Тупиковая область — особая область среды OSPF. Два маршрутизатора должны согласовать флаг тупиковой области в пакетах приветствия. Назначение тупиковой области позволяет уменьшить число обновлений маршрутизации, заменив их на маршрут по умолчанию.

Каждый маршрутизатор имеет собственное представление о топологии, но при этом все маршрутизаторы используют одну базу данных состояний канала для вычисления дерева кратчайших путей.

Стоимость (метрика) интерфейса обозначает издержки отправки пакетов через определенный интерфейс. Стоимость интерфейса обратно пропорциональна полосе пропускания интерфейса, т. е. чем выше полоса пропускания, тем ниже стоимость. При передаче данных по последовательному каналу T1 издержки (стоимость) и временные задержки выше, чем при передаче через канал Ethernet 10 Мбит/с.

Формула расчета стоимости OSPF: стоимость = эталонная полоса пропускания/полоса пропускания интерфейса (в бит/с).

Эталонная полоса пропускания — 10^8 или 100 000 000, что эквивалентно полосе пропускания Fast Ethernet. Поэтому стоимость по умолчанию канала интерфейса Ethernet 10 Мбит/с будет $10^8 / 10^7 = 10$, стоимость канала T1 будет $10^8 / 1\,544\,000 = 64$.

Чтобы отрегулировать эталонную полосу пропускания для каналов с полосой пропускания выше, чем у сети Fast Ethernet, используйте команду `ospf autocost referencebandwidth` эталонная_полоса_пропускания.

3.3. Настройка технологии OSPF на виртуальной машине

Для начало настройки надо построи графический структура сети. Для этого мы используем программу Cisco Packet Tracer.

Состав сети входит 4 маршрутизатора: Cisco 2811, 4 Switch: 2960-24TT и конечные устройства(персональный компьютеры, ноутбуки и принтеры), а также сервер провайдера.

Маршрутизаторы соединены со Switch с помощью кабелем витая пара(экранированная витая пара STP). Она обозначена черной линией и с двумя зелёными точками.

 - витая пара(экранированная витая пара STP).

Также Switch и конечные устройства(персональный компьютеры, ноутбуки и принтеры) соединены между собой кабелем витая пара.

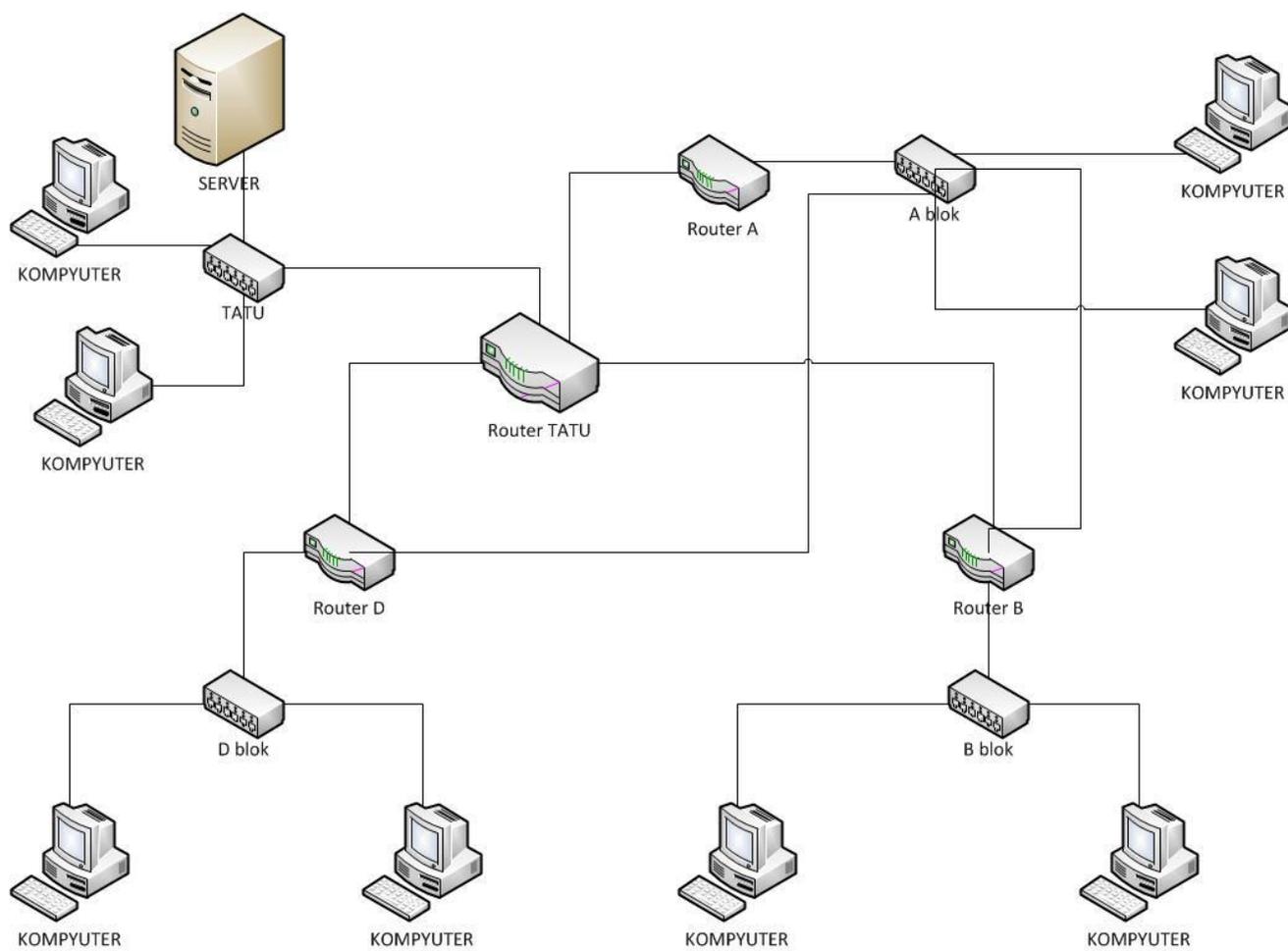


Рис. 8 Принципиальная схема проектируемого сети

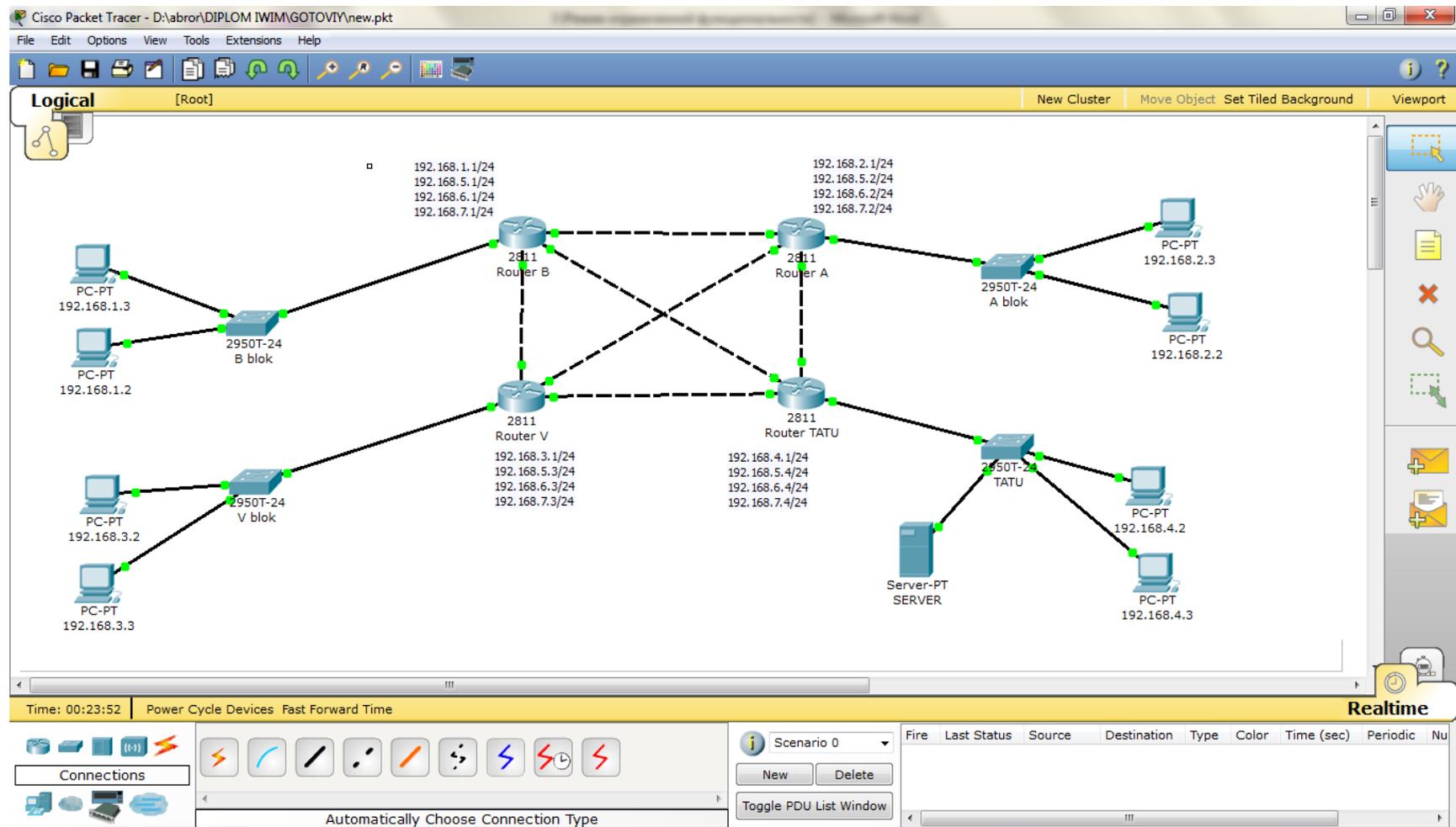


Рис. 8 Графическое обозначение сети OSPF в программе Cisco Packet Tracer

Настройка OSPF

На схеме представлены 4 роутера. TATU и Router В являются пограничными ELSR - Edge Label Switch Router (иногда их еще называют PE – Provider Edge Router). Они занимаются, с одной стороны, для «навешивания» (pushing) меток при входе пакета в домен MPLS и, с другой стороны, для «снятия» (popping) меток при выходе из домена MPLS. Роутеры Router В и Router D являются внутренними роутерами домена MPLS и называются LSR - Label Switch Router (второе название P – Provider Router). Они занимаются только передачей пакетов от одного MPLS роутера другому. Итак, приступим. Для организации сетевой доступности (IP) будем использовать протокол динамической маршрутизации OSPF. Хосты для проверки расположены в разных сетях.

Начнем с настройки стандартной сетевой доступности. Заходим на роутер TATU:

```
R1>en
R1#conf t
R1(config)#hostname TATU
R1(config)#int loopback 0 – создаем loopback интерфейс;
TATU(config-if)#ip address 192.168.4.1 255.255.255.0
TATU(config-if)#exit
TATU(config)#int fa 0/0
TATU(config-if)#ip address 192.168.5.4 255.255.255.0
TATU(config-if)#no sh
TATU(config-if)#exit
TATU(config)#int fa 1/0
TATU(config-if)#ip address 192.168.6.4 255.255.255.0
TATU(config-if)#no sh
TATU(config-if)#exit
TATU(config)#int fa 2/0
TATU(config-if)#ip address 192.168.7.4 255.255.255.0
TATU(config-if)#no sh
TATU(config-if)#exit
TATU(config)#router ospf 1 – настраиваем протокол динамической
маршрутизации OSPF;
TATU(config-router)#passive-interface default – выберем, на какие интерфейсы
отправлять дежурные пакеты OSPF;
TATU(config-router)#no passive-interface fastEthernet 1/0
TATU(config-router)#no passive-interface fastEthernet 2/0
TATU(config-router)#network 192.168.1.0 255.255.255.0 area 1 –определяем
сети для объявления;
TATU(config-router)#network 192.168.1.0 255.255.255.0 area 0
TATU(config-router)#network 192.168.3.0 255.255.255.0 area 0
TATU(config-router)#network 192.168.2.0 255.255.255.0 area 0
```

```
TATU(config-router)#exit
```

```
TATU(config)#exit
```

```
TATU#wr
```

```
TATU#
```

Рouter Router B:

```
R2>en
```

```
R2#conf t
```

```
R2(config)#hostname Router B
```

```
Router B(config)#int loopback 0
```

```
Router B(config-if)#ip address 192.168.1.1 255.255.255.0
```

```
Router B(config-if)#exit
```

```
Router B(config)#int fa 0/0
```

```
Router B(config-if)#ip address 192.168.5.1 255.255.255.0
```

```
Router B(config-if)#no sh
```

```
Router B(config-if)#exit
```

```
Router B(config)#int fa 1/0
```

```
Router B(config-if)#ip address 192.168.6.1 255.255.255.0
```

```
Router B(config-if)#no sh
```

```
Router B(config)#int fa 1/1
```

```
Router B(config-if)#ip address 192.168.7.1 255.255.255.0
```

```
Router B(config-if)#no sh
```

```
Router B(config-if)#exit
```

```
Router B(config)#router ospf 1
```

```
Router B (config-router)#network 192.168.2.0 255.255.255.0 area 0
```

```
Router B (config-router)#network 192.168.3.0 255.255.255.0 area 0
```

```
Router B (config-router)#network 192.168.4.0 255.255.255.0 area 0
```

```
Router B(config-router)#exit
```

Router B(config)#exit

Router B#wr

Router B#

Рouter Router D:

R3>en

R3#conf t

R3(config)#hostname Router D

Router D(config)#int loopback 0

Router D(config-if)#ip address 192.168.3.1 255.255.255.0

Router D(config-if)#exit

Router D(config)#int fa 0/0

Router D(config-if)#ip address 192.168.5.3 255.255.255.0

Router D(config-if)#no sh

Router D(config-if)#exit

Router D(config)#int fa 1/0

Router D(config-if)#ip address 192.168.6.3 255.255.255.0

Router D(config-if)#no sh

```
Router D(config)#int fa 1/1
Router D(config-if)#ip address 192.168.7.3 255.255.255.0
Router D(config-if)#no sh
Router D(config-if)#exit
Router D(config)#router ospf 1
Router D(config-router)#network 192.168.1.0 255.255.255.0 area 0
Router D(config-router)#network 192.168.2.0 255.255.255.0 area 0
Router D(config-router)#network 192.168.4.0 255.255.255.0 area 0
Router D(config-router)#exit
Router D(config)#exit
Router D#wr
Router D#
```

И поутер Router A:

```
R4>en
R4#conf t
R4(config)#hostname Router A
Router A(config)#int loopback 0
Router A(config-if)#ip address 192.168.2.1 255.255.255.0
Router A(config-if)#exit
Router A(config)#int fa 0/0
Router A(config-if)#ip address 192.168.5.2 255.255.255.0
Router A(config-if)#no sh
Router A(config-if)#exit
Router A(config)#int fa 1/0
Router A(config-if)#ip address 192.168.6.2 255.255.255.0
Router A(config-if)#no sh
Router A(config-if)#exit
```

```
Router A(config)#int fa 0/1
Router A(config-if)#ip address 192.168.7.2 255.255.255.0
Router A(config-if)#no sh
Router A(config-if)#exit
Router A(config)#router ospf 1
Router A(config-router)#passive-interface default
Router A(config-router)#no passive-interface fastEthernet 0/0
Router A(config-router)#no passive-interface fastEthernet 1/0
Router A(config-router)#no passive-interface fastEthernet 0/1
Router A(config-router)#network 192.168.1.0 255.255.255.0 area 2
Router A(config-router)#network 192.168.3.0 255.255.255.0 area 0
Router A(config-router)#network 192.168.4.0 255.255.255.0 area 0
Router A(config-router)#exit
Router A(config)#exit
Router A#wr
Router A#
```

Стоимость OSPF

Стоимость (метрика) интерфейса обозначает издержки отправки пакетов через определенный интерфейс. Стоимость интерфейса обратно пропорциональна его полосе пропускания. Более высокая полоса пропускания подразумевает более низкую стоимость. По умолчанию маршрутизаторы Cisco рассчитывают стоимость интерфейса на основе полосы пропускания. Однако вы можете принудительно назначить стоимость интерфейса с помощью команды `ip ospf cost {значение}` в режиме конфигурации интерфейса.

Если к месту назначения доступно несколько путей с одинаковой стоимостью, версия протокола OSPF Cisco может отслеживать до 16 последующих переходов в таблице маршрутизации (это называется распределением нагрузки). По умолчанию маршрутизаторы Cisco поддерживают до 4 путей OSPF к месту назначения. С помощью команды `maximum paths` в режиме конфигурации процесса маршрутизатора OSPF можно задать число путей с одинаковой стоимостью которые можно добавить в таблицу маршрутизации.

Для поиска маршрутов с одинаковой стоимостью используется команда `show ip route`. Ниже приводится пример вывода команды `show ip route` для подсети, для которой доступно несколько маршрутов в таблице маршрутизации. В примере выводится три пути к сети 194.168.20.0 с одинаковой стоимостью.

Обратите внимание, что вывод содержит три блока дескрипторов маршрутизации. Каждый блок представляет один из доступных маршрутов. Кроме того, один из блоков обозначен звездочкой (*). Звездочка указывает на активный маршрут, используемый для нового трафика. Термин «новый трафик» обозначает одиночный пакет или поток данных, направленный к месту назначения, в зависимости от того, в каком режиме распределения нагрузки работает маршрутизатор — распределение по месту назначения или распределение по пакетному.

Заключение

В выпускной квалификационной работе была рассмотрена обзор поставленной задачи и пути ее решения, основные принципы работы и технология MPLS, проектировано технологии MPLS на виртуальной машине, создано сеть MPLS, а также выявлена достоинства и недостатки технологий MPLS.

Для достижения цели решены следующие задачи:

- найти достоинства и недостатки технологий MPLS;
- построение виртуальных частных сетей (VPN) на основе технологии MPLS;
- сравнение сегодняшних сетей и мультисервисных сетей будущего;
- обнаружение проблем качества обслуживания;
- выявит преимущества технологии MPLS;
- изучения элементы архитектуры.

В выпускной квалификационной работе было разработана сеть OSPF на основе динамической маршрутизации, так как на виртуальной машине нет возможности отобразить данную технологию.

Была дана сравнительная оценка возможностей технологии MPLS, проблемы качества обслуживания (QoS) на магистральных участках сетей, стоящие перед современными операторами связи, обеспечение совместимости технологии MPLS с другими технологиями современными операторами связи, принцип работы MPLS и коммутации, элементы архитектуры, выбор маршрута, управление трафиком в технологии MPLS.

Список литературы