

# **1 АКТУАЛЬНОСТЬ ПОСТАВЛЕННОЙ ЗАДАЧИ. ПУТИ ЕЕ РЕШЕНИЯ**

## **1.1 Сравнительная оценка возможностей технологии MPLS**

### **1.1.1 Характеристики современного трафика магистральных сетей**

Целью данной дипломной работы является создание программного обеспечения, задачей которого будет сбор статистических данных (таких как задержка пакета при прохождении через коммутатор, определение топологии сети и др.), и базирующегося на использовании основных принципов работы технологии MPLS (Multi Protocol Label Switching – быстрая коммутация пакетов в многопротокольных сетях, основанная на использовании меток).

В последние годы объем трафика, передаваемого по IP сетям, неуклонно растёт, становятся сильнее тенденции разбиения трафика по видам (типам), например, голос и данные. Причинами здесь являются: появление качественно новых услуг в сфере обслуживания трафика, увеличение видов сервисов, предлагаемых современными провайдерами, рост числа пользователей глобальной сети Интернет, разработка новых телекоммуникационных технологий и т.д. Изменения влекут за собой новые проблемы при передаче разнотипного трафика, например, задержки и, соответственно, способы их решения, т.е. разработку новых технологий передачи и обработки трафика, в том числе и рассматриваемую в данной дипломной работе, технологию многопротокольной коммутации по меткам (MPLS).

Сбор статистических данных о процентном соотношении различных видов трафика, передаваемого по современным IP-сетям, и его росте представляется трудоёмкой задачей, являющейся работой больших аналитических компаний, специализирующихся в данной области. Поэтому автор данной дипломной работы решил акцентировать внимание на трафике IP телефонии, передаваемом по сетям MPLS.

Актуальность выбора данного вида трафика подтверждается следующими данными. Согласно исследованиям иностранных компаний\* объем международного VoIP (Voice over IP, передача голоса по IP-сетям) трафика вырос в 2003 году на 80% и превысил 18 млрд. минут, что составило 10,4% от всего международного телефонного трафика.

---

\*по данным Frost&Sullivan/Probe

Прогноз на 2004 год: рост — 36,1%, объем — 24,5 млрд. мин., доля — 12,8%.

Крупнейшими транзитными VoIP-операторами остаются ITXC и iBasis, каждый из которых пропустил в 2003 году по своим сетям более чем по 2,5 млрд. мин. международного телефонного трафика. Недавно известный VoIP-оператор компания ITXC объявила, что ежеквартальный объем ее трафика приблизился к 1 млрд. мин. Иностранные специалисты отмечают, что быстрый рост передаваемого трафика в международных VoIP-сетях связан с тем, что многие традиционные и сотовые операторы обращаются к их услугам.

По прогнозам Frost&Sullivan/Probe до 2005 года мировой рынок оптового IP-трафика будет ежегодно расти со средней скоростью 112%, рынок розничного потребительского рынка — в среднем на 91% в год, а самую высокую динамику покажет розничный корпоративный рынок, среднегодовые темпы роста которого составят 350% в год (рис. 1).

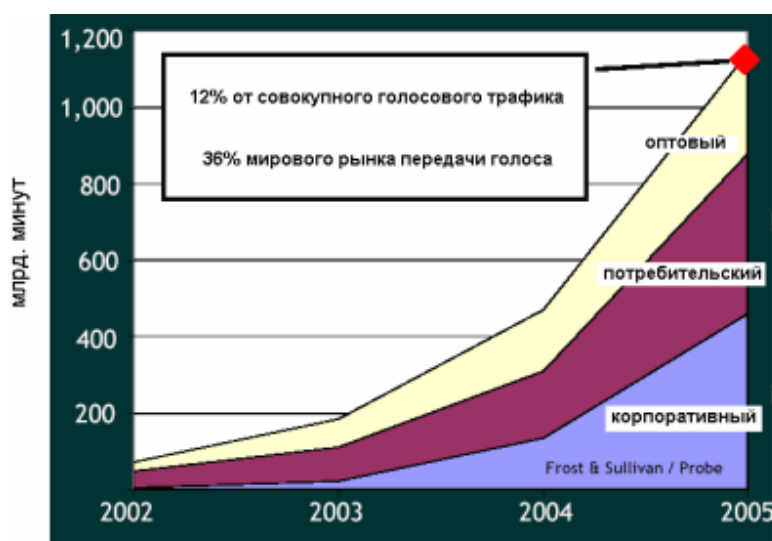


Рис.1. Объем международного трафика IP-телефонии

Из вышеприведенных цифр можно сделать вывод в о том, что перед современными операторами IP сетей остро стоит проблема поиска новых решений по инжинирингу трафика, реконфигурации старых сетей таким образом, чтобы обеспечить бесперебойность и качество в работе в условиях быстрого роста IP трафика. Одним из наиболее перспективных решений в данной области является магистральная сетевая технология

MPLS. Эта технология предоставляет следующие возможности по сравнению с аналогичными транспортными технологиями для IP трафика:

- ускорение скорости продвижения IP-пакетов по сети за счет сокращения времени обработки маршрутной информации до уровня, необходимого для передачи разнородного трафика;
- организация управления трафиком (traffic engineering) в магистральных сетях. С помощью меток каждому информационному потоку (например, несущему телефонный трафик) может назначаться требуемый класс обслуживания (CoS – Class of Service). Потоки с более высоким классом CoS получают приоритет перед всеми другими потоками. Таким образом, с помощью технологии MPLS обеспечивается качество обслуживания (QoS – Quality of Service);
- полное обособление друг от друга виртуальных корпоративных сетей за счет создания для каждой из них туннелей на третьем (стандарт RFC 2547) или втором уровнях эталонной модели взаимосвязи открытых систем (ЭМВОС);
- прозрачный пропуск через ядро IP/MPLS трафика протоколов 2-го уровня ЭМВОС – Ethernet, Frame Relay или ATM. Для этих целей приняты такие стандарты, как PWE3 (Pseudo-Wire Emulation Edge to Edge – псевдо-проводная эмуляция передачи из конца в конец) или PPVPN (Provider Provisioned VPN – поддерживаемые провайдером VPN);

### **1.1.2 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.

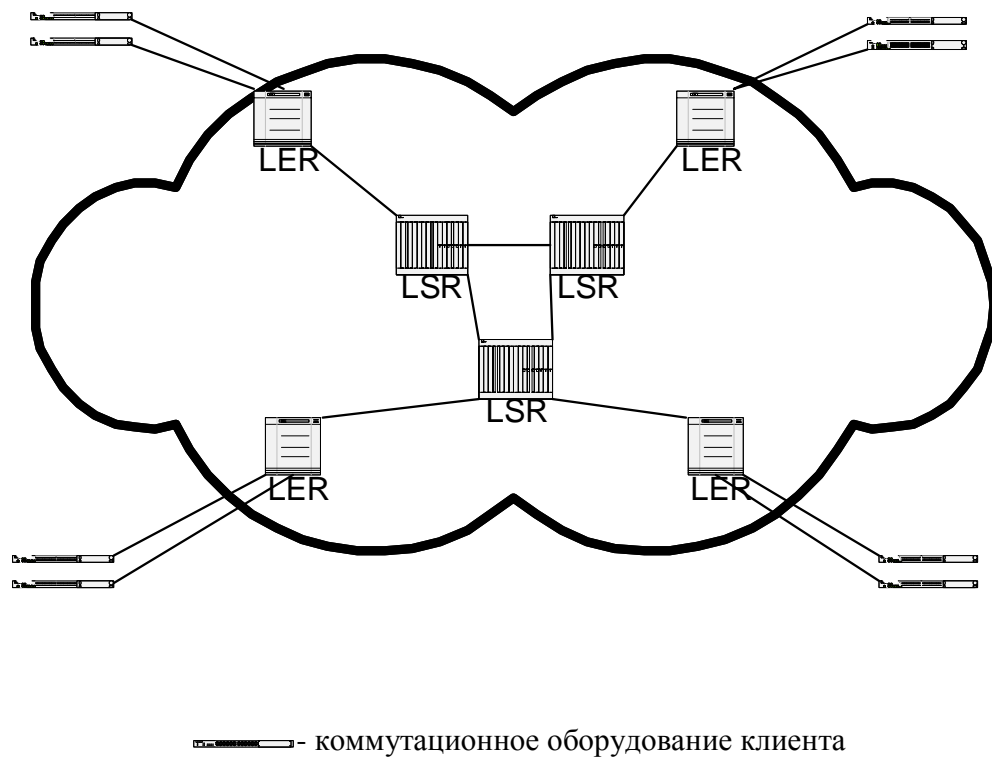
Таким образом, интерес к технологии MPLS со стороны операторов не случаен: эта технология открывает массу возможностей — от формирования трафика с заданными параметрами и его обслуживания в соответствии с выбранной схемой QoS до организации высокозащищенных виртуальных частных сетей (VPN, Virtual Private Networks). Более подробно технология MPLS рассматривается в главе 2 данной дипломной работы.

### **1.1.3 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.

Новейшей концепцией в этой области является концепция виртуальных частных сетей (VPN, рис.2). 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. Компьютеры не должны быть сосредоточены в одном месте или здании. Это, несомненно, удобно, например, если необходима связь между различными филиалами компании или, скажем, между производителями продукции и дилерами. В дополнение к этому при организации виртуальной частной сети намного повышается степень защиты трафика данных, в связи с тем, что вероятность взлома становится фактически равной нулю (среднее время взлома применяемых в настоящее время ключей шифрования оценивается в сотни лет). И вдобавок, как было сказано выше, вы можете получить некоторые дополнительные сервисы.



подробнее подписать рисунок, так как не видно разницы между обычной сетью

MPLS и MPLS VPN

Рис. 2. 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.

#### **1.1.4 Мультисервисный доступ в сетях MPLS**

Среди направлений развития современных средств связи и телекоммуникаций выделяются мультисервисность, конвергенция и интеллектуализация. Речь идет о создании унифицированной сетевой среды в целях повышения эффективности и гибкости обслуживания клиентов при снижении стоимости эксплуатации.

Благодаря поддержке технологий ATM, Frame Relay, MPLS, маршрутизации IP, мультисервисные 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 мультисервисных 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.

Концепция мультисервисности заключается в следующем (рис. 3): 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.).

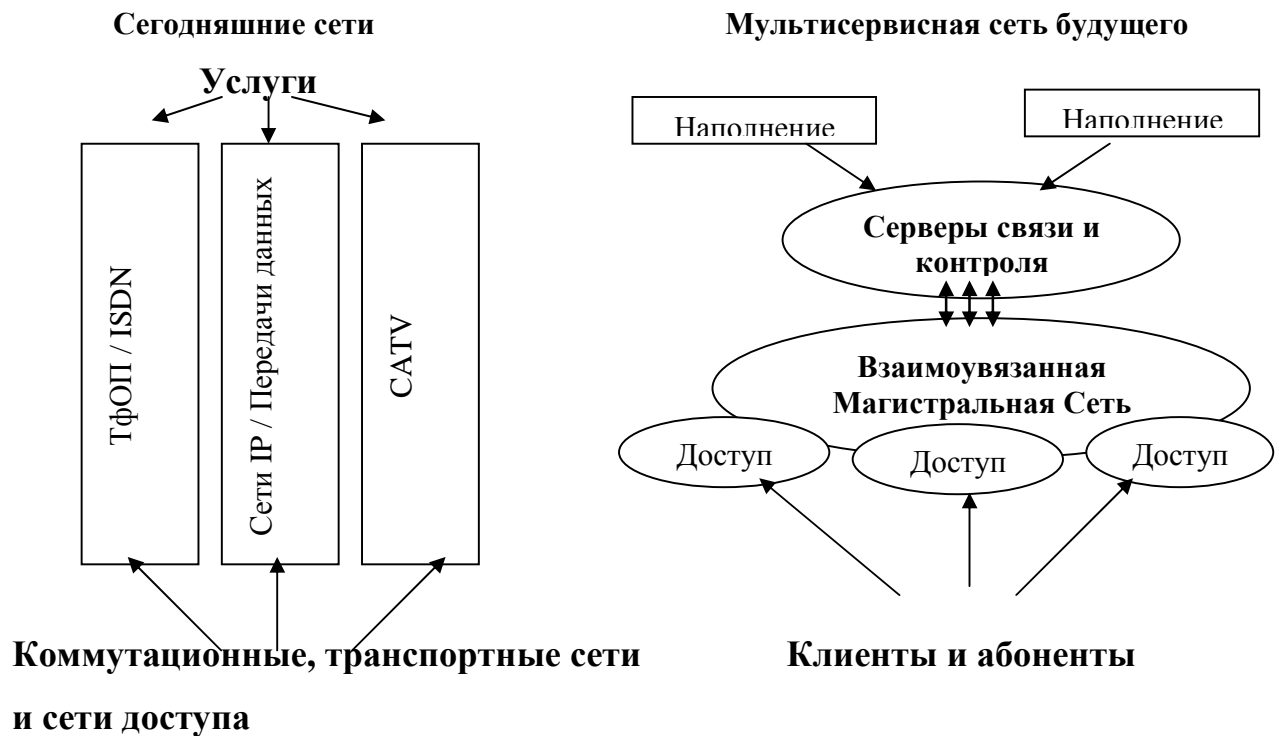


Рис. 3. Сравнение сегодняшних сетей и мультисервисных сетей будущего

Резюмируя параграф 1.1 «Сравнительная оценка возможностей технологии MPLS», автор дипломной работы пришел к нижеизложенным выводам. 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 мультисервисные 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 и 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 объемы 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.

## **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.
- **Управление выходными очередями:** после процесса перезаписи переключатель поместит пакет/кадр, в выходную очередь для последующей коммутации. Управление буфером осуществляется так, чтобы не произошло переполнение. Когда буферы окажутся заполнены до определенного уровня, пакеты/кадры с низким уровнем приоритета отбрасываются, в очереди сохраняются только высокоприоритетные пакеты/кадры.

### **1.2.1 Качество обслуживания в IP – сетях**

Сети IP базируются на двух протоколах передачи данных: UDP (User Datagram Protocol – доставка сообщений в режиме реального времени) и TCP (Transmission Control Protocol – гарантированная доставка сообщений). Рассмотрим достоинства и недостатки каждого из них с точки зрения обеспечения качества обслуживания.

Протокол UDP предоставляет прикладным программам возможность отправлять сообщения другим приложениям, используя минимальное количество параметров протокола. Этот протокол не обеспечивает достоверность доставки пакетов, защиты дублирования данных или надежности от сбоев в передаче. За исключением параметров приложения - номеров портов отправителя и получателя пакета, UDP практически ничего не добавляет к IP-датаграмме. Протокол UDP намного проще, чем TCP и полезен в ситуациях, когда мощные механизмы обеспечения надежности протокола TCP не требуются или будут только помехой для решения определенного рода задач, например, аутентификации пользователей. Тем не менее, не гарантированность доставки является

большим минусом в обеспечении качества обслуживания QoS протоколом UDP, хотя передача трафика в реальном времени (Real Time Transfer), необходимая для некоторых специализированных приложений, - положительный момент обеспечения качества обслуживания QoS в данном протоколе.

Приложения, требующие гарантированного получения потоков данных, должны использовать протокол TCP. Этот протокол обеспечивает сквозную доставку данных между прикладными процессами, запущенными на узлах, взаимодействующих по сети. Протокол IP занимается пересылкой датаграмм по сети, никак не гарантируя доставку, целостность, порядок прибытия информации и готовность получателя к приему данных; все эти задачи возложены на протокол TCP. Протокол TCP требует, чтобы все отправленные данные были подтверждены принявшей их стороной. Он использует таймауты и повторные передачи для обеспечения надежной доставки. Отправителю разрешается передавать некоторое количество данных, не дожидаясь подтверждения приема ранее отправленных данных. Таким образом, между отправленными и подтвержденными данными существует окно уже отправленных, но еще неподтвержденных данных. В итоге, механизмы качества обслуживания QoS протокола TCP предоставляют гарантию доставки информации адресату, но не могут обеспечить выполнение заданных параметров скорости передачи данных.

### **1.2.1.1 Протокол резервирования ресурсов RSVP**

Протокол сигнализации Resource reSerVation Protocol (RSVP) обеспечивает управление резервированием сетевых ресурсов в IP-сети для реализации интегрированных сервисов (Integrated Services, IntServ).

**Технологии** с гарантированной (IntServ Guaranteed) и с контролируемой сетевой нагрузкой (IntServ Controlled) работают по протоколу RSVP. В первом случае речь идет об эмуляции выделенного виртуального канала в IP-сети: потоку гарантируется доступность запрошенной полосы пропускания и, одновременно, задаются жесткие границы для величины суммарной задержки. Технологию IntServ Guaranteed можно воспринимать в качестве технологии для формирования сети коммутации каналов, наложенной на сеть коммутации пакетов. Во втором случае конкретные диапазоны задержек и других параметров передачи не устанавливаются.

Сервисная модель IntServ позволяет организовать гибкое обслуживание разнотипного трафика, максимально учитывая потребности каждого приложения, а использование метода взвешенных очередей для обслуживания пакетов гарантирует предельное значение величины задержки. Эта особенность делает модель IntServ идеальной для обслуживания мультимедийного трафика.

Однако высокая гибкость и "желание" удовлетворить потребности единичных потоков являются источником слабых мест модели IntServ. Основным недостатком модели считается недостаточная масштабируемость. Производительность модели IntServ зависит от количества обрабатываемых потоков, следовательно, такую сервисную модель практически невозможно реализовать в сети с миллионами пользователей. Поэтому стало понятно, что для больших сетей нужна более простая и масштабируемая технология, а область применения модели IntServ ограничилась внутренними и оконечными сетями.

### **1.2.1.2 Технология дифференцированного обслуживания DiffServ**

Разработка технологии Differentiated Services (DiffServ) стала попыткой преодолеть недостатки, присущие протоколу RSVP, прежде всего его плохую масштабируемость. В самом деле, в крупной сети число потоков огромно, и для каждого из них сетевые узлы должны хранить спецификации потока, запроса и фильтра, а также ряд дополнительных сведений. Обработка этой информации способна привести к снижению общей производительности маршрутизаторов.

Технология DiffServ подразумевает отнесение пакетов к тому или иному классу обслуживания с помощью маркеров — кодовых слов, помещаемых в заголовки каждого IP-пакета. Все операции маркировки пакетов реализуются на границе между сетями клиента и провайдера, а магистральным устройствам остается лишь дифференцированно обслуживать небольшое число классов трафика.

Технология DiffServ реализует услуги с различными уровнями "чувствительности" по таким параметрам, как задержка и потеря данных, то есть, не привязывая их к каким-то конкретным величинам и гарантиям. Технология DiffServ не пытается предоставить гарантированный уровень обслуживания (услуг). Вместо этого она стремится к относительному упорядочению различных блоков данных для того, чтобы эти блоки

обрабатывались в разной последовательности, в зависимости от правил поведения, приписанных каждому из них.

Достаточные возможности сети по работе с максимальными объемами трафика, а также (благодаря классификации трафика) определенная степень защиты от трафика с низким уровнем приоритетности позволяет получить желаемый уровень обслуживания. Подготовленность сети к наибольшей загрузке путей передачи трафика также становится гарантией того, что в большинстве случаев и остальной трафик обслуживается должным образом, возможно, при помощи простой дифференциации. В случае перегрузки потоки подстраивают трафик под имеющиеся ресурсы и продолжают работать, хотя и с более низким уровнем качества обслуживания. Преимуществом этой схемы является высокая общая эффективность: получателя достигает большее число потоков, процесс передачи данных становится проще, необходимая поддержка сигнализации сводится до минимума, а механизмы определения маршрута данных значительно упрощаются.

### **1.2.1.3 Многопротокольная технология коммутации по меткам MPLS**

Технология MPLS, в первую очередь, ориентирована не на реализацию конкретной схемы качества обслуживания QoS, а на формирование трафика и оптимизацию процесса его маршрутизации таким образом, чтобы обеспечить максимально выгодное сочетание всех параметров механизмов QoS, задействованных в работе сети. Как показывает практика последних лет, применение технологии MPLS позволяет реализовать гибкое управление сетевыми ресурсами, без которого реализация современных схем качества обслуживания QoS невозможна.

Технология MPLS во многом схожа с технологией DiffServ, здесь также используется маркировка пакетов на входе в сеть MPLS, а их передача напоминает транспортировку трафика по виртуальному каналу в сетях ATM или Frame Relay. Существенное различие между этими технологиями заключается в том, что в сети MPLS присвоение меток нацелено на определение следующего узла на пути следования пакетов, тогда как в DiffServ во главу угла ставится приоритезация трафика.

Уже из краткого описания технологии MPLS видны основные преимущества коммутации по меткам перед обычной маршрутизацией. Алгоритм замены меток предоставляет провайдеру значительную гибкость в управлении маршрутизацией трафика,

поскольку сопоставление пути передачи с конкретным классом эквивалентности может базироваться на самых различных правилах. Оператор получает возможность настроить пути маршрутизации в соответствии с потребностями конкретных приложений, будь то минимальная полоса пропускания, ограничения на задержку или необходимость обойти наименее надежные сетевые узлы.

Тот же подход эффективен для динамического выравнивания нагрузки между различными участками сети, благоприятно сказывающегося на качестве услуг. Наконец, процедура замены меток может быть реализована на аппаратном уровне, а это предоставляет дополнительный выигрыш в производительности.

Подводя итоги параграфа о качестве обслуживания в современных сетях связи и основываясь на статистических исследованиях опыта построения сетей, базирующихся на вышеприведенных технологиях, российскими операторами связи, можно сказать о том, что на сегодняшний день многие из перечисленных нами механизмов качества обслуживания остаются нереализованными или реализованными не в полной мере. Вместе с тем, ведется непрерывная работа по улучшению технологий качества обслуживания QoS и разработке новейших методов обеспечения требуемого современным рынком телекоммуникаций качества обслуживания.

### **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.

#### **1.3.1 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.

Сегодня технология ATM используется в IP-сетях для создания ядра сети с поддержкой нескольких уровней обслуживания и в целях распределения трафика между несколькими высокоскоростными каналами. С появлением технологии MPLS, по крайней мере некоторые Интернет-провайдеры надеются получить эти преимущества без помощи коммутаторов ATM. Для них построение сети целиком на базе маршрутизаторов является вполне логичным и выгодным с точки зрения их профессионального опыта. По иронии судьбы, целая группа провайдеров IP-сетей преследует прямо противоположные цели — использовать технологию MPLS для расширения объемов ATM-коммутации в своей сети. Поскольку фиксированные пути в MPLS - сети ведут себя аналогично виртуальным каналам ATM - сети, то виртуальный канал технологии ATM может быть без труда сопряжен с фиксированным путем MPLS. На самом деле это настолько просто, что стандарт на технологию MPLS определяет соответствующий подход, а некоторые производители (в том числе Cisco) уже реализовали его. Причина расширения присутствия технологии ATM в сетях на базе технологии MPLS кроется в возможности управления качеством обслуживания QoS.

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.

Появление подобных высокоскоростных интерфейсов у коммутаторов ATM даёт возможность операторам нарастить пропускную способность ядра своей сети ATM за счёт введения узлов нового уровня иерархии. Однако такие шаги не исключают необходимости перехода на MPLS-технологию, а лишь отодвигают её на неопределённое время. Понимая неизбежность перехода на технологию MPLS, производители пытаются защитить инвестиции в оборудование операторов связи. Поэтому ещё одной особенностью коммутаторов нового поколения является их повсеместная поддержка технологии IP/MPLS помимо технологии ATM. Одновременная поддержка в магистральных



коммутаторах технологий ATM и IP/MPLS даёт возможность операторам реализовать ещё одну схему их взаимодействия – смешанную.

Собственно это даже не схема, а стратегия постепенной миграции магистрали ATM к IP/MPLS. По мере установки в сеть всё большего количества коммутаторов нового поколения с поддержкой технологии MPLS, оператор сможет увеличить и количество путей LSP (Label Switched Path, маршрут коммутации по меткам) между граничными устройствами, не отказываясь в то же время от уже работающих виртуальных ATM-соединений. При этом производители таких коммутаторов рекомендуют операторам начать с перевода на сети на такую конфигурацию по технологии MPLS, которая будет требовательна к качеству обслуживания трафика, для которого оператор не обязан гарантировать клиентам каких-либо количественных характеристик качества обслуживания QoS. И только «попрактиковавшись» с трафиком подобного класса и накопив опыт работы с технологией MPLS, операторы могут обратиться к переводу на пути LSP других классов трафика (в том числе и чувствительных к задержкам).

### **1.3.2 Краткая характеристика взаимодействия технологий DiffServ и MPLS**

Технология MPLS может оказать помощь провайдерам при внедрении технологии дифференцированных услуг (DiffServ). Сама модель DiffServ определяет целый ряд механизмов для разделения всего трафика на небольшое число классов обслуживания. Как известно, пользователи нуждаются в сети Интернет как в сети общего пользования для самых разных целей и приложений — от неприхотливой электронной почты до передачи голоса и видео, весьма чувствительных к задержкам. Чтобы удовлетворить их требования, сервис-провайдер должен использовать не только моделирование трафика, но и средства для его классификации.

В сетях MPLS возможны два подхода к пересылке пакетов с учетом класса обслуживания. Первый подход предусматривает обработку пакетов в выходных очередях LSR-маршрутизаторов с учетом значений приоритета, указанных в заголовке MPLS. Второй базируется на том, что для каждой пары, состоящей из входного и выходного LSR-маршрутизаторов, определяются несколько LSP-маршрутов с различными характеристиками производительности, полосы пропускания, времени задержки и других

параметров. После этого входной маршрутизатор направляет один тип трафика по одному пути, другой — по другому, третий — по третьему и т. д.

### **1.3.3 Краткая характеристика взаимодействия протокола RSVP и технологии MPLS**

Технология MPLS работает только на маршрутизаторах и не управляется приложениями. MPLS является технологией «конструирования трафика» в той же мере, что и технологией обеспечения качества обслуживания QoS. Маршрутизация MPLS используется для образования виртуальных каналов в IP-сетях, причем предполагается, что для этих каналов выделяются определенные ресурсы маршрутизаторами сети. Способ резервирования и поддержки качества обслуживания остается за пределами технологии MPLS. Например, резервирование может осуществлять как администратор, так и протокол RSVP. Механизмы технологии MPLS обеспечивают сквозные пути передачи потока. При этом отдельные потоки можно объединять в классы, что позволяет добиться высокой масштабируемости и согласованного управления трафиком. Классифицируя потоки трафика, технология MPLS создает эффективный «канал» для этих потоков. Для того чтобы обеспечить эти каналы качеством обслуживания, лучшим, чем в соответствии с принципом best effort (предоставление соединения без гарантий), трафик этих виртуальных каналов не должен превосходить пропускную способность сети. Технология MPLS не содержит механизмы определения потребностей в пропускной способности потоков и назначения необходимых ресурсов для выделенного использования, тогда как эти механизмы входят в состав протокола RSVP. В настоящее время существует предложение использовать в протоколе RSVP «явные маршруты» (explicit route) для направления переключаемых на основе меток потоков RSVP по predetermined маршрутам. Эти потоки будут использовать виртуальные каналы, установленные в MPLS-маршрутизаторах (LSR). Кроме того, можно сделать так, чтобы в MPLS-сетях назначались метки в соответствии со спецификацией потока протокола RSVP. Преимущества будут заключаться в том, что, имея указания в виде меток MPLS, маршрутизаторы могут не заниматься поддержкой состояния по протоколу RSVP. Использование протокола RSVP на границе сети и технологии MPLS в магистральном сегменте может оказаться удачным решением проблемы обеспечения гарантированного качества обслуживания.

## 1.4 Обоснование выбора темы дипломного проекта

Ситуация на рынке современной телекоммуникационной связи такова, что ввод в эксплуатацию сетей, работающих по новым технологиям представляет собой долгий и трудоемкий процесс, требующий постоянного мониторинга, анализа, поиска узких мест и наиболее слабых узлов сети. В первые несколько лет работы сети операторы уделяют больше внимания инсталляции новых устройств и разработке разнообразных алгоритмов, ограничений и других технологических дополнений для установленного оборудования. Подобные частые изменения конфигурации и состава сети подразумевают собой временную нестабильность и сбои в работе, что может привести к потере части клиентского состава, качественные и количественные изменения в характеристиках передачи трафика и так далее. Из всего вышесказанного следует, что современные операторы нуждаются в программных средствах сбора статистики и онлайн-мониторинга работы сети не менее чем в технологических доработках.

Было принято решение создать программный продукт, обладающий вышеназванной функциональностью и использующий в качестве объекта исследования и анализа конфигурацию и связность участка сети MPLS, параметры которого задаются оператором перед началом работы сети. Сети MPLS были взяты за основу в связи с тем, что технология MPLS является новой на рынке телекоммуникаций, обладает большими возможностями, исследования о которых проведены автором в предыдущих пунктах дипломной работы. Задание параметров работы сети было решено сделать вручную, так как это позволяет перебирать большое количество вариантов построения сети и находить оптимальные для задач оператора решения. Кроме того, произведенный анализ позволяет собирать данные о разнообразных элементах сети, как физических, так и концептуальных: маршрутизаторах, путях коммутации, потоках информации от отдельных пользователей, статистику работы сети в целом.

## 1.5 Постановка задачи

Целью данной дипломной работы является разработка программного обеспечения, представляющего собой инструмент по сбору статистической информации в сети, работающей на основе технологии MPLS. Программное приложение должно позволять задавать вручную конфигурацию сети MPLS, задавать исходные параметры работы сети. Созданное программное приложение поможет широкому кругу пользователей, для которых предназначено данное ПО (студентам, операторам связи и др.), внедряющим и изучающим данную технологию, определить следующие качественные и количественные характеристики своей будущей сети за 1 цикл работы:

- Количество маршрутизаторов в данном цикле работы сети;
- Топологию сети (количество отправителей, связность маршрутизаторов и т.д.);
- Загрузку (в %) каждого канала;
- Производительность для каждого из маршрутизаторов;
- Размеры очередей на маршрутизаторах в данном сеансе работы сети;
- Общее количество пакетов, прошедших через маршрутизатор за сеанс;
- Общее количество потерянных пакетов на каждом маршрутизаторе за сеанс;
- Процент потерь пакетов для каждого маршрутизатора за сеанс;
- Среднюю задержку пакета на каждом маршрутизаторе за сеанс;
- Общее количество пакетов каждого потока, прошедших по каждому из коммутируемых путей за сеанс;
- Процент потерь пакетов для каждого потока, прошедших по каждому из коммутируемых путей за сеанс;

В результате работы с приложением пользовательская аудитория должна приобрести навыки выбора наилучшей для поставленного круга задач конфигурации сети MPLS, научиться исследовать модели обслуживания и распределения трафика в сетях MPLS при использовании сопутствующих протоколов маршрутизации, анализировать вышеперечисленные статистические данные и делать на их основе выводы об узких участках сети. На основе программного приложения решено было создать цикл лабораторных работ по анализу процессов маршрутизации разнородного трафика в сетях MPLS.

## **2 ТЕХНОЛОГИЯ MPLS. ОСНОВНЫЕ ПРИНЦИПЫ РАБОТЫ**

Задачей данной дипломной работы является создание программного обеспечения, призванного помочь оператору в анализе наиболее оптимальной конфигурации своей сети, улучшении её отдельных участков и дать представление об основных технических характеристиках оборудования, 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. Исходя из этого, во второй главе автор считает необходимым исследовать базовые принципы работы технологии MPLS и сопутствующих протоколов и решить, какие параметры и характеристики сети должны быть учтены при разработке программного обеспечения.

### **2.1 Введение в технологию MPLS.**

MPLS (MultiProtocol Label Switching) — это технология быстрой коммутации пакетов в многопротокольных сетях, основанная на использовании меток. Технология MPLS разрабатывается и позиционируется как способ построения высокоскоростных IP-магистралей, однако область ее применения не ограничивается протоколом IP, а распространяется на трафик любого маршрутизируемого сетевого протокола.

Традиционно главными требованиями, предъявляемыми к технологии магистральной сети, были высокая пропускная способность, малое значение задержки и хорошая масштабируемость. Однако современное состояние рынка диктует новые правила игры. Теперь поставщику услуг недостаточно просто предоставлять доступ к своей IP-магистрале. Изменившиеся потребности пользователей включают в себя и доступ к интегрированным сервисам сети, и организацию виртуальных частных сетей (VPN), и ряд других интеллектуальных услуг. Растущий спрос на дополнительные услуги, реализуемые поверх простого IP-доступа, обещает принести Интернет-провайдерам огромные доходы.

Для решения этого круга задач и разрабатывается архитектура MPLS, которая обеспечивает построение магистральных сетей, имеющих практически неограниченные возможности масштабирования, повышенную скорость обработки трафика и

беспрецедентную гибкость с точки зрения организации дополнительных сервисов. Кроме того, технология MPLS позволяет интегрировать сети, работающие по технологиям IP и ATM, за счет чего поставщики услуг смогут не только сохранить средства, инвестированные в оборудование асинхронной передачи, но и извлечь дополнительную выгоду из совместного использования этих протоколов.

За развитие архитектуры MPLS отвечает рабочая группа с одноименным названием, входящая в секцию по маршрутизации консорциума IETF. В деятельности группы принимают активное участие представители крупнейших поставщиков сетевых решений и оборудования. Эта архитектура выросла из системы Tag Switching, предложенной Cisco Systems, однако некоторые идеи были заимствованы у конкурирующей технологии IP-коммутиации, созданной компанией Ipsilon, и проекта ARIS корпорации IBM. В архитектуре MPLS собраны наиболее удачные элементы всех упомянутых разработок, и вскоре она должна превратиться в стандарт сетей Интернет благодаря усилиям IETF и компаний, заинтересованных в скорейшем продвижении данной технологии на рынок.

## 2.2 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.

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.).

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.

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 (рис.4). 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. 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.

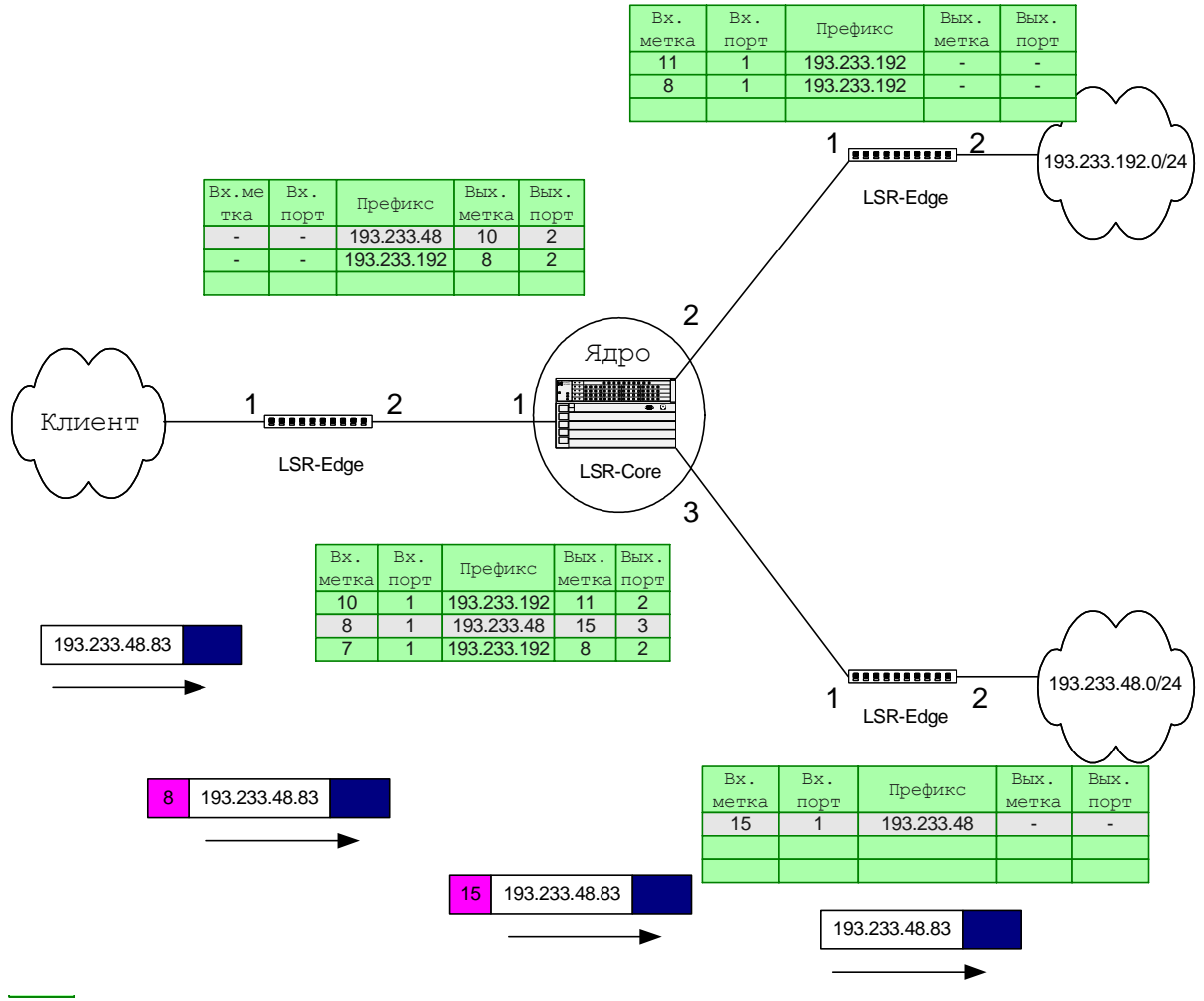


Рис. 4. Схема коммутации IP-пакетов по технологии MPLS.

Поскольку на установление соответствия пакетов определенным классам FEC могут влиять не только IP-адреса, но и другие параметры, нетрудно реализовать, например, назначение различных путей LSP пакетам, относящимся к различным потокам протокола RSVP или имеющим разные приоритеты обслуживания. Конечно, подобный сценарий удастся осуществить и в обычных маршрутизируемых сетях, но решение на базе технологии MPLS оказывается проще и к тому же гораздо лучше масштабируется.

Каждый из классов FEC обрабатывается отдельно от остальных — не только потому, что для него строится свой путь LSP, но и в смысле доступа к общим ресурсам (полосе пропускания канала и буферному пространству). В результате технология MPLS позволяет очень эффективно поддерживать требуемое качество обслуживания, не нарушая



предоставленных пользователю гарантий. Применение в маршрутизаторах LSR таких механизмов управления буферизацией и очередями, как WRED (Weighted Random Early Detection, взвешенное случайное раннее обнаружение) - вероятностный алгоритм управления очередью, который сохраняет среднюю длину очереди малой за счет раннего уведомления адаптивного транспортного протокола о приближении перегрузки, WFQ (Weighted Fair Queing, взвешенное недискриминационное распределение по очереди) - технология управления буферизацией и обслуживанием потоков, способствующая предотвращению перегрузок) или CBWFQ (Class Based WFQ — технология WFQ, действие которой распространяется на несколько классов трафика с совместным доступом к ресурсам), дает возможность оператору сети MPLS контролировать распределение ресурсов и изолировать трафик отдельных пользователей. Использование явно задаваемого маршрута в сети MPLS свободно от недостатков стандартной IP-маршрутизации от источника, поскольку вся информация о маршруте содержится в метке и пакету не требуется нести адреса промежуточных узлов, что улучшает управление распределением нагрузки в сети.

## **2.3 Элементы архитектуры**

### **2.3.1 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 сред с множественным доступом необходим один набор меток на модуль или все устройство. В реальных условиях угроза исчерпания пространства меток очень маловероятна.

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.

### 2.3.2 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.

Стек меток представляет собой последовательность записей. Каждая запись в стек имеет длину 4 октета. Формат такой записи показан на рис.5. 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 верху 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.5 Формат записи стека меток

### 2.3.2.1 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.

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 мультикастинга, и поддержка команды "traceroute". Это означает, что имеется две проблемы, связанные с TTL, которые технология MPLS должна решить:

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

Когда пакет движется по пути LSP, он должен появляться с тем же значением TTL, которое он бы имел, если бы он проходил через ту же последовательность маршрутизаторов, без коммутации меток. Если пакет проходит через иерархию путей LSP, то полное число пройденных шагов-LSR должно быть отражено в его значении TTL.

### **2.3.3 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. Таким образом, если

промежуточные узлы способны посылать протоколно зависимые сообщения об ошибках для помеченных пакетов, все метки в стеке должны отвечать критериям, приведенным выше для меток, которые занесены на дно стека.

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.

### 2.3.3 Компоненты коммутируемого маршрута

Коммутируемый путь (LSP) одного уровня состоит из последовательного набора участков, коммутация на которых происходит с помощью метки данного уровня (рис. 6).

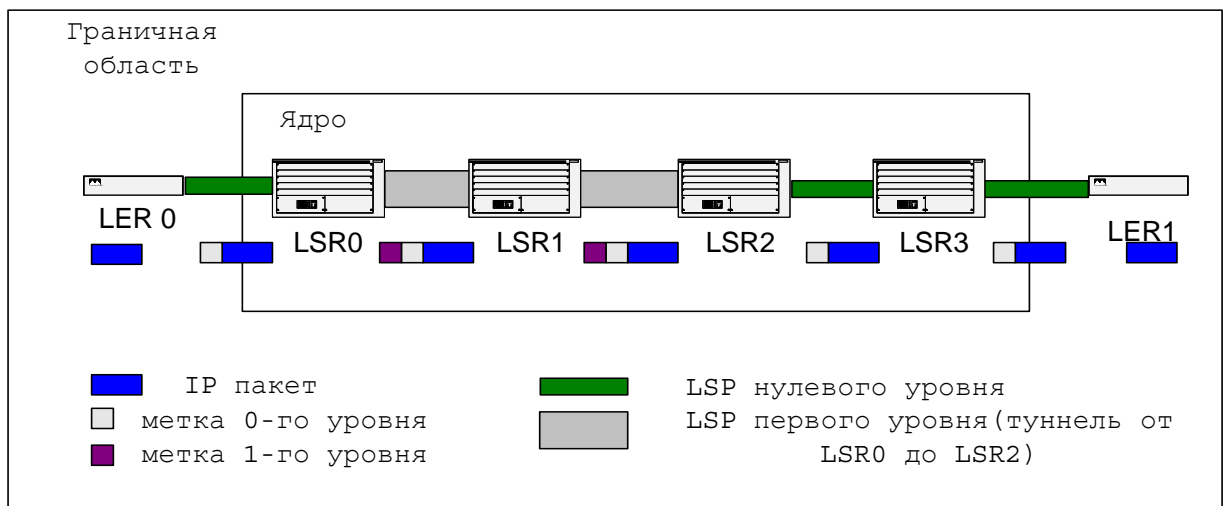


Рис. 6. Компоненты коммутируемого соединения

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.

### **2.3.4 Привязка и распределение меток**

Под привязкой понимают соответствие между определенным классом FEC и значением метки для данного сегмента пути LSP. Привязку всегда осуществляет «нижний» маршрутизатор LSR, поэтому и информация о ней распространяется только в направлении от нижнего LSR к верхнему. Вместе с этими сведениями могут передаваться атрибуты привязки.

Обмен информацией о привязке меток и атрибутах осуществляется между соседними маршрутизаторами LSR с помощью протокола распределения меток. Архитектура MPLS не зависит от конкретного протокола, поэтому в сети могут применяться разные протоколы сетевой сигнализации. Очень перспективно в данном отношении использование протокола RSVP для совмещения резервирования ресурсов и организации путей LSP для различных потоков.

Существуют два режима распределения меток: независимый и упорядоченный. Первый предусматривает возможность уведомления верхнего узла о привязке до того, как конкретный маршрутизатор LSR получит информацию о привязке для данного класса от своего нижнего соседа. Второй режим разрешает высылать подобное уведомление только после получения таких сведений от нижнего маршрутизатора LSR, за исключением случая, когда маршрутизатор LSR является выходным для этого класса FEC.

Распространение информации о привязке может быть инициировано запросом от верхнего устройства LSR (downstream on-demand) либо осуществляться спонтанно (unsolicited downstream).

## **2.3. 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.

Маршрутизация шаг-за-шагом позволяет каждому узлу независимо выбрать следующий шаг для каждого класса FEC. Это обычный режим существующих сегодня IP-сетей. "маршрутизируемый шаг-за-шагом LSP" является путь LSP, чей маршрут выбирается по схеме шаг-за-шагом.

В пути LSP при явной маршрутизации, каждый маршрутизатор LSR не выбирает следующий шаг независимо; скорее один маршрутизатор LSR, обычно вход LSP или выход LSP, специфицирует несколько (или все) LSR в LSP. Если один маршрутизатор LSR специфицирует весь путь LSP, LSP является явно маршрутизированным. Если один маршрутизатор LSR специфицирует только некоторые пути LSP, LSP является "неточно" маршрутизированным.

Последовательность маршрутизаторов LSR, за которой следует явно маршрутизированные пути LSP, могут быть выбраны при конфигурации, или могут быть выбраны динамически одним узлом (например, выходной узел может использовать топологическую информацию, полученную из базы данных состояния канала, для того чтобы вычислить весь путь для дерева с корнем в выходном узле).

Явная маршрутизация может быть полезной для ряда целей, таких как политика маршрутизации или управление трафиком (TE). В технологии MPLS, явный маршрут должен быть специфицирован в момент формирования метки, но явный маршрут не должен быть специфицирован для каждого IP-пакета. Это делает явную маршрутизацию в сетях MPLS более эффективной, чем альтернативную IP-маршрутизацию отправителя.

### **2.3.1 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).

Рассмотрим на примере, как происходит заполнение таблиц меток по протоколу LDP (рис. 7). Предположим, что выбран упорядоченный режим распределения меток LSP со спонтанным распространением сведений о привязке.

На стадии А каждое из устройств сети MPLS строит базу топологической информации, задействуя любой из современных протоколов маршрутизации (на схеме — OSPF, Open Shortest Path First — «первым выбирается кратчайший путь», разновидность протокола маршрутизации внутри автономной системы). На стадии В маршрутизаторы LSR применяют процедуру нахождения соседних устройств и устанавливают с ними сеансы по протоколу LDP.

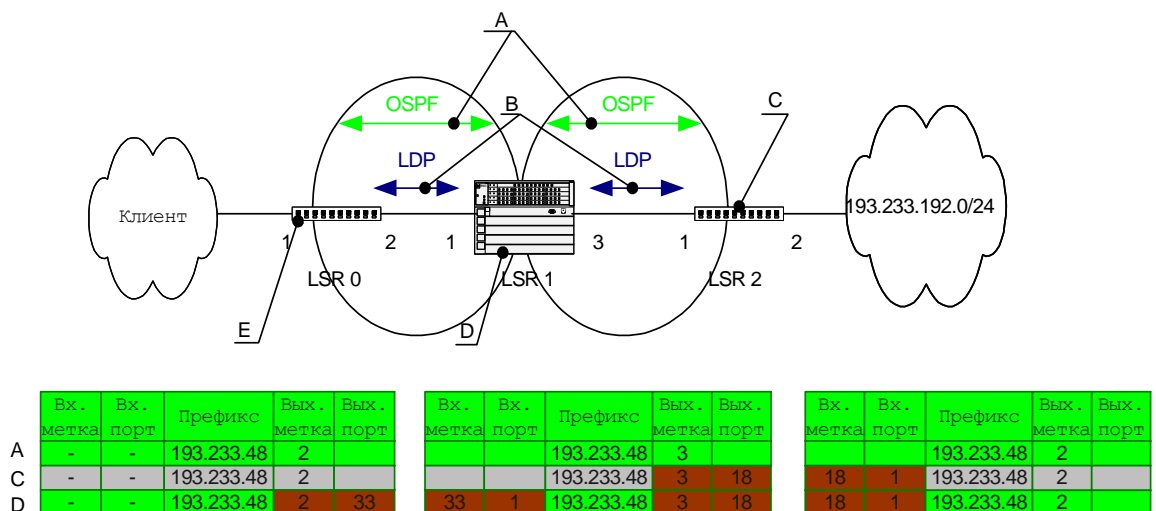


Рис. 7. Построение коммутуемого пути по протоколу LDP

Далее (стадия С) маршрутизатор LSR 2 на основе анализа собственных таблиц маршрутизации обнаруживает, что он является выходным маршрутизатором LSR для пути, ведущего к IP-сети 193.233.48.0. Тогда маршрутизатор LSR 2 ассоциирует класс FEC с пакетами, адрес получателя которых соответствует префиксу данной сети, и присваивает



этому классу случайное значение метки — в нашем случае 18. Получив привязку, протокол LDP уведомляет верхний маршрутизатор LSR (LSR 1) о том, что потоку, адресованному сети с префиксом 193.233.48, присвоена метка 18. Маршрутизатор LSR 1 помещает это значение в поле выходной метки своей таблицы.

На стадии D устройство LSR 1, которому известно значение метки для потока, адресованного на префикс 193.233.48, присваивает собственное значение метки данному классу FEC и уведомляет верхнего соседа (LSR 0) об этой привязке. Теперь маршрутизатор LSR 0 записывает полученную информацию в свою таблицу. После завершения данного процесса все готово для передачи пакетов из сети «клиента» в сеть с адресом 193.233.48.0, т.е. по выбранному пути LSP.

Спецификация класса FEC может содержать несколько компонентов, каждый из которых определяет набор пакетов, соответствующих данному классу. На сегодняшний день определены два компонента FEC: адрес узла (host address) и адресный префикс (address prefix). Пакет классифицируется как принадлежащий к данному классу FEC, если адрес получателя точно совпадает с компонентом адреса узла либо имеет максимальное совпадение с адресным префиксом. В нашем примере узел-маршрутизатор LSR 0 выполняет в процессе передачи классификацию пакетов, поступающих к нему из сети клиента, и (если адрес получателя в них совпадает с префиксом 193.233.48), присвоив пакету метку 33, отправляет его через интерфейс 2.

### 2.3.2 Протокол LDP

Label Distribution Protocol (LDP) – протокол распространения меток. Функции и характеристики протокола:

- Предоставляет возможность маршрутизаторам с коммутацией меток LSR (Label Switching Router) обнаруживать друг друга и устанавливать взаимодействие. Входной маршрутизатор LSR для прокладки пути к какой-либо сети назначения посылает служебное сообщение протокола сигнализации LDP, разработанного специально для решения задачи ускоренной маршрутизации в сетях MPLS. Входной, а также все последующие маршрутизаторы LSR распространяют сообщение протокола LDP вдоль пути на основе IP-адреса назначения пакета и собственных

таблиц маршрутизации. Поэтому путь коммутации меток совпадает с кратчайшим путем стандартных протоколов маршрутизации, причем неважно каких — RIP, OSPF или других;

- Определяет четыре класса сообщений:
  1. *Discovery messages*: сообщения обнаружения – используются для объявления и поддержки присутствия посылающего их маршрутизатора LSR в сети;
  2. *Advertisement messages*: сообщения объявления – для создания, изменения и отмены привязки метки к классу FEC;
  3. *Session messages*: сеансовые сообщения – предназначены для установления, поддержки и разрушения LDP сессий;
  4. *Notification messages*: уведомляющие сообщения – содержат вспомогательную информацию и информацию, сигнализирующую об ошибках;
- Для обеспечения надежности передачи сообщений протокол работает "поверх" протокола TCP, позволяющего обеспечить гарантированность доставки

Метки могут выдаваться нижним маршрутизатором как по собственной инициативе, так и по запросу верхнего. Наконец, возможен "либеральный" или "консервативный" режим распределения меток. В либеральном режиме нижний маршрутизатор LSR раздает метки вышестоящим маршрутизаторам LSR, как имеющим с ним прямую связь, так и доступным лишь через промежуточные маршрутизаторы LSR. В консервативном режиме вышестоящий маршрутизатор LSR обязан принять метку, если ее выдает смежный маршрутизатор LSR, но может отказаться от метки, пришедшей к нему транзитом.

### 2.3.3 Протокол маршрутизации BGP

Все методы многоуровневой коммутации, в том числе и MPLS, базируются на двух основных принципах:

- функций пересылки пакетов и управления этим процессом;
- пакетов с использованием последовательных меток.

Многоуровневая коммутация предполагает четкое разделение всех функций по две компоненты: пересылка пакетов и управление. Управляющая компонента задействует стандартные протоколы маршрутизации (OSPF, BGP-4) для обмена информацией с другими маршрутизаторами. На основе этой информации формируется и модифицируется сначала таблица маршрутизации, а затем, с учетом информации о смежных системах на каждом интерфейсе, - таблица пересылки пакетов. Когда система получает новый пакет, пересылающая компонента анализирует информацию, содержащуюся в его заголовке, ищет соответствующую запись в таблице пересылки и направляет пакет на выходной интерфейс.

Протокол BGP очень устойчив и является базовым протоколом Internet. Основное назначение BGP - передавать другим BGP- информацию о наличии сетей и о структуре этих сетей . BGP формирует единую иерархическую структуру маршрутизации, связывающую в единую MPLS/IP интрасеть различные узлы и сети.

Каждый из компонентов MPLS/IP сети, называемый автономной системой (AS), представляет собой самодостаточный независимый объект, не имеющий полученных каким - логическим путем сведений о других сетях в составе глобальной сети. Актуальность такой функциональности вполне очевидна, поскольку сегодня технически невозможно создать систему, которая имела бы сведения о топологии всех существующих в мире IP - сетей. Решение этой проблемы и берет на себя протокол BGP, позволяя системам, не известным друг другу, свободно устанавливать связь между собой.

В данной дипломной работе автором рассматривается версия 4 протокола BGP, наиболее распространенная на сегодняшний день. Фактически BGP-4 включает в себя два отдельных протокола. Протокол EBGP - External Border Gateway Protocol - используется для маршрутизации данных между автономными системами, о чем и было сказано выше. Второй компонент – это протокол IBGP - Internal Border Gateway Protocol - используется для маршрутизации данных внутри автономной системы.

Еще один принцип положен в основу BGP - принцип вектора расстояния. Протоколы маршрутизации по принципу действия делятся на две категории: протоколы состояния канала и протоколы вектора расстояния. Каждая категория использует свои алгоритмы для определения маршрута между системами, свои формулы вычисления этого маршрута на основании значений метрик, которые указываются в таблице маршрутизации для каждого маршрута. Принцип вектора расстояния подразумевает выбор маршрута

исходя из наикратчайшего пути между системами, определяемого числом пересылок между маршрутизаторами. Протоколы вектора расстояния называют маршрутизацией с помощью последующих пересылок, так как они рассматривают число пересылок (hop) между маршрутизаторами.

Для вычисления маршрута в таких протоколах вектора расстояния обычно применяется алгоритм Беллмана - Форда. Согласно этому алгоритму осуществляются расчет значения метрики (например, стоимости маршрута, задержки и т. д.) для каждой пересылки в сети и поиск минимальных суммарных значений пересылок. При маршрутизации по протоколу BGP пересылки могут осуществляться как между внутренними маршрутизаторами (внутри определенной AS), которые работают под управлением протокола IBGP, так и между внешними маршрутизаторами, соединяющими эти автономные системы AS, в которых маршрутизация выполняется под управлением протокола.

### **2.3.3.1 Протокол IBGP**

Автономные системы являются основной структурной единицей сетей, поддерживающих BGP. Автономная система (AS) - это определенная группа узлов, каким – либо образом связанных между собой. Таким образом, автономная система является средой.

Очевидно, что BGP - маршрутизаторы, находящиеся в одной AS, обмениваются между собой маршрутной информацией. Это необходимо для согласованного отбора внешних маршрутов в соответствии с политикой данной AS и для передачи транзитных маршрутов через автономную систему. Такой обмен производится по протоколу IBGP.

Отличие IBGP от EBGP состоит в том, что при объявлении маршрута соседнему маршрутизатору, находящемуся в той же самой AS, в поле AS\_Path не добавляется номер собственной автономной системы. AS\_Path - список номеров автономных систем, через которые должна пройти датаграмма по пути в указанную сеть. Действительно, если номер AS будет добавлен, и сосед анонсирует этот маршрут далее (с добавлением номера той же AS), то одна и та же AS будет перечислена AS\_Path дважды, что расценивается как цикл. Чтобы не возникло циклов, маршрутизатор не может анонсировать по IBGP маршрут,

полученный также по IBGP, поскольку нет способов определить заикливание при объявлении BGP- внутри одной AS.

Следствием этого является необходимость создания полного графа IBGP-соединений между пограничными маршрутизаторами одной автономной системы: то есть каждая пара маршрутизаторов должна устанавливать между собой соединение по протоколу IBGP. При этом возникает проблема большого числа соединений. Для уменьшения числа соединений применяются различные решения: разбиение AS на конфедерации (подсистемы), применение серверов маршрутной информации и др.

Сервер маршрутной информации (назначенного маршрутизатора в OSPF), обслуживающий группу BGP- маршрутизаторов, работает следующим образом: он принимает маршрут от одного участника группы и рассылает его всем остальным. Поэтому участникам группы нет необходимости устанавливать BGP-соединения попарно, вместо этого каждый из них устанавливает соединение с сервером. Группой маршрутизаторов могут быть, например, все BGP-маршрутизаторы данной AS, однако маршрутные серверы могут применяться для уменьшения числа соединений также и на внешних BGP-соединениях - в случае, когда в одной физической сети находится много BGP- маршрутизаторов из различных AS. Сервер маршрутной информации не является маршрутизатором. То есть в общем случае узел, на котором работает модуль BGP, - не обязательно маршрутизатор. В технических документах этот факт подчеркивается тем, что для обозначения BGP- используется термин BGP-speaker (не router).

### **2.3.3.2 Карты маршрутов**

Карты маршрутов BGP дают администратору возможность, выбрать, какие маршруты будут перераспределяться его спикерами, из огромного числа маршрутов BGP, которыми ежедневно обмениваются маршрутизаторы в сети Интернет. Карты маршрутов работают только на уровне сообщений о корректировках и не фильтруют маршруты, поступающие в маршрутизатор. В карте маршрутов содержатся метрики, по которым выполняется алгоритм маршрутизации. Эти метрики представляют собой назначаемые администратором значения, по которым выбирается наиболее подходящий маршрут для отправки данных среди альтернативных маршрутов к одному и тому же пункту назначения. Как правило, выбирается маршрут, который имеет самое низкое совокупное

значение метрик, или, другими словами, самую низкую стоимость. Администратор может самостоятельно присвоить какому либо маршруту более приоритетное значение метрики. Для технологии MPLS это означает возможность присваивать для трафика определенного типа и от определенного источника необходимый для него приоритет и возможность перераспределить этот приоритет путем динамического изменения метрик.

Наиболее распространенной возможностью применения маршрутной карты является изменение такого атрибута маршрутов BGP, как локальный приоритет (Local Preference).

Когда во время однорангового сеанса происходит разрыв соединения спикера BGP с каким - либо другим маршрутизатором, числящимся в его таблице маршрутизации, то говорят, что происходит флелпинг (flapping) маршрута. Причиной флелпинга может быть сбой в работе процессора или любой другой отказ в канале или во всей сети. Явление флелпинга в одном из маршрутов, когда все спикеры, соединенные с этим маршрутом, продолжают перераспределять информацию об этом маршруте по сети Интернет, может привести к перегрузке маршрутизатора, отправляющего сообщения по неисправному маршруту. Для избежания этого разработана система демпфирования флелпинга (flap dampening), принцип работы которой состоит в удалении из таблиц маршрутизации маршрутов, подверженных флелпингу на протяжении определенного времени. Когда маршруты временно отключаются при демпфировании, впоследствии после восстановления работоспособности они ожидают определенное время до вхождения в рабочий режим.

Рассмотренные выше маршрутные карты помогают администратору изменять значение метрик, которые в протоколе BGP называются атрибутами и определяют алгоритм маршрутизации. Приведём наиболее важные из атрибутов, используемых маршрутизаторами BGP при выборе маршрутов:

- Атрибут путь AS (AS-Path) включается в сообщение о корректировке BGP и подсчитывает число AS, через которые проходит сообщение о корректировке на пути к пункту назначения;
- Атрибут следующая пересылка (Next Hop) работает аналогично AS-Path; однако он указывает IP- интерфейса маршрутизатора, используемого для достижения определенной AS;

- Атрибут источник (origin) указывает, от какого источника поступило данное сообщение о корректировке, является ли маршрут внутренним (IBGP) или внешним (EBGP). Атрибут origin может иметь одно из трех значений: IGP, EGP или незавершенный;
- Атрибут локальный приоритет (Local Preference) используется для определения преимущества одного маршрута перед другим, когда имеется два и более равноценных маршрута к пункту назначения. В этом случае маршрутизатор сравнивает атрибуты Local Preference для выбора предпочтительного маршрута. Чем выше локальный приоритет маршрута, тем выше вероятность его использования.
- Атрибут Aggregator это необязательный атрибут, содержащий в начальных 2 байтах номер последней AS, сформировавшей объединённый маршрут, и в следующих 4 байтах IP-адрес BGP-спикера, сформировавшего объединённый маршрут. Создание объединённого маршрута - это процесс комбинирования характеристик нескольких отдельных маршрутов таким образом, что для них может быть объявлен один общий объединённый маршрут.

### 2.3.4 Протокол маршрутизации OSPF

Протокол состояния каналов OSPF (Open Shortest Path First, «кратчайший путь - первым») осуществляет алгоритм выбора маршрута на базе информации о состоянии канала, используя при этом любую из следующих метрик: ширину полосы пропускания, задержку, надежность, нагрузку и т. д.

Для осуществления маршрутизации в сети MPLS необходимо заполнить таблицы меток в маршрутизаторах LSR по протоколу LDP. Для этого каждое из устройств сети MPLS строит базу топологической информации, задействуя любой из современных протоколов маршрутизации. В том числе может использоваться и протокол OSPF. Маршрутизатор, используя процедуры OSPF, обнаруживает соседние маршрутизаторы, после чего становится «видимой» структура сети. Это дает возможность маршрутизаторам LSR с помощью протокола LDP находить соседние LSR и устанавливать с ними сеансы LDP.

Таким образом, протокол OSPF является одним из вспомогательных средств, используемым в технологии MPLS.

#### **2.3.4.1 Базы данных протокола OSPF**

В каждом маршрутизаторе, работающем по протоколу OSPF, имеются три типа баз данных:

- Смежная база данных (таблица соседей), используется маршрутизатором для хранения информации о соседних маршрутизаторах OSPF, непосредственно соединенных с тем же локальным сегментом сети. В начале работы маршрутизатора OSPF в диалоговом режиме, он обнаруживает все соседние локальные OSPF-маршрутизаторы и рассылает приветственные пакеты по групповому адресу 224.0.0.5 для представления себя соседним маршрутизаторам, которые, в свою очередь, добавляют новый маршрутизатор в свою таблицу соседей и отвечают на приветствие своими собственными приветственными сообщениями, в которых идентифицируют себя. В результате каждый маршрутизатор создает свою смежную базу данных.
- База состояния каналов (карта) содержит данные обо всех сетях, подсетях и пунктах назначения в пределах области OSPF. Она формируется путем обмена информацией между соседними маршрутизаторами (в смежную базу данных) и является полной топологической схемой своей области OSPF. Используя эту базу данных состояния каналов, каждый маршрутизатор создает древовидную структуру, в которой он сам является «корнем дерева», соединенным с каждым пунктом назначения наикратчайшим путем.
- База передачи данных (маршрутизации) сохраняет наилучшие маршруты к сетям, подсетям и пунктам назначения OSPF. Эта база формируется на основе базы данных состояния каналов и является фактически таблицей маршрутизации, по которой маршрутизатор запускает алгоритм SPF для вычисления лучших маршрутов ко всем известным пунктам назначения.



### 2.3.4.2 Принципы работы протокола OSPF

Работу протокола OSPF в общем случае можно представить следующим образом: вначале идёт распространение информации о топологии сети. На базе обмена этими сообщениями (router links advertisement - объявление о связях маршрутизатора) каждый маршрутизатор строит граф связей сети, в котором вершинами графа являются маршрутизаторы, а ребрами - интерфейсы маршрутизаторов.

После инициализации OSPF-маршрутизаторы знают только о связях с непосредственно подключенными сетями. Каждый маршрутизатор посылает сообщение HELLO по всем своим интерфейсам, распространяя данную информацию своим соседям, так что каждый маршрутизатор узнает идентификаторы своих ближайших соседей. Эта топологическая информация начинает распространяться по сети от соседа к соседу, пополняя топологические базы новой информацией, и через некоторое время достигает самых удаленных маршрутизаторов.

В результате распространения топологической информации все маршрутизаторы сети располагают идентичными сведениями о графе сети, которые хранятся в топологической (каналов) базе данных каждого маршрутизатора. Далее выполняется нахождение оптимальных маршрутов с помощью полученного графа, причем каждый маршрутизатор считает себя центром сети и ищет оптимальный маршрут до каждой известной ему сети. В каждом найденном таким образом маршруте запоминается только один первый шаг до следующего маршрутизатора, в соответствии с принципом одношаговой маршрутизации. Задача нахождения оптимального пути на графе является достаточно сложной и трудоемкой. В протоколе OSPF для ее решения используется итеративный алгоритм Дейкстры. Если несколько маршрутов имеют одинаковую метрику до сети назначения, то в таблице маршрутизации запоминаются первые шаги всех этих маршрутов.

Все маршрутизаторы, сети и подсети, поддерживающие OSPF, логически объединены в одну область или в некоторую иерархию зон, позволяющую локализовать изменения маршрутов и трафик корректировки маршрутов в пределах каждой зоны. Таким образом, объединенная сеть, использующая протокол OSPF, независимо от того, состоит ли она из единственной или включает множество зон, представляет собой одну автономную систему - один домен маршрутизации.

Благодаря иерархической структуре зон, уменьшаются перегрузки, связанные с поддержкой огромных таблиц маршрутизации и пересчетом этих таблиц в случае изменения маршрутов. Сообщения о корректировках являются инициированными, т.е. они посылаются, только если в сети происходят изменения. Инициированные сообщения рассылаются всем маршрутизаторам OSPF, что сокращает время сходимости. Кроме того, каждое сообщение о корректировке включает только изменение маршрутной информации, а не всю таблицу маршрутизации. Сообщения о корректировках относятся только к измененным маршрутам внутри отдельной зоны OSPF.

## **2.4 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.

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. 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 ТЕ в RFC 2702 "Requirements for Traffic Engineering Over MPLS" ("Требования для управления трафиком в сетях MPLS"). В данном документе, содержащем общие рекомендации IETF по решению задач ТЕ с помощью MPLS, в качестве целевой функции оптимизации путей предложено выражение:  $\min (\max K_i)$ , где  $K_i$  - коэффициент использования  $i$ -го ресурса.

Другим способом постановки задачи ТЕ стал поиск такого набора путей, при которых все значения коэффициентов использования ресурсов не будут превышать некоторый заданный порог  $K_{\max}$ . Подобный подход более прост в реализации, так как связан с перебором меньшего количества вариантов, поэтому он чаще применяется на практике. Однако мало найти решение - надо его реализовать. После того как пути заданы, необходим механизм, посредством которого пакеты, относящиеся к определенному потоку трафика, направлялись бы именно через выбранные промежуточные маршрутизаторы. Эта задача для сетей IP не тривиальна, так как основной режим маршрутизации предлагает единственный "кратчайший" маршрут, а режим маршрутизации от источника, когда отправитель пакета сам задает точную последовательность промежуточных узлов вдоль пути, обладает несколькими очень серьезными ограничениями. Во-первых, он поддерживается для текущей четвертой версии протокола IP далеко не всеми производителями оборудования. Во-вторых, при выборе маршрутизации от источника степень избыточности служебной информации значительно повышается, так как каждый пакет содержит все адреса промежуточных маршрутизаторов, а их может быть и не так уж мало. В-третьих, этот режим чрезвычайно уязвим с точки зрения безопасности; именно поэтому администраторы при конфигурировании маршрутизаторов, как правило, его отключают.

Используемая в MPLS техника продвижения пакетов типична для сетей с виртуальными каналами, в частности для таких достаточно проработанных решений, как ATM и Frame Relay. Но тогда возникает вопрос, зачем понадобилось создавать новую

технологии, когда можно пользоваться уже существующими? Дело в том, что главная особенность и достоинство MPLS заключаются не в технике продвижения пакетов, а в способе выбора и установления пути коммутации меток. Если традиционные технологии определяют свои виртуальные пути только на основе собственной информации о топологии сети, то MPLS привлекает к решению этой задачи интеллектуальные возможности протокола IP. Это позволяет ускорить передачу трафика, более рационально загрузить сеть, устранить дублирование функций на канальном и сетевом уровнях, а также во многих случаях исключить необходимость выполнения большого объема ручной работы при прокладке виртуальных каналов. Рассмотрим, например, работу IP поверх ATM - очень популярный сегодня способ организации магистральных сетей. Коммутируемые виртуальные каналы (SVC) для трафика IP прокладываются на основе информации о топологии сети коммутаторов ATM, которые они получают от протокола маршрутизации PNNI. Такой подход имеет два недостатка. Во-первых, перед передачей данных возникает задержка, равная времени установления коммутируемого виртуального канала, во-вторых, поддерживаются две системы маршрутизации трафика - на уровне IP (протоколы BGP, OSPF, IS-IS или RIP) и на уровне ATM (протокол PNNI). При использовании постоянных коммутируемых каналов (PVC) проявляются другие недостатки: большое количество ручной работы по выбору путей, их установлению и изменению, низкая масштабируемость полносвязной схемы, когда все маршрутизаторы IP связаны друг с другом; наличие промежуточных узлов, замедляющих продвижение пакетов при неполносвязной схеме соединений маршрутизаторов.

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. Собственно, прародительница MPLS - технология IP-коммутации компании Ipsilon - и появилась в свое время как решение по обеспечению тесной интеграции IP и ATM за счет установки в сети комбинированных устройств IP/ATM с общими протоколами маршрутизации и общей топологической базой данных. Прокладка пути заключается в создании во всех LSR вдоль пути следования согласованных таблиц

коммутации, на основе которых продвигались бы пакеты с метками MPLS. Для этого предназначены протоколы сигнализации, разработанные специально для MPLS, или же модернизированные протоколы других технологий. Особую роль в сети выполняют пограничные LSR, т. е. те устройства, часть интерфейсов которых связана с маршрутизаторами, не поддерживающими MPLS. Они должны в общем случае выполнять классификацию, входной контроль, создание заголовков MPLS и задание для входящего в домен MPLS трафика начального значения метки соответствующего пути, а при выходе трафика из этого домена - удаление заголовка MPLS и отправку пакета по его IP-адресу назначения. Все промежуточные LSR вдоль пути просто продвигают пакет на основе значения поля метки. При решении задачи ускоренного продвижения пакетов, пути коммутации меток прокладываются вдоль тех маршрутов, которые указаны в таблицах маршрутизации модулей IP всех LSR сети. Входной LSR для прокладки пути к какой-либо сети назначения посылает служебное сообщение протокола сигнализации (Label Distribution Protocol, LDP), разработанного специально для решения задачи ускоренной маршрутизации в сетях MPLS.

#### **2.4.1 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.

## 2.5 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.

Анализируя выводы, сделанные в результате исследований, произведенных автором во второй главе, 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.

### **3. РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ**

#### **3.1 Обоснование выбора языка программирования**

На сегодняшний день наиболее популярными средами визуальной разработки являются Visual C++ фирмы Microsoft и Delphi фирмы Borland. Среда разработки Delphi неслучайно выбрана для разработки программного обеспечения данной дипломной работы. Эта среда разработки является визуальной, то есть позволяет видеть приложение до его непосредственной компиляции и выполнения. Причем в среде Delphi средства визуальной разработки отличаются в лучшую сторону от аналогичных механизмов языка программирования Visual C++ с точки зрения удобства использования.

В настоящее время большинство персональных компьютеров работает под управлением операционной системы Windows, однако все большую популярность набирает операционная система Linux. В этом отношении последняя разработка компании Borland - Delphi 7 Studio выгодно отличается от последних разработок Visual C++, так как язык Delphi теперь можно устанавливать как на персональных компьютерах, работающих под управлением ОС Windows, так и под управлением ОС Linux. Delphi 7 Studio включает в себя лучшую среду разработки для Linux - Borland Kylix 3 for Delphi. К тому же Borland Delphi 7 Studio обеспечивает давно ожидаемый разработчиками путь перехода к Microsoft .NET. При использовании Delphi выбор платформы всегда остается за программистом.

Немаловажным фактором является то, что Borland Delphi 7 Studio воплощает концепцию быстрой разработки, предоставляемую Model Driven Architecture и визуальной средой UML.

UML – это унифицированный язык моделирования (UML, Unified Modeling Language), он является преемником методов объектно-ориентированного анализа и проектирования (OOA&D), которые появились в конце 80-х и начале 90-х годов. Язык UML прошел процесс стандартизации в рамках консорциума OMG (Object Management Group) и в настоящее время является стандартом OMG. UML – это название языка моделирования, но не метода. Большинство методов включают в себя, по крайней мере язык моделирования и процесс. Язык моделирования – это нотация (главным образом, графическая), которую используют методы для описания проектов. Процесс - это



рекомендация относительно этапов, которые необходимо выполнить при разработке проекта.

Разделы многих книг по методам, в которых описывается процесс, выглядят поверхностно. Большинство программистов, утверждающих, что они используют метод, на самом деле используют язык моделирования, изредка при этом соблюдая требования процесса. Таким образом, зачастую язык моделирования является наиболее важной частью метода. Кроме того, язык, несомненно, является главным средством общения. Если необходимо обсудить с кем-либо проект, то каждый из участников дискуссии должен понимать именно язык моделирования, а не процесс, который используется при разработке этого проекта.

Как видно из вышеизложенного, среда Delphi является одной из ведущих сред визуального программирования, а новые версии Delphi, в частности Borland Delphi 7 Studio, а также Kylix, вобравшие в себя последние разработки в области проектирования – UML и в области программирования - Microsoft NET, позволяют уже сейчас говорить о том, что созданные проекты будут соответствовать последним достижениям в области разработки программных продуктов.

Языком разработки программного обеспечения для создания инструментов конфигурации и анализа функционирования магистральной сети по технологии MPLS был выбран Delphi 5.0. Хотя часть dsitghbdtltyys[ концепций и не была реализована в Delphi 5.0, но совместимость приложений Delphi снизу-вверх (то есть проекты, созданные в более ранних версиях Delphi могут быть активизированы и доработаны в последующих версиях) позволяет работать с проектами, созданными в предыдущих версиях, и пользоваться всеми мощными средствами языка Borland Delphi 7 Studio.

### **3.2 Возможности языка Delphi 5.0, задействованные при написании программного приложения**

Для разработки программного обеспечения решено было задействовать следующие стандартные элементы языка программирования Delphi 5.0:

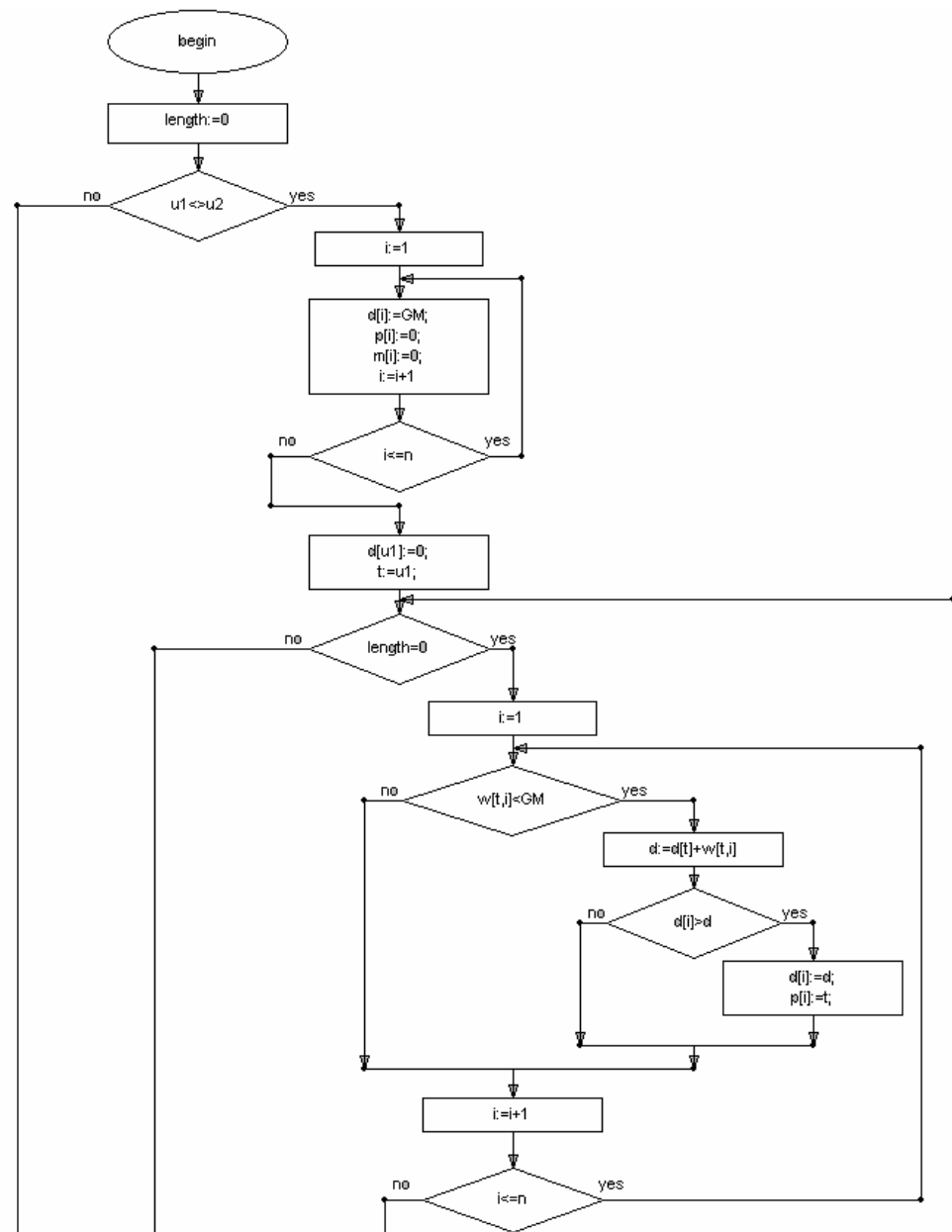
- 1).

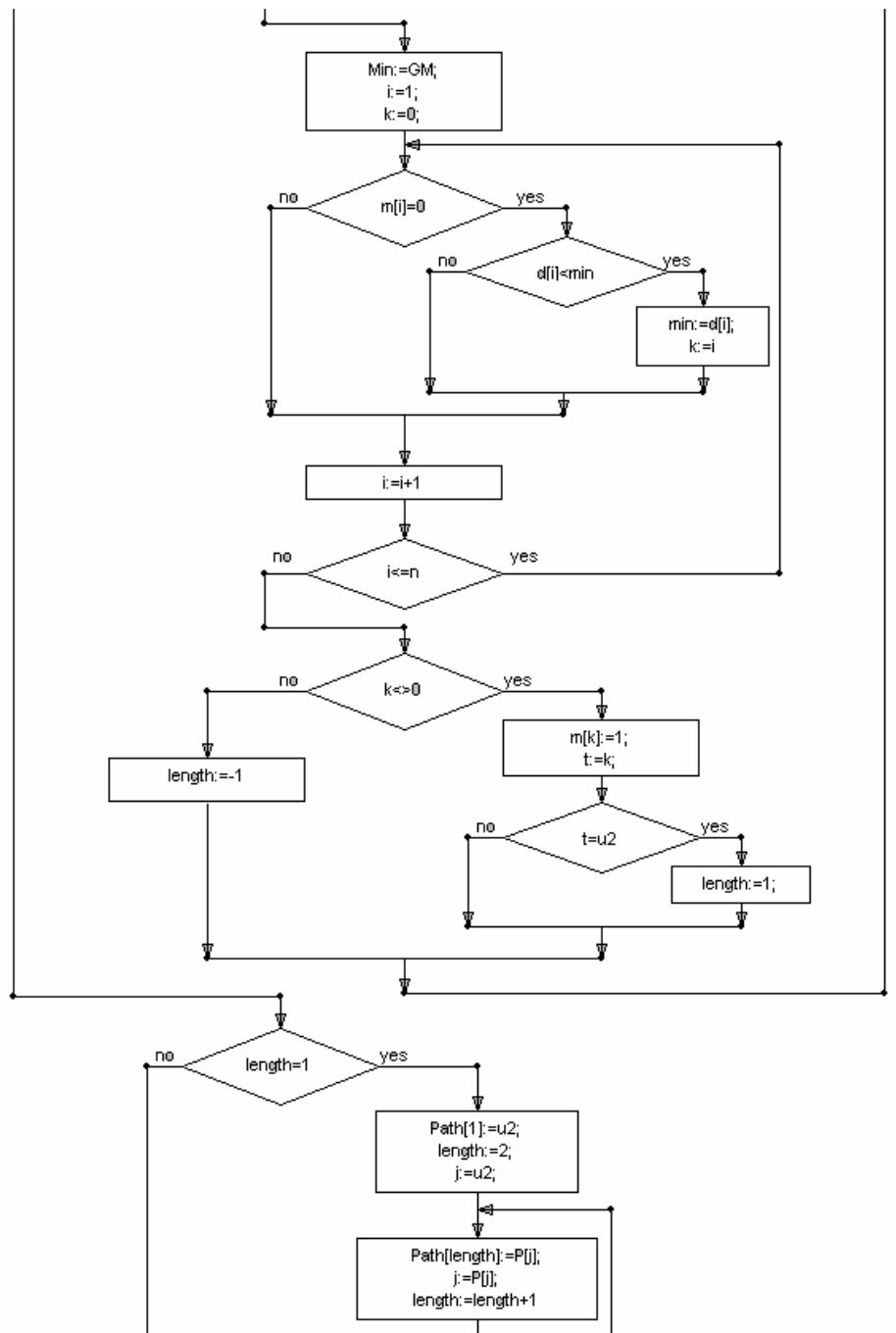
### 3.3 Разработка алгоритмов работы программы

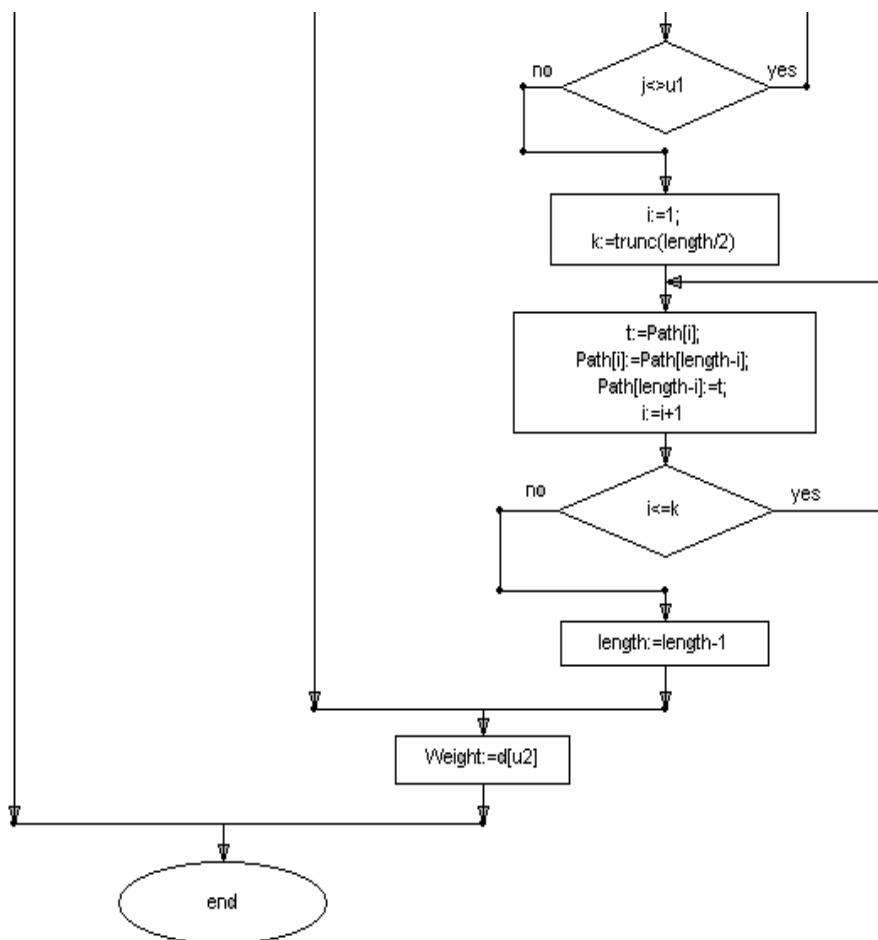
#### 3.3.1 Алгоритм поиска наикратчайшего пути от отправителя к получателю

Для поиска наикратчайшего пути от отправителя к получателю автором дипломной работы решено было разработать алгоритм, основанный на использовании элементов алгоритма Дейкстры для поиска минимального расстояния во взвешенном графе. Начальной вершиной будем считать входной для трех отправителей маршрутизатор LSR ( $u_1$ ), выходной – граничный маршрутизатор LER ( $u_2$ ) на стороне получателя. Веса представляют собой расстояния между маршрутизаторами. Веса заданы при помощи матрицы  $W$ . В результате работы алгоритма получаем длину пути ( $length$ , сумма всех весов на данном пути). Длина пути = 0 если начальная вершина является конечной и = -1 если пути не существует. Для реализации последнего случая в программе должен быть предусмотрен вывод соответствующей ошибки. В алгоритме обозначено:

- $Weight$  – вес пути;
- $Path$  – последовательность номеров маршрутизаторов, определяющая путь;
- $GM$  – переменная, используемая для обозначения максимально возможного числа.







### 3.3.2 Алгоритм сбора статистических данных для подсчета процента потерь пакетов на каждом маршрутизаторе

В связи с тем, что ведение статистики, учитывающей потери информации, является важнейшей частью для анализа рабочих характеристик современных маршрутизаторов сетей MPLS, было решено разработать данный алгоритм.

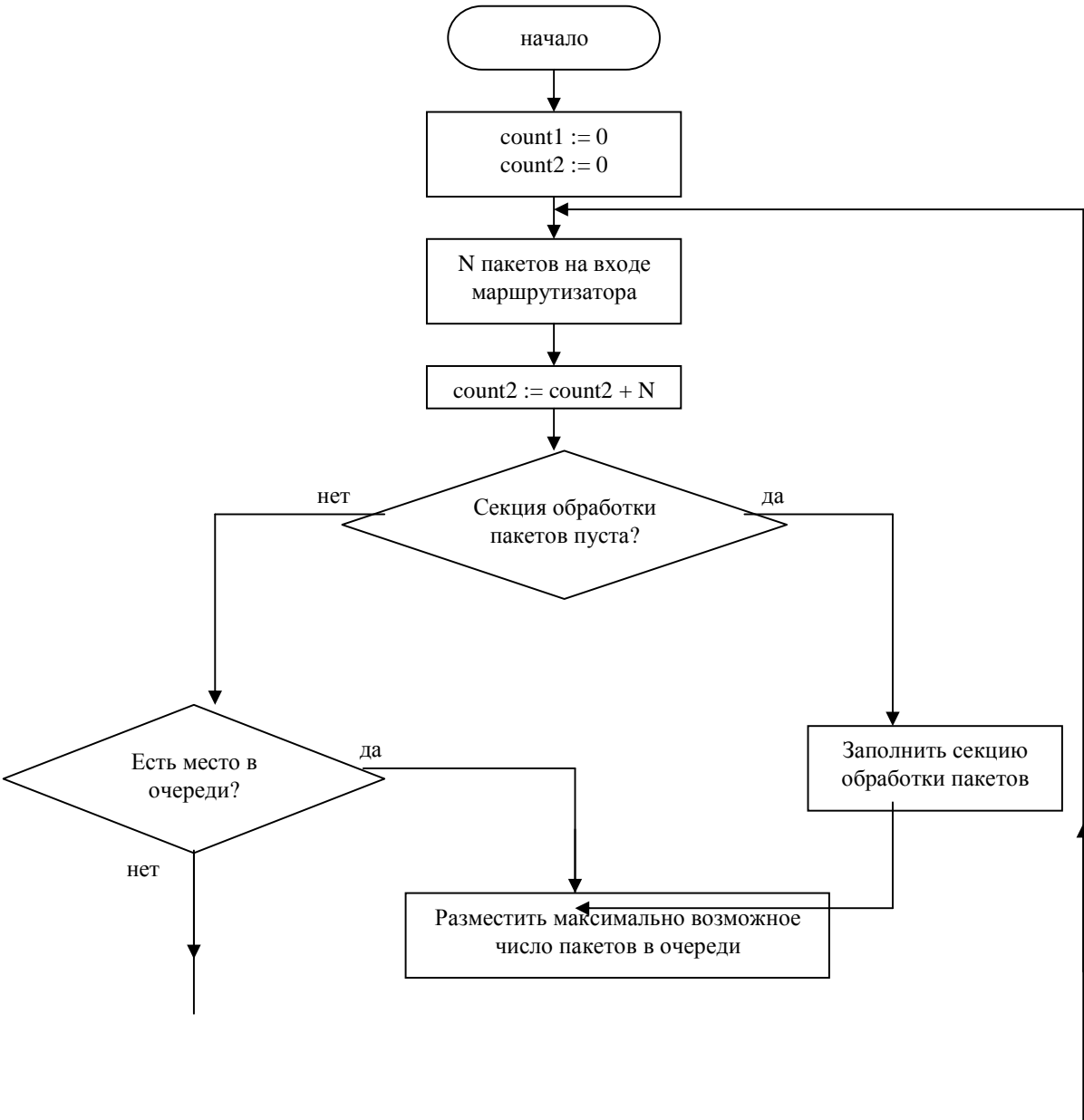
Учет потерь пакетов необходим для передачи приоритетной информации, такой как голосового и видео трафика, так как большой процент потерь ведёт к резкому ухудшению качества обслуживания, что неприемлемо для приложений этого вида.

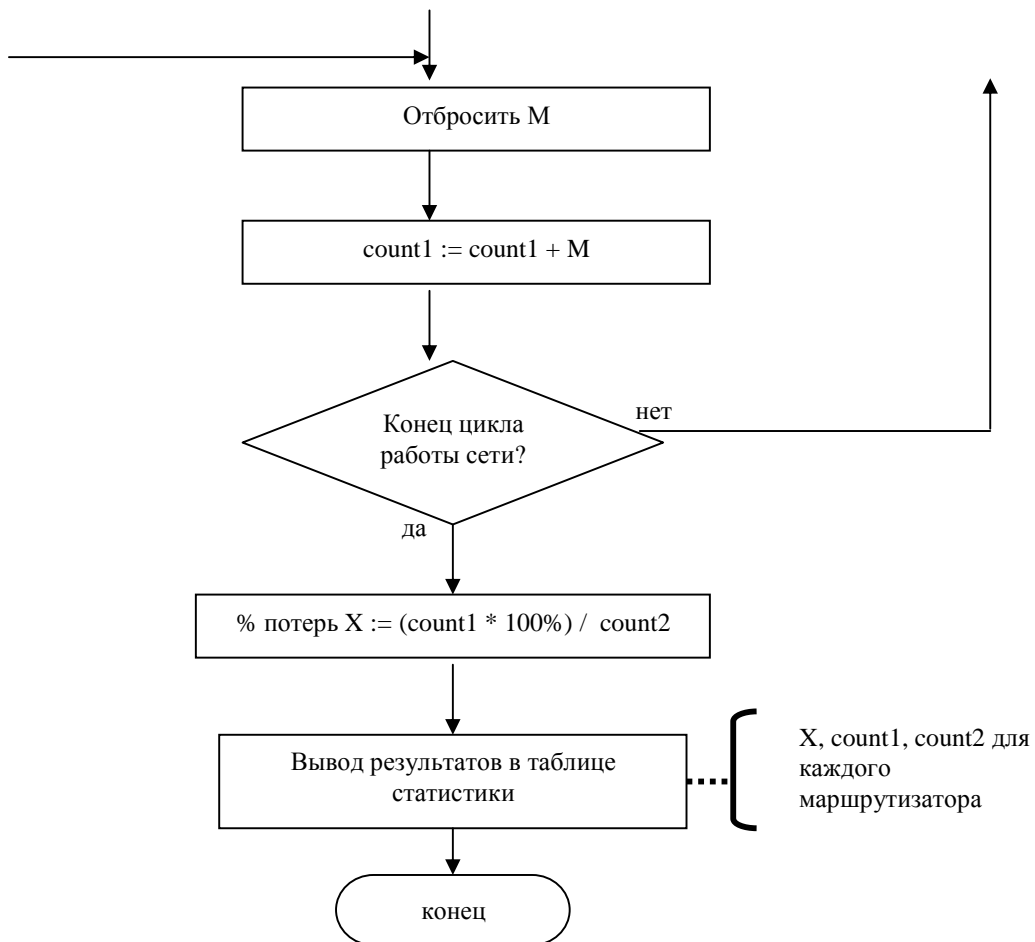
В разрабатываемом алгоритме используются следующие условные обозначения:

- count 1 – счетчик числа пакетов, прошедших через маршрутизатор за сеанс работы сети;

- count 2 – счетчик числа отброшенных пакетов на маршрутизаторе за сеанс работы сети;
- N – число пакетов на входе маршрутизатора;
- M – непоместившиеся в очередь пакеты.

На каждом маршрутизаторе организована очередь на ожидание освобождения секции обработки. Под секцией обработки понимается та часть программного обеспечения маршрутизатора, которая производит замену метки в пакете. Размер секции обработки (одновременно обрабатываемое число пакетов) и максимальный размер очереди задаются вручную в начале работы программы после завершения процессов конфигурации сети и поиска путей.





### 3.3.3 Алгоритм расчёта средней задержки пакета на маршрутизаторе за сеанс работы сети

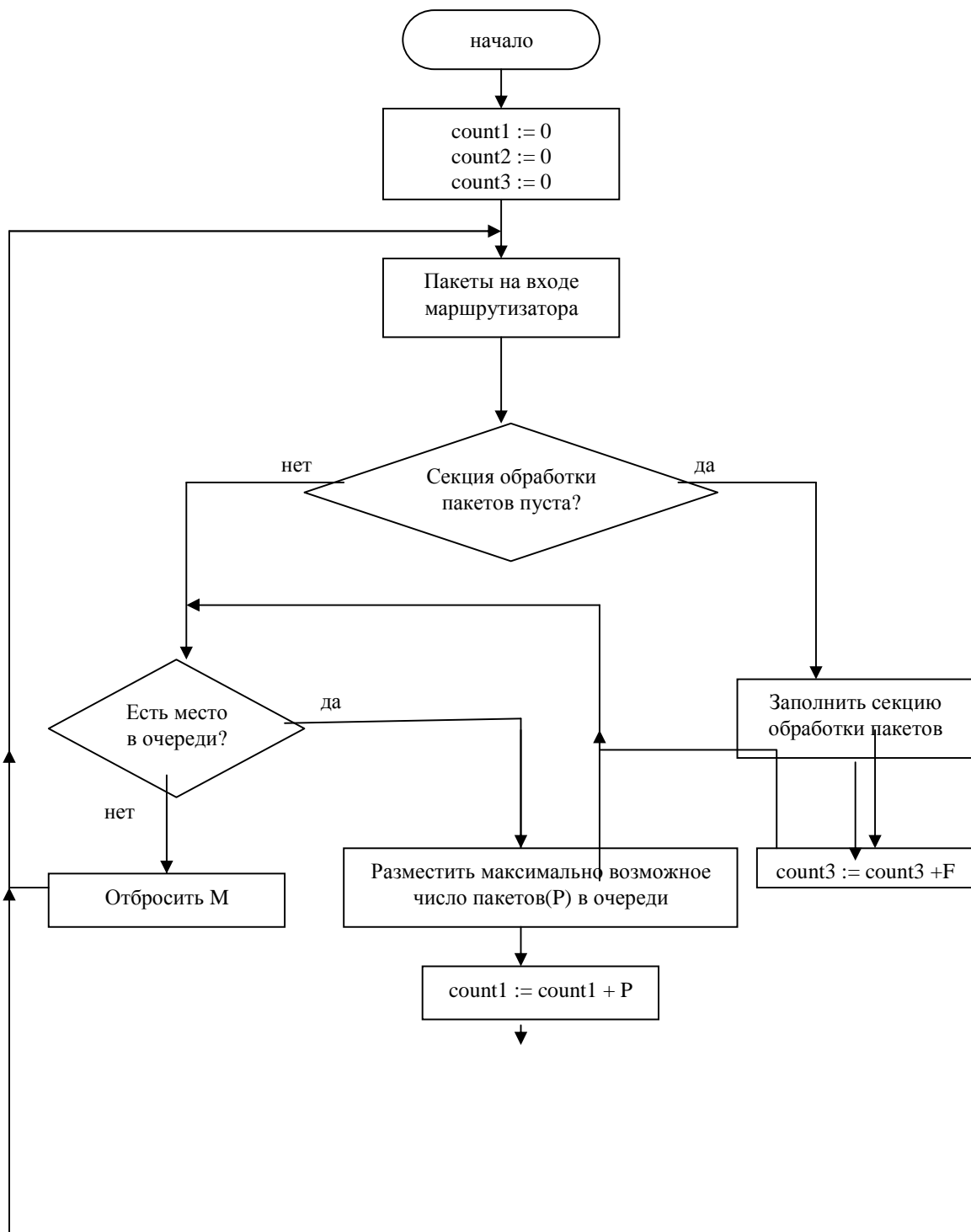
Параметр «средняя задержка пакета на маршрутизаторе» является не менее важной характеристикой обеспечения качества обслуживания в сетях MPLS. Особенно это касается приоритетного трафика, для которого устанавливается критическое значение времени задержки, превысив которое может быть потерян целый поток данных.

Данный алгоритм вычисляет среднее время задержки на маршрутизаторе путем взятия среднего арифметического от суммы задержек всех неотброшенных пакетов, прошедших через маршрутизатор за сеанс.

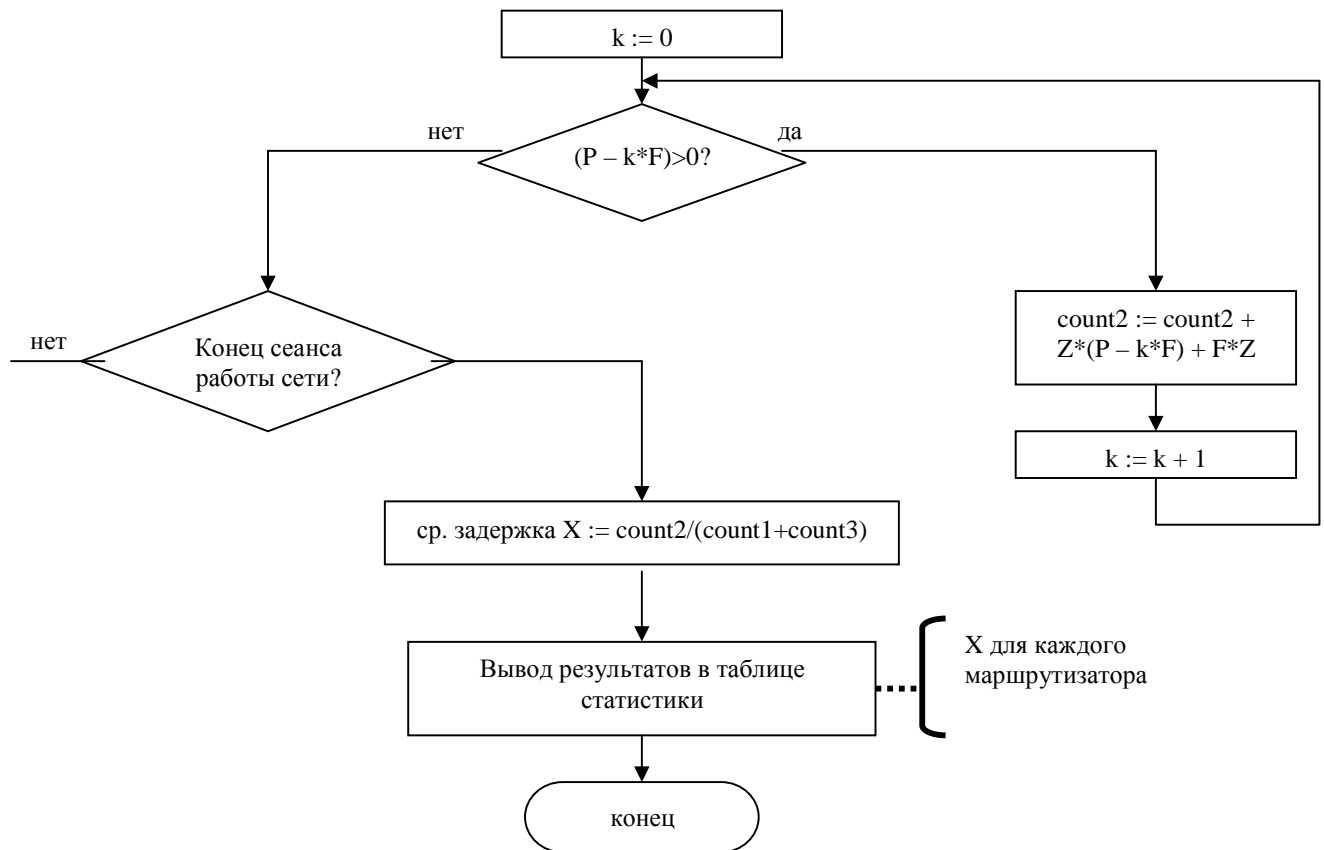
В алгоритме использованы следующие условные обозначения:

- count1 – счетчик количества неотброшенных пакетов, прошедших через маршрутизатор за сеанс и стоявших в очереди;
- count2 – сумма задержек всех пакетов, прошедших через очередь;

- count3 - счетчик количества неотброшенных пакетов, прошедших через секцию обработки за сеанс;
- T – общее число мест в очереди;
- Z – задержка пакета при одном такте работы сети. Такт работы сети – это время, за которое будет обработано количество пакетов равное мощности маршрутизатора;
- P – число свободных мест в очереди;
- F – число одновременно обрабатываемых пакетов;
- M – непоместившиеся в очередь пакеты.







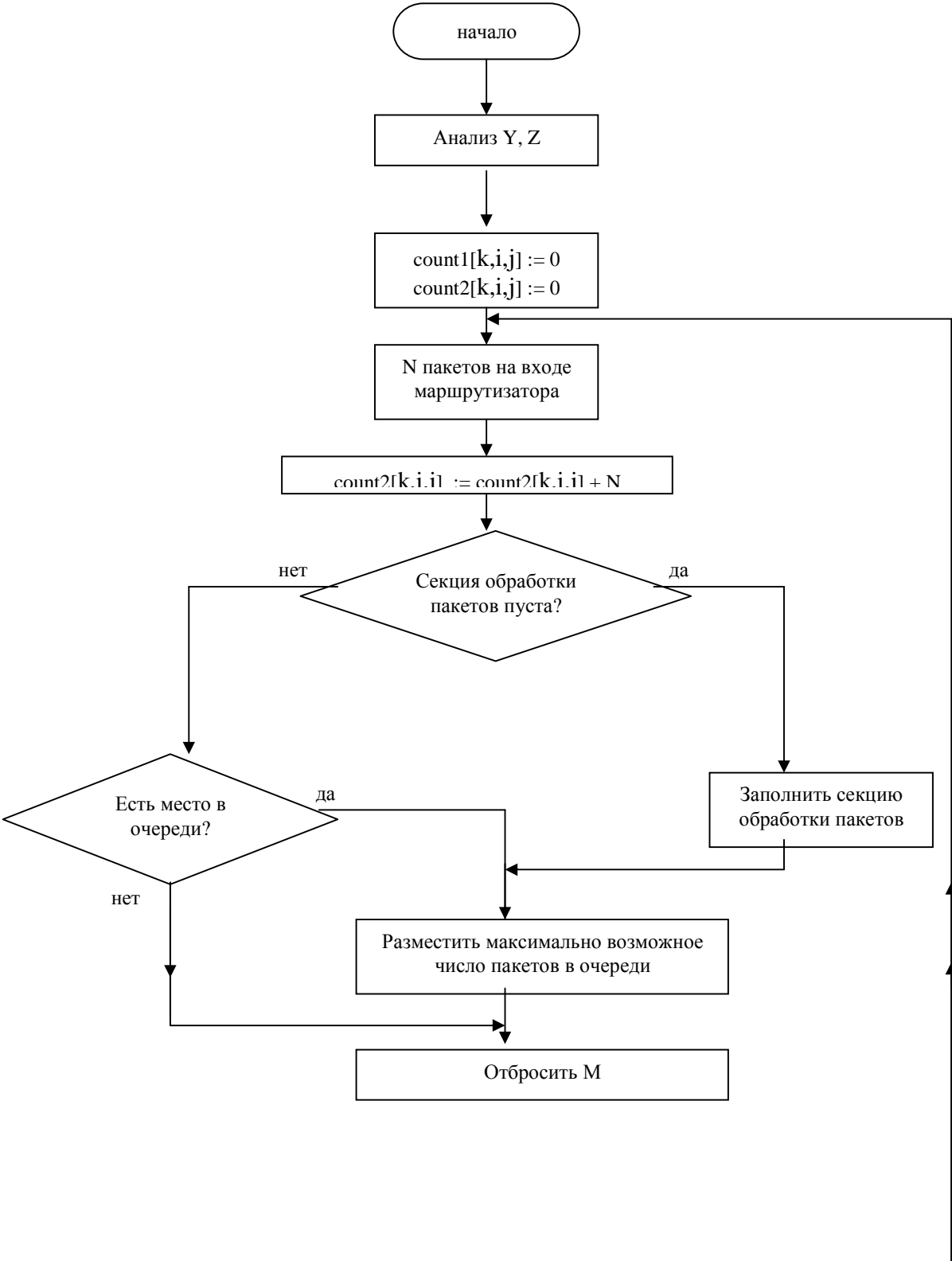
### 3.3.4 Алгоритм сбора статистических данных для подсчета процента потерь пакетов на каждом маршрутизаторе для потоков данных от каждого отправителя

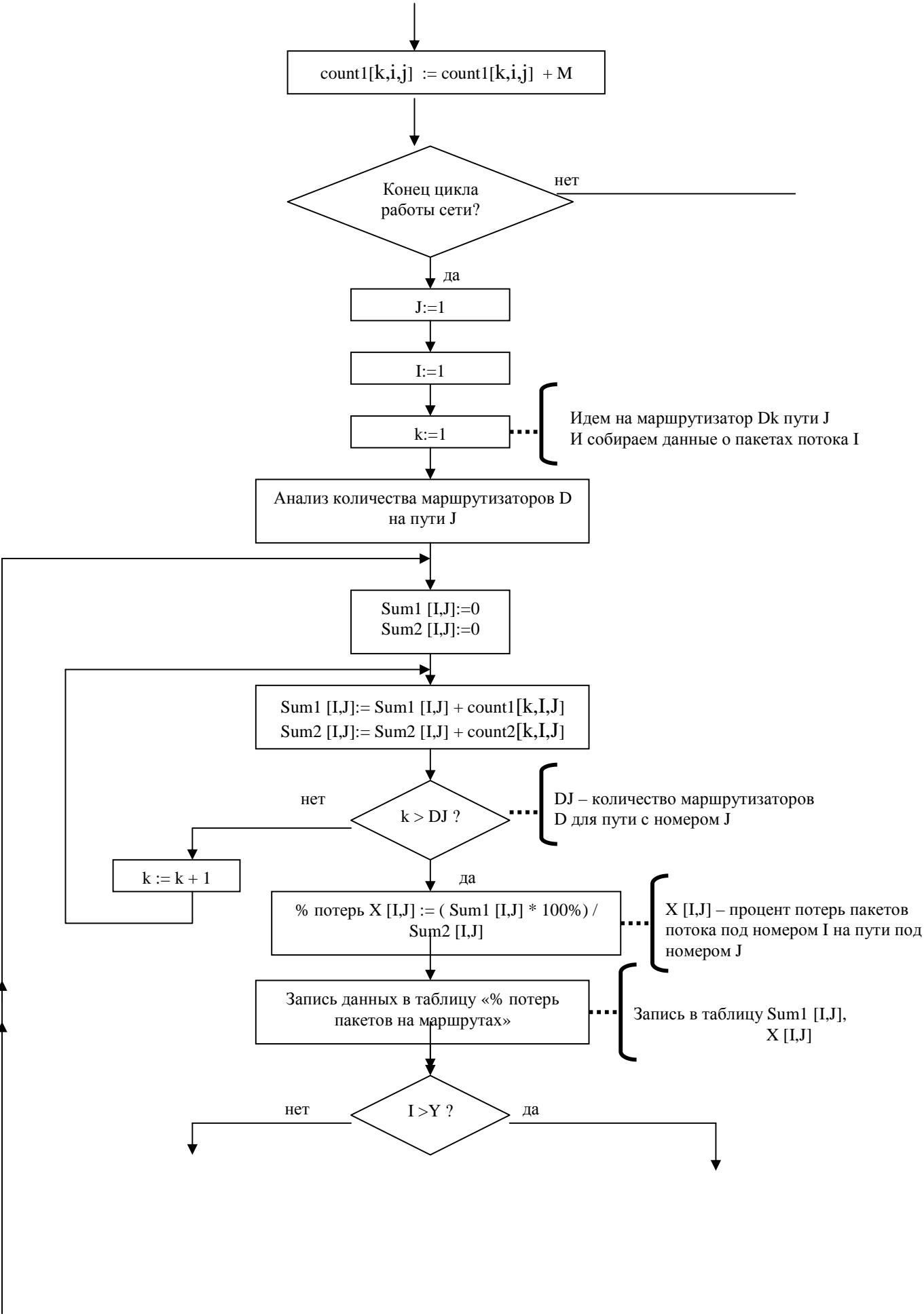
Для организации обслуживания потоков пакетов от определённых пользователей в сети MPLS могут быть выделены отдельные ресурсы. Оператору сети MPLS необходимо анализировать возможности своей сети для обслуживания вышеназванных потоков для предоставления гарантированных параметров обслуживания. В связи с этим оператор исследует параметры потоков от каждого пользователя на каждом возможном пути их передачи и делает выводы об узких участках работы сети и необходимости их коррекции.

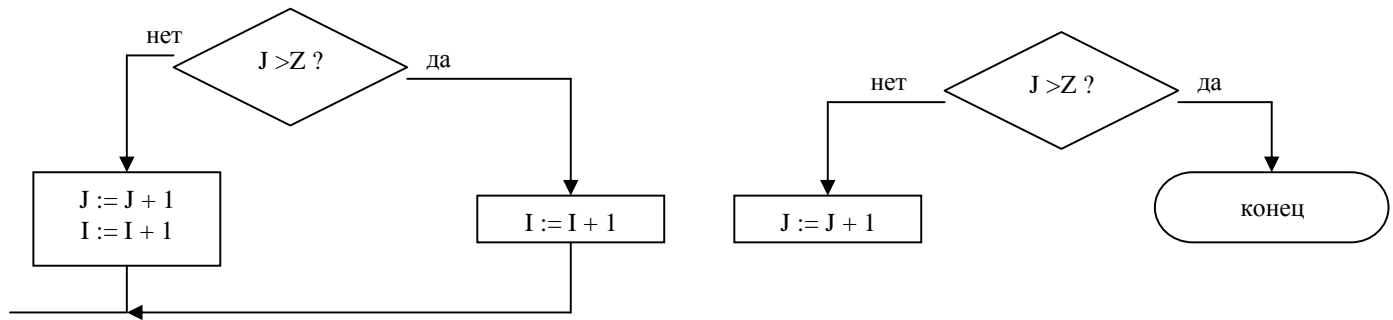
В алгоритме использованы следующие условные обозначения:

- $Y$  – число отправителей для сконфигурированной сети MPLS (минимально-1, максимальное – 3);
- $Z$  – число возможных путей для передачи трафика (минимально-1, максимальное – 2);

- $D$  – число маршрутизаторов на пути;
- $count1[k,i,j]$  – счетчик числа пакетов потока под номером  $i$  ( $i [1...Y]$ ), прошедших через маршрутизатор под номером  $k$  ( $k [1...D]$ ), принадлежащий пути  $j$  ( $j [1...Z]$ ), за сеанс работы сети;
- $count2[k,i,j]$  – счетчик числа отброшенных пакетов потока под номером  $i$ , прошедших через маршрутизатор под номером  $k$ , принадлежащий пути  $j$ , за сеанс работы сети;







### 3.4 Разработка пользовательского интерфейса

Для обеспечения работы пользователя с сетью MPLS и анализа исследования статистических данных о сети необходимо разработать графическую диалоговую оболочку пользователя, выполненную в виде стандартных элементов приложений Windows. Внешний вид диалоговой оболочки пользователя приведен на рисунке 4.4.

Пользовательский интерфейс следует разработать с использованием стандартных графических элементов Windows (меню, контекстные меню, кнопки, полосы прокрутки, поля редактирования и др.) и компонент из библиотеки визуальных компонент языка программирования Delphi.

Интерфейс программы-конструктора и анализатора сети MPLS должен быть удобным, понятным и предоставлять пользователю возможность выполнять все требуемые операции. Интерфейс должен включать в себя экранные формы для ввода, вывода и просмотра информации, информационные сообщения-предупреждения и сообщения об ошибках (например, ошибочный ввод), которые позволяют пользователю быстро сориентироваться в любой ситуации во время работы с сетью. Для обеспечения единообразия пользовательского интерфейса диагностические и предупреждающие сообщения следует кодировать с использованием API функции Message Box (диалоговые сообщения Windows).

В программе необходимо использовать контекстные меню, что упростит выполнение действий для пользователя и ускорит процесс его работы с программным приложением.

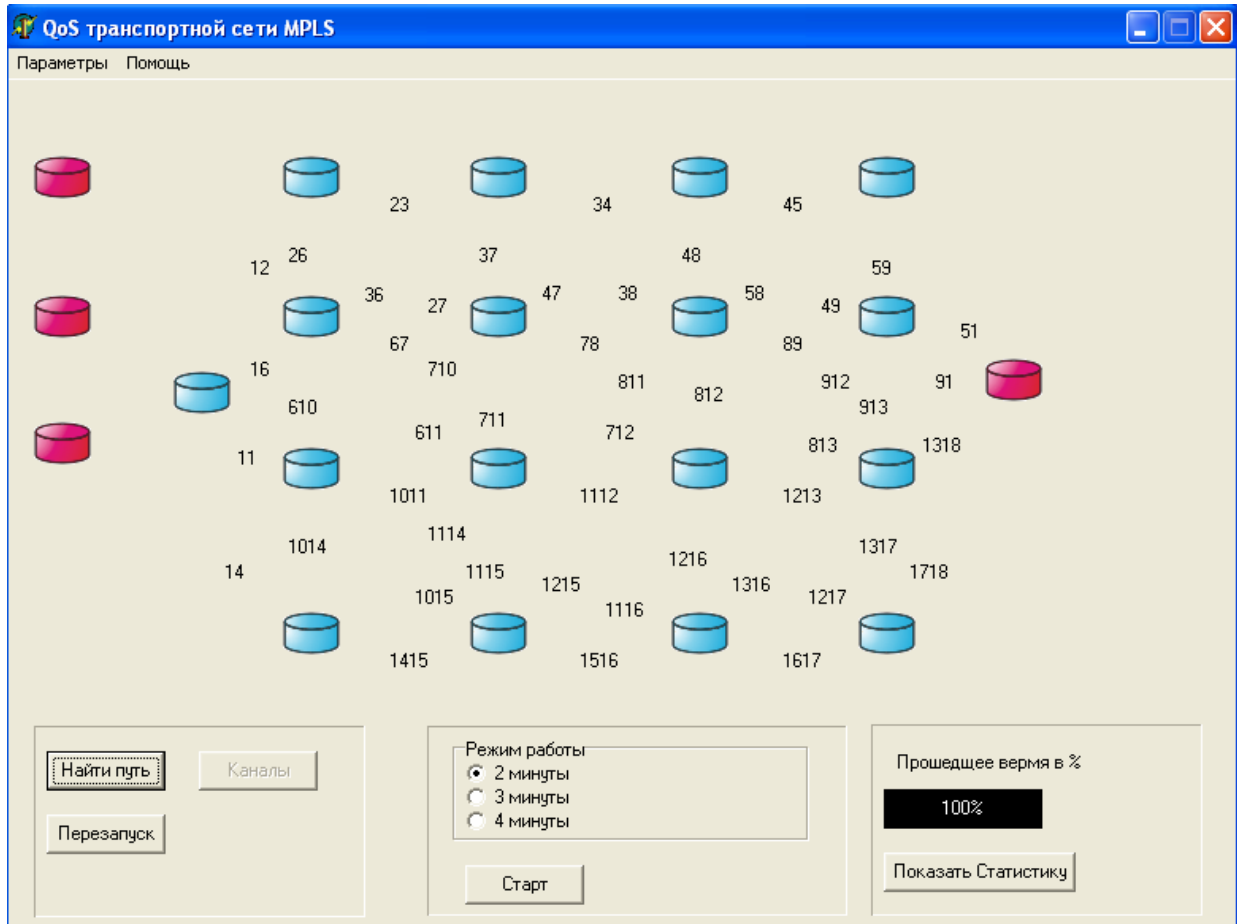


Рисунок . Внешний вид главного рабочего окна ПО.

Для работы пользователя с сетью MPLS были разработаны следующие кнопки нижнего меню, для создания которых решено было использовать компоненту Press Button палитры компонентов Standard из пакета среды разработки библиотеки VCL, так как они наиболее часто используются в среде Windows и имеют привычный для пользователю вид:

- «Перезапуск» - пользователь должен иметь возможность начать работы по конфигурации и параметризации сети заново в любой момент работы программного приложения. Для этого необходимо предусмотреть наличие соответствующей кнопки;
- «Найти путь» - после завершения пользователем выбора своей сетевой конфигурации следующим этапом работы программы должна быть работа алгоритмов поиска возможных маршрутов. Для обозначения начала работы этих маршрутов необходимо разработать кнопку, нажатием на которую пользователь

дает знать программному приложению о готовности к работе с сетью по сбору и анализу данных. Кроме того, при нажатии на кнопку «Найти путь» пользователь должен иметь возможность увидеть отображение выбора маршрутов для своей сети, чтобы проанализировать сделанный выбор и, возможно, внести корректировки в конфигурацию сети;

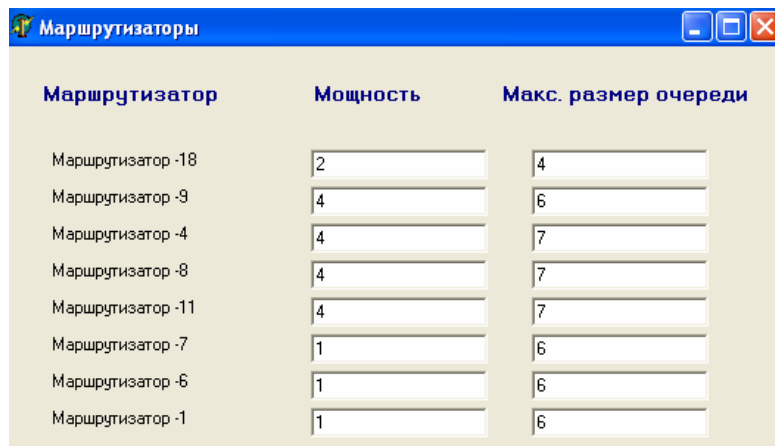
- «Каналы» - в связи с тем, что ПО предназначено для моделирования реальных процессов по передаче данных в сетях MPLS, необходимо внести в сеть дополнительные нагрузки извне и параметризовать ее (задать набор ограничений для пропускной способности и скорости обработки). Следовательно, необходимо заполнить таблицы для каждого маршрутизатора о его параметрах. Для этого решено было не загружать главное рабочее окно большими таблицами данных, а предусмотреть их ввод в отдельных тематических окнах. В результате были разработаны формы, представленные на **рисунках и**

Канал	Загрузка
Канал -18-9	2
Канал -9-4	4
Канал -4-8	2
Канал -8-11	2
Канал -11-7	9
Канал -7-6	1
Канал -6-1	2
Канал -18-13	9
Канал -13-16	8
Канал -16-11	9
Канал -11-10	3
Канал -10-1	1

Рисунок . Окно «Список каналов и их загрузка»

В столбце «канал» перечислены все каналы между включенными в сконфигурированную сеть маршрутизаторами. Поля для ввода загрузки каждого маршрутизатора, его мощности и максимального размера очереди выполнены в

виде компонент Edit панели Standard, поскольку они предоставляют хорошие возможности для вывода и редактирования текста.



Маршрутизатор	Мощность	Макс. размер очереди
Маршрутизатор -18	2	4
Маршрутизатор -9	4	6
Маршрутизатор -4	4	7
Маршрутизатор -8	4	7
Маршрутизатор -11	4	7
Маршрутизатор -7	1	6
Маршрутизатор -6	1	6
Маршрутизатор -1	1	6

Рисунок . Окно «Маршрутизаторы».

- «Старт» - для запуска рабочего режима сети было решено предусмотреть данную кнопку, при нажатии на которую выявляются ошибки, сделанные пользователем во время конфигурирования сети, а в случае их отсутствия – блокируются все дальнейшие операции с программным обеспечением до истечения времени работы сети.

## **4. МЕРОПРИЯТИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ЖИЗНЕДЕЯТЕЛЬНОСТИ**

### **4.1 Анализ характеристик разрабатываемого пакета, трудовой деятельности и производственной среды**

Разрабатываемое программное приложение представляет собой учебный материал для практических лабораторных занятий студентов и специалистов в области современных сетевых технологий.

Трудовая деятельность, связанная с данной работой – непосредственно использование самого программного обеспечения. Данный вид работ производится в офисных помещениях или учебных компьютерных лабораториях, все работы производятся в виде операций по работе с вычислительной техникой.

В нижеследующих разделах будут рассмотрены меры по эргономическому обеспечению рабочего места пользователя ПК, мероприятия по технике безопасности и мероприятия по пожарной безопасности.

### **4.2 Мероприятия по эргономическому обеспечению**

#### **4.2.1 Нормативные документы для расчета эргономических параметров рабочего места с компьютером.**

В настоящем стандарте использованы ссылки на следующие стандарты:

ГОСТ 12.1.005–88 ССБТ. Общие санитарно-гигиенические требования к воздуху рабочей зоны.

ГОСТ 12.1.050–86 ССБТ. Метод измерения шума на рабочих местах.

ГОСТ 427–75. Линейки измерительные металлические. Технические условия.

ГОСТ 7721–89. Источники света для измерений цвета. Типы. Технические требования. Маркировка.



ГОСТ 21889–76 СЧМ. Кресло человека-оператора. Общие эргономические требования.

ГОСТ 24940–96. Здания и сооружения. Метод измерения освещенности.

ГОСТ 50948–96. Средства отображения информации индивидуального пользования. Общие эргономические требования и требования безопасности.

ГОСТ 50949–96. Средства отображения информации индивидуального пользования. Методы измерения и оценки эргономических параметров их приборов безопасности.

#### **4.2.2 Общие требования**

Рабочее место с дисплеем должно обеспечивать пользователю возможность удобного выполнения работ в положении сидя и не создавать перегрузки костно-мышечной системы.

Основными элементами рабочего места пользователя являются: рабочий стол, рабочий стул (кресло), дисплей, клавиатура; вспомогательными – держатель бумаг, подставка для ног.

#### **4.2.3 Требования к рабочему столу**

Конструкция рабочего стола должна обеспечивать возможность размещения на рабочей поверхности необходимого комплекта оборудования и документов с учетом характера выполняемой работы.

Рабочие столы по конструктивному исполнению подразделяют на регулируемые и нерегулируемые по изменению высоты рабочей поверхности.

Регулируемая высота рабочей поверхности стола должна изменяться в пределах от 680 до 800 мм. Механизмы для регулирования высоты рабочей поверхности стола должны быть легко достигаемыми в положении сидя, иметь легкость управления и надежную фиксацию.

Высота рабочей поверхности стола при нерегулируемой высоте должна составлять 725 мм. Размеры рабочей поверхности стола должна быть:

- глубина – не менее 600 (800) мм;
- ширина – не менее 1200(1600) мм.

**Примечание:** в скобках указаны дополнительные значения.

Рабочий стол должен иметь пространство для ног высотой не менее 600 мм, шириной – не менее 500 мм, глубиной на уровне колен – не менее 450 мм и на уровне вытянутых ног – не менее 650 мм.

Рабочая поверхность стола не должна иметь острых углов и краев. Покрытие рабочей поверхности стола должна быть из диффузно отражающего материала с коэффициентом отражения 0,45 – 0,50.

#### **4.2.4 Требования к рабочему столу (креслу)**

Рабочий стул (кресло) должен обеспечивать поддержание физиологически рациональной рабочей позы пользователя в процессе трудовой деятельности, создавать условия для изменения позы с целью снижения статического напряжения мышц, шейно-плечевой области и спины, а также для исключения нарушения циркуляции крови в нижних конечностях.

Рабочий стул должен быть подъемно-поворотным и регулируемым по высоте и углам наклона сиденья и спинки, а также расстоянию спинки от определенного края сиденья.

В целях снижения статического напряжения мышц рук следует использовать стационарные или съемные подлокотники, регулирующиеся по высоте над сиденьем и внутреннему расстоянию между подлокотниками.

Регулирование каждого положения должно быть независимым, легко осуществимым и иметь надежную фиксацию.

Поверхность сиденья должна иметь ширину и глубину не менее 400 мм. Должна быть предусмотрена возможность изменения угла наклона поверхности сиденья от 15° вперед до 5° назад. Высота поверхности сиденья должна регулироваться в пределах от 400 до 550 мм.

Опорная поверхность спинки стула (кресла) должна иметь высоту (300±20) мм, ширину не менее 380 мм и радиус кривизны в горизонтальной плоскости 400 мм.

Угол наклона спинки в вертикальной плоскости должен регулироваться в пределах 0°±30° от вертикального положения.

Расстояние спинки от предельного края сиденья должно регулироваться в пределах от 260 до 400 мм.

Подлокотники должны быть длиной не менее 250 мм, шириной – 50–70 мм, иметь возможность регулирования по высоте над сиденьем в пределах  $(230\pm 30)$  мм и регулирования внутреннего расстояния между подлокотниками в пределах от 350 до 500 мм.

#### **4.2.5 Требования к подставке для ног**

Подставка для ног должна регулироваться по высоте в пределах от 150 мм и углу наклона опорной поверхности – до  $20^\circ$ .

Ширина опорной поверхности подставки для ног должна быть не менее 300 мм, глубина – не менее 400 мм.

Поверхность подставки должна быть рифленой. По переднему краю должен быть предусмотрен бортик высотой 10 мм.

#### **4.2.6 Требования к дисплею**

Дисплей на рабочем месте пользователя должен располагаться так, чтобы изображение в любой его части было различимо без необходимости поднять или опустить голову.

Дисплей на рабочем месте должен быть установлен ниже уровня глаз пользователя. Угол наблюдения экрана пользователем относительно горизонтальной линии взгляда не должен превышать  $60^\circ$ .

Требования к конструкции дисплея, визуальным параметрам экрана параметрам излучений – по ГОСТ Р 50948.

#### **4.2.7 Требования к клавиатуре**

Клавиатура на рабочем месте пользователя должна располагаться так, чтобы обеспечивалась оптимальная видимость экрана.

Клавиатура должна иметь возможность свободного перемещения. Клавиатуру следует располагать по поверхности стола на расстоянии от 100 мм до 300 мм от переднего края, обращенного к оператору, или на специальной регулируемой по высоте рабочей поверхности, отделенной от основной столешницы.

#### **4.2.8 Требование к пюпитру**

Пюпитр должен иметь по длине и ширине размеры, соответствующие размерам устанавливаемых на нем документов.

Угол наклона пюпитра должен регулироваться в пределах  $30^{\circ}$  -  $70^{\circ}$  от вертикального положения.

Пюпитр должен быть установлен на одном уровне с экраном дисплея, и отстоять от глаз оператора на том же расстоянии, что и экран, либо отличаться от него, но не более на 100 мм.

Поверхность пюпитра должна иметь покрытие из диффузно отражающего материала с коэффициентом отражения 0,45 – 0,50.

Иллюстрация правильной организации рабочего места представлена на рисунке (см. рис.20)

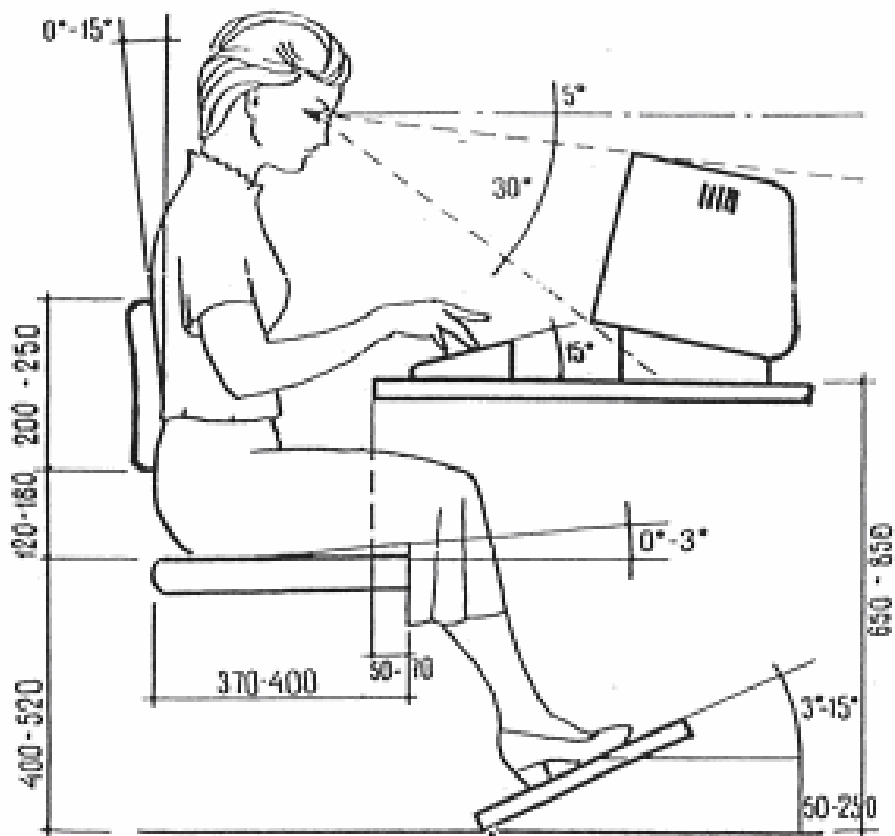


Рисунок 20. Правильная организация рабочего места

#### 4.2.9 Требования к освещению

Освещенность рабочего места оператора на рабочем столе в горизонтальной плоскости от общего искусственного освещения должна быть от 300 до 500 лк.

Освещенность на пюпитре в вертикальной плоскости должна быть не менее 300лк.

Для освещения зоны расположения документов допускается установка светильников местного освещения.

отношение яркостей в зоне наблюдения (экран, документ, поверхность стола) должно быть не менее 10:1

В поле зрения оператора должны отсутствовать прямая и отраженная блескость.

Для снижения блескости необходимо:

- оборудовать светопроемы солнцезащитными устройствами (шторами, регулируемые жалюзи, внешними козырьками и т. д.);
- использовать для общего освещения светильники с рассеивателями и экранирующими решетками, яркость которых в зоне углов излучения более 50° от вертикали не должна превышать 200 кд/м<sup>2</sup>;
- использовать для местного освещения светильники с непросвечивающим отражателем и защитным углом не менее 40°;
- размещать рабочий стол так, чтобы оконный проем находился сбоку (справа или слева), при этом дисплей должен располагаться на поверхности стола справа или слева от оператора;
- размещать рабочий стол между рядами светильников общего освещения;
- использовать дисплей, имеющий антибликовое покрытие экрана или антибликовый фильтр.

На рабочем месте оператора должна быть ограничена пульсация освещенности от газоразрядных источников света.

Для ограничения пульсации освещенности следует использовать в светильниках с газоразрядными лампами высокочастотные пускорегулирующие аппараты или включать лампы в многоламповых светильниках (или рядом расположенные светильники общего освещения) на разные фазы трехфазной сети и использовать преимущественно люминесцентные лампы белого света.

#### 4.2.10 Требования к шуму

Уровень шума на рабочем месте оператора не должен превышать значений, указанных в таблице (см. таб.2).

Таблица 2. Требования к шуму

Уровень звукового давления, дБ, в октавных полосах со среднегеометрическими частотами, Гц									Уровень звука и эквивалентный уровень звука, дБ.
31,5	63	125	250	500	1000	2000	4000	8000	
86	71	61	54	49	45	42	40	38	50

#### **4.2.11 Требования к микроклимату**

На рабочем месте оператора должны обеспечиваться оптимальные микроклиматические условия в холодный и теплый периоды года.

Температура воздуха на рабочем месте холодный период года должна быть от 22° до 24°С, в теплый период года - от 23° до 25°С.

Разница температур на уровне пола и уровне головы оператора в положении сидя не должна превышать 3°С.

Относительная влажность воздуха на рабочем месте оператора должна составлять 40-60%. Скорость движения воздуха на рабочем месте оператора должна быть 0,1 м/с.

#### **4.3 Мероприятия по технике безопасности**

Для обеспечения электробезопасности должны применяться отдельно или в сочетании друг с другом следующие технические способы и средства:

- защитное заземление;
- зануление;
- выравнивание потенциалов;
- малое напряжение;
- электрическое разделение сетей;
- защитное отключение;
- изоляция токоведущих частей (рабочая, дополнительная, усиленная, двойная);
- компенсация токов замыкания на землю;
- оградительные устройства;
- предупредительная сигнализация, блокировка, знаки безопасности;
- средства защиты и предохранительные приспособления.

В случае питания аппаратуры от промышленной 3-х фазной 4-х проводной сети с заземленной нейтралью и напряжением 380/220 В с частотой 50 Гц, эффективным способом защиты от поражения электрическим током при пробое изоляции, или замыканий токоведущих частей на корпус является устройство защитного зануления.

В таблице приведены предельно допустимые уровни неионизирующих электромагнитных излучений (см. таб.3).

Таблица 3. Предельно допустимые уровни неионизирующих электромагнитных излучений

Наименование параметров С 01.01.1997	Допустимое значение.
1.Напряженность электромагнитного поля на расстоянии 50 см. ВДТ по электрической составляющей должна быть не более: - в диапазоне частот 5 Гц – 2 кГц - в диапазоне частот 2 – 400 кГц	25 В/м 2,5 В/м
2. Плотность магнитного потока должна быть не более: - в диапазоне частот 5 Гц – 2 кГц - в диапазоне частот 2 – 400 кГц	250 нТл 25 нТл
3.Поверхностный электростатический потенциал не должен превышать	500 В

Уровни удовлетворяют нормам при качественном устройстве заземления.

#### **544 Мероприятия по пожарной безопасности**

Пожарная безопасность обеспечивается системой предотвращения пожара и системой пожарной защиты. Во всех служебных помещениях обязательно должен быть «План эвакуации людей при пожаре», регламентирующий действия персонала в случае возникновения очага возгорания и указывающий места расположения пожарной техники. Отделка помещения ОПС должна соответствовать нормам пожарной безопасности: ГОСТ 12.1.004-91 ССБТ «Пожарная безопасность. Общие требования».



Пожар, возникший на предприятии, может привести к выходу из строя различной аппаратуры, и уничтожению материальных ценностей. Пожар часто угрожает жизни и здоровью людей.

Основными причинами возникновения пожаров являются:

- небрежное, неосторожное или неумелое обращение с открытым огнем;
- неисправности в устройствах систем отопления и нарушение правил их эксплуатации;
- неисправности электрооборудования, электропроводки, производственного оборудования и нарушение правил их эксплуатации;
- самовозгорание и самовоспламенение горючих веществ;
  - разряды статического и атмосферного электричества;
  - неправильное хранение материалов, опасных в пожарном отношении;
  - нарушение установленного технологического процесса производства без учета пожарной опасности;
  - курение в местах, не разрешенных пожарной охраной.

Мероприятия, предупреждающие возникновение пожаров или ограничивающие их дальнейшее распространение, называются профилактическими. Задачи организационно-технических мероприятий по пожарной профилактике сводятся к следующим:

- не допустить возникновения пожара от любой причины;
- не допустить распространение пожара в случае его возникновения;
- обеспечить эвакуацию людей и материальных ценностей из загоревшихся помещений;
- как можно быстрее ликвидировать пожар.

При проектировании, строительстве и эксплуатации предприятий необходимо предусматривать следующие инженерно-технические мероприятия по пожарной профилактике. К ним относятся:

- применение в проектируемых объектах негорюемых и огнестойких материалов;
- правильная планировка и расположение зданий предприятия, устройство необходимого количества входов и выходов, рациональное размещение лестниц и выходов;

- организация технологического процесса производства, расположение установок и оборудования с учетом пожарной безопасности и эвакуации людей;
- соблюдение необходимой ширины проходов и проездов;
- правильный выбор системы отопления и вентиляции, правильное их устройство и соблюдение правил пожарной профилактики при их эксплуатации;
- устройство, монтаж и своевременный контроль изоляции установленного оборудования и аппаратуры. Расчет электроизоляции и выбор изоляционных материалов аппаратуры в соответствии с требованиями пожарной безопасности;
- установление на предприятии необходимого режима работы и соблюдение правил внутреннего распорядка.

Для тушения пожаров на начальных стадиях широко применяются огнетушители. В соответствии с ГОСТ Р 51057-97 «Техника пожарная. Огнетушители переносные. Общие технические требования. Методы испытаний» в ОПС целесообразно использовать углекислотный огнетушитель, который применяется для тушения пожаров в электротехнических установках и приборах, находящихся под напряжением и для тушения особо ценных материалов (почты, ценных бумаг, книг), когда нельзя использовать воду или пену.

**Выводы:** Выполнение требований по эргономическому обеспечению трудовой деятельности, соблюдение правил техники безопасности и выполнение норм пожарной безопасности обеспечивает комфортные и благоприятные трудовые условия.

## **ПРИЛОЖЕНИЕ 1**

Санкт-Петербургский Государственный Университет телекоммуникаций  
им.проф. М.А.Бонч-Бруевича

Ловель О., Бочков Р.

# **Методические указания к выполнению цикла лабораторных работ**

По теме: «Принципы работы транспортных сетей MPLS»

2004 г.

## **ВВЕДЕНИЕ**

Данные методические указания предназначены для организации занятий студентов в лабораториях по курсам сетевых дисциплин с использованием прилагающегося программного обеспечения. В результате выполнения лабораторных работ студенты должны изучить следующие вопросы:

1. Устройства, используемые в сетях MPLS и их основные функции.
2. Принципы коммутации пакетов в сетях MPLS. Процедуру замены меток.
3. Использование протокола резервирования ресурсов RSVP в сетях MPLS.

4. Использование протокола LDP для определения маршрутов LSP в сетях MPLS.
5. Реализацию схемы тунелирования в сетях MPLS, коммутацию по меткам с использованием стека меток.
6. Параметры обмена трафиком в сетях MPLS, такие как: задержки, загрузку каналов, скорость передачи пакетов, потери пакетов в канале и на маршрутизаторах, организацию очередей с потерями.

## **1. ТЕОРЕТИЧЕСКАЯ СПРАВКА**

### **1.1 Основные характеристики технологии MPLS**

MPLS (MultiProtocol Label Switching) — это технология быстрой коммутации пакетов в многопротокольных сетях, основанная на использовании меток. Технология MPLS сочетает в себе возможности управления трафиком, присущие технологиям канального (второго) уровня (Data Link Layer 2), масштабируемость и гибкость протоколов, характерные для сетевого (третьего) уровня (Network Link Layer 3). Термин "многопротокольность" в названии технологии означает, что MPLS – инкапсулирующая технология и может транспортировать множество других протоколов

Благодаря отображению трафика двух различных сетевых архитектур друг на друга в сетях MPLS достигаются характеристики сетей третьего уровня:

- Качество обслуживания QoS (Quality of Service);
- Регулирование трафика (traffic engineering, TE);
- Управление полосой пропускания.

### **1.2 Состав и структура сетей MPLS**

Основными составляющими сетей MPLS являются:

- граничные маршрутизаторы LER (Label Edge Router) – расположены на стыке сети доступа (например, сети ATM) и транспортной сети MPLS. Основная функция пограничных маршрутизаторов – удаление меток из пакетов, когда пакет покидает границы сети MPLS, и ввод их в поступающие из других сетей пакеты;

- внутренние маршрутизаторы LER (Label Switching Router) – расположены на всем протяжении сети MPLS. Основная функция – замена меток.

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 MPLS сети. Маршрутизаторы ядра занимаются только коммутацией. Все функции классификации пакетов по различным классам FEC, а также реализацию таких дополнительных сервисов, таких как фильтрация, явная маршрутизация, выравнивание нагрузки и управление трафиком, берут на себя граничные маршрутизаторы LER. В результате интенсивные вычисления приходится на граничную область, а высокопроизводительная коммутация выполняется в ядре, что позволяет оптимизировать конфигурацию устройств сети MPLS в зависимости от их местоположения в сети.

### **1.3 Принципы коммутации пакетов по меткам**

В основе технологии MPLS лежит принцип обмена меток. Метка (Label) - это короткий идентификатор фиксированной длины. Любой передаваемый пакет ассоциируется с тем или иным классом сетевого уровня (Forwarding Equivalence Class, FEC), каждый из которых идентифицируется определенной меткой.

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.).

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.

Таблица1. Таблица коммутации для каждого маршрутизатора сети MPLS.

Входная метка подсети LSR	Входная метка подсети LER (если есть)	№ вх. порта	Префикс (IP-адрес адресата)	№ исх. порта	Выходная метка подсети LER (если есть)	Выходная метка подсети LSR

## 1.4 Алгоритмы маршрутизации в сетях MPLS

### 1.OSPF.

Протокол состояния каналов OSPF (Open Shortest Path First, «кратчайший путь - первым») осуществляет алгоритм выбора маршрута на базе информации о состоянии канала, используя при этом любую из следующих метрик: ширину полосы пропускания, задержку, надежность, нагрузку и т. д.

Вначале распространяется информация о топологии сети. На базе обмена этими сообщениями каждый маршрутизатор строит граф связей сети, в котором вершинами графа являются маршрутизаторы, а ребрами - интерфейсы маршрутизаторов.

В результате распространения топологической информации все маршрутизаторы сети располагают идентичными сведениями о графе сети, которые хранятся в топологической базе данных каждого маршрутизатора. Задача нахождения решается с помощью алгоритма Дейкстры (см. рис.1).

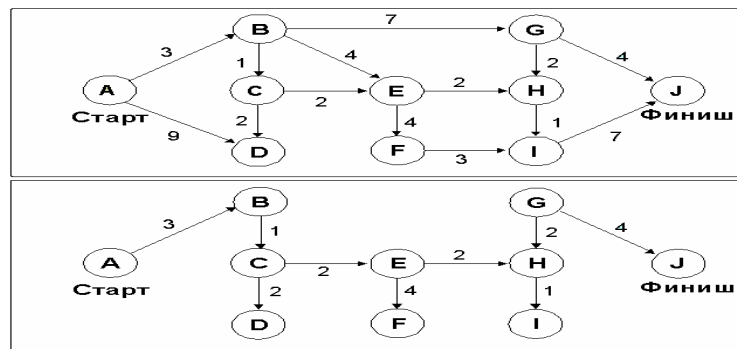


Рис.1 Пример работы алгоритма Дейкстры.

## 2. ТУННЕЛИРОВАНИЕ.

Туннелирование трафика осуществляется при прохождении пакетом на всем пути магистральной сети MPLS через более чем два пограничных маршрутизатора. Для осуществления операции туннелирования организована передача с пакетом не одной метки, а целого стека меток, организованного по принципу «last-in first-out» или LIFO («последним вошел - первым вышел»). Глубина стека меток определяется как: кол-во маршрутизаторов LER на пути следования пакетов / 2. Маршрутизаторы LER, расположенные ближе к отправителю (первая половина пути LSP) «кладут» новую метку в стек, расположенные ближе к получателю LER – убирают верхнюю метку и меняют следующую за ней по таблице коммутации, промежуточные между ними маршрутизаторы LSR (называются подсетью из LSR) всегда меняют только верхнюю в стеке метку.

### **1.5 Использование сопутствующих протоколов в сетях MPLS**

#### 1. LDP.

Протокол распределения меток LDP (Label Distribution Protocol) представляет собой набор процедур и сообщений, при помощи которого маршрутизатор LSR устанавливает в сети путь коммутации по меткам, обмениваясь информацией о привязке меток к классу FEC между двумя маршрутизаторами LSR. С помощью протокола LDP создается путь коммутации LSP. LDP начинает работать сразу после определения топологии сети (например, по протоколу OSPF).

Сначала посредством многоадресной рассылки сообщений UDP (User Datagram Protocol) коммутирующие маршрутизаторы определяют свое «соседство» в рамках протокола LDP. После того как соседство установлено, протокол LDP открывает транспортное соединение между участниками сеанса поверх протокола TCP (Transmission

Control Protocol). 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).

## 2. RSVP.

Для того чтобы удовлетворить требованиям приложений к пропускной способности и качеству обслуживания трафика (задержка, величина джиттера), необходим механизм, позволяющий приложениям информировать сеть о своих требованиях. На основе данной информации сеть может резервировать внутри себя ресурсы для того, чтобы гарантировать выполнение требований, или отказать приложению, заставляя его пересмотреть первоначальные требования к качеству услуг или прекратить установление соединения, отложив сеанс связи. В роли такого механизма и выступает протокол резервирования ресурсов RSVP (Resource Reservation Protocol). Применение протокола RSVP в сетях MPLS – это, в основном, использование явного указания маршрутов следования пакетов, снабженных MPLS-метками, т.е. фиксирование (резервирование) путей для передачи приоритетного трафика. По резервированным с помощью протокола RSVP путям LSP передается обычный трафик до тех пор, пока не поступает на обслуживание приоритетный. В этом случае передача непериприоритетного трафика по данному пути LSP прекращается и он используется только для приоритетного.

### **1.6 Обеспечение механизмов качества обслуживания QoS в сетях MPLS**

Технология MPLS поддерживает следующие услуги в сфере предоставления качества обслуживания QoS:

- Классификация пакетов и их пометка. Классификация пакетов позволяет разделить трафик на несколько потоков с разными приоритетами или классами обслуживания;
- Исключение перегрузки. Эта услуга реализуется за счет алгоритма WRED (Weighted Random Early Detection, взвешенные очереди), работающего на уровне интерфейса и осуществляющего управление буфером;
- Управление перегрузкой. Когда сетевой интерфейс оказывается перегруженным, необходимы средства обслуживания очередей, чтобы гарантировать определенные условия для приоритетных приложений по отношению к непериприоритетным;



- Кондиционирование трафика. Использование управления трафиком или политики может определить свойства входящего сетевого трафика. Такое кондиционирование может при заданной скорости сгладить поток;
- Управление. Протокол резервирования ресурсов RSVP является основным механизмом реализации управления доступом для сетевых потоков. Протокол RSVP может запросить ресурсы, необходимые для осуществления обмена некоторым конкретным приложением в заданной сети.

### **3. СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ**

1. Камер Д. Компьютерные сети и Internet, 2002
2. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы Второе издание. СПб, 2003
3. Семенов Ю.А. Протоколы и ресурсы Интернет, М. 1996
4. Шринивас Вегешна. Качество обслуживания в сетях IP. 2003

### **4. ЛАБОРАТОРНАЯ РАБОТА №2.**

#### **«Сбор и анализ статистических данных в сетях MPLS»**

##### **4.1 Описание лабораторной работы**

Для подготовки работы с конструктором сети MPLS, необходимо открыть программный файл MPLS\_Stats.exe, хранящийся в папке «NetLabs» на жестком диске D. . В ходе выполнения лабораторной работы должны быть выполнены следующие действия:

- 1). Рассмотреть топологию сети MPLS, представленную в главном рабочем окне приложения. Она состоит из 17 внутренних маршрутизаторов LSR, 3 граничных маршрутизаторов LER и возможных связей между всеми маршрутизаторами, которые представляют собой каналы передачи данных с наложенными на них весами (расстояниями).
- 2). Курсором мыши обозначить связи между маршрутизаторами, выбирая самостоятельно конфигурацию сети MPLS. Необходимо учесть, что между отправителем и получателями должен существовать как минимум один путь LSP, проверить реакцию сети на отсутствие путей коммутации между адресатом и адресантами.

- 3). Найти 2 маршрута (или один если больше нет вариантов) между адресатом и адресантами при помощи клавиши «найти пути» на панели инструментов. Подсчитать расстояние между пунктами назначения для обоих маршрутов, выявить наикратчайший. Сверить результаты своих вычислений с результатами работы ПО.
- 4). Ввести исходные параметры работы сети при нажатии на клавишу «Каналы». В появившемся окне «Список каналов и их загрузка» ввести процентное значение загрузки для каждого канала для моделирования рабочего режима сети. В связи с тем, что данная сеть MPLS используется для передачи трафика как от представленных в рабочем окне отправителей, так и от посторонних отправителей, статистику работы сети для которых мы не исследуем, то предполагается резервация в % некоторой пропускной способности канала. Это приближает работу представленной в программном приложении сети к реальным условиям функционирования больших сетей MPLS.
- 5). Ввести исходные параметры работы сети при нажатии на клавишу «Параметры маршрутизаторов» после ввода загрузки каналов. В появившемся окне «Маршрутизаторы», в столбце «Мощность» ввести данные о максимально возможном количестве пакетов, подлежащих одновременной обработке (имеется в виду замена меток). Значения должны принадлежать диапазону 1-5.
- 5). В столбце «Максимальный размер очереди» ввести значения в диапазоне от 3 до 9 для каждого маршрутизатора.
- 4). Выбрать один из предложенных режимов работы сети по времени. По статистике, один сеанс связи между отправителем и получателем длится в среднем от 2 до 4 минут, если этот сеанс представляет собой телефонный разговор. Моделируемая сеть MPLS предназначена преимущественно для переноса голосового трафика, в связи с этим и были выбраны вышеназванные временные режимы.
- 5). Начать работу сети с помощью клавиши «Старт».
- 6). По окончании работы сети (процесс выполнения в % отображается на статус баре), начать работу со статистикой:
  - Вывести на экран Таблицу 1: «Процент потерь на маршрутизаторах». Проанализировать узкие места для сконфигурированной сети, изменить первоначальные параметры работы, повлиявшие на появление больших потерь для некоторых маршрутизаторов. Запустить рабочий режим сети с новыми

параметрами. Проверить значения потерь для каждого маршрутизатора в таблице опять. Сделать вывод о произошедших изменениях.

- Вывести на экран Таблицу 2: «Средняя задержка пакета на маршрутизаторе». Найти в таблице маршрутизаторы, на которых была максимальная задержка пакетов. Повторить действия предыдущего пункта, Проверить значения средней задержки для маршрутизаторов с измененными параметрами, сделать выводы о произошедших изменениях.
- Вывести на экран Таблицу 1: «Процент потерь для потоков данных от каждого отправителя для каждого из путей коммутации». Сделать вывод о том, состоялся ли сеанс связи для каждого отправителя. Исследовать причины большего процента потерь пакетов на одном пути коммутации, чем на другом. Попытаться изменить первоначальные параметры таким образом, чтобы разница в потерях для каждого пути была несущественной.

## 4.2 Руководство пользователя

1). Представленная в главном рабочем окне приложения топология MPLS сети состоит из 17 внутренних маршрутизаторов LSR и 4 граничных маршрутизаторов LER, один из которых расположен на стороне получателя, остальные – на стороне отправителя. Таким образом, наблюдается наличие 2-х подсетей: одна из LER, вторая из LSR.

2). Цифрами между маршрутизаторами на сетевом поле обозначены веса (расстояния между маршрутизаторами) для каждого канала передачи данных. Для того, чтобы убрать веса с экрана, необходимо убрать галочку перед надписью «Показать веса» в главном пользовательском меню (верхнее меню) в разделе «Параметры».

3). Первый этап работы с сетью заключается в ее конфигурировании. Пользователь выбирает ту конфигурацию, которая наиболее соответствует решению поставленных перед ним задач. Для этого необходимо предпринять следующие шаги:

- обозначить галочкой (одно нажатие левой клавишей мыши по маршрутизатору) каждый нужный вам маршрутизатор;
- второй галочкой (одно нажатие левой клавишей мыши по маршрутизатору) обозначить следующий за ним маршрутизатор.;
- В результате этих действий отобразится канал, соединяющий 2 маршрутизатора.

- Действия повторять, пока между отправителями, потоки данных от которых объединяются на входном в сеть маршрутизаторе, и получателем не будет прорисован хотя бы 1 путь. В случае отсутствия путей между отправителями и получателями при попытке заполнения таблиц исходных параметров работы сети MPLS (нажатие на клавишу каналы), на экран выводится предупреждающее сообщение о невозможности работы сети в связи с этой ошибкой.

4). После выбора конфигурации сети, необходимо нажать клавишу «Найти путь» из пользовательского меню. Здесь возможны следующие варианты работы программного обеспечения:

- При наличии только одного пути он отмечается как наикратчайший и выделен зеленым цветом;
- При наличии двух путей, наикратчайший из них обозначается зеленым цветом, второй – красным;
- При наличии более чем 2 путей ищется, в соответствие с алгоритмом Дейкстры, наикратчайший (зеленый цвет) и следующий по сумме весов за наикратчайшим путь (красный цвет).

5). После завершения конфигурирования нужного вам участка транспортной сети MPLS и поиска путей, необходимо заполнить таблицы исходных параметров работы сети MPLS, выводимых на экран по нажатию клавиши «Каналы». Ниже представлены необходимые шаги при заполнении таблиц и их последовательность:

- Заполнить столбец «Загрузка» таблицы №1 «Список каналов и их загрузка». Значения вводятся в процентах от 1 до 100 соответственно. Каждая строка таблицы ассоциируется с одним из маршрутизаторов для сконфигурированной сети. Таким образом, перечисленные все отмеченные при конфигурировании маршрутизаторы. Программа ожидает заполнения всех строк таблицы, только после этого на экран автоматически выводится следующая таблица;
- По окончании заполнения предыдущей таблицы, на экране появляется таблица № 2: «Исходные параметры для маршрутизаторов». Заполнить столбец «Мощность» значениями в диапазоне от 1 до 5. Таким образом, назначается максимальное число одновременно обрабатываемых пакетов на каждом маршрутизаторе, т.е. емкость секции обработки (обработка пакета –замена метки в нем в соответствии с таблицей коммутации каждого маршрутизатора, размер очереди в мощность не входит).

Заполнить столбец «Максимальный размер очереди» значениями в диапазоне от 3 до 9 мест для каждого маршрутизатора. При вводе числа, выпадающего за пределы указанных диапазонов, на экран выводится сообщение об ошибке и число необходимо изменить для продолжения работы с ПО. Программа ожидает заполнения всех строк таблицы, только после этого на экран автоматически возвращается в главное пользовательское окно приложения.

- 6). При изменении последовательности всех перечисленных выше этапов на экран выводятся предупреждающие сообщения и сообщения об ошибке.
- 7). В нижней средней части экрана выбрать один временной режим работы сети (далее сеанс) из предложенных 2, 3 и 4-х минутных режимов.
- 8). Запуск сеанса происходит по нажатию клавиши «Старт». В правом нижнем углу экрана активизируется графическая статусная строка, на котором в процентном соотношении отображается длительность сеанса. Во время сеанса все остальные действия с программным приложением блокируются во избежание сбоев в работе. По окончании сеанса активируются кнопки вывода статистики.
- 9). При нажатии на кнопку «Вывод статистики» на экране появляется окно, в котором выводятся таблицы со статистикой следующего вида:

Таблица 1. Статистика потерь пакетов на маршрутизаторе за сеанс работы сети.

Маршрутизатор	Общее кол-во пакетов, прошедших через маршрутизатор за сеанс	Общее кол-во потерянных пакетов	% потерь

Таблица 2. Статистика задержек пакетов на маршрутизаторах.

Маршрутизатор	Средняя задержка одного пакета

Таблица 3. Статистика потерь пакетов для потоков данных от каждого отправителя на каждом возможном маршруте.

номер маршрута	общее кол-во пакетов потока 1	общее кол-во пакетов потока 2	общее кол-во пакетов потока 3	% потерь потока 1	% потерь потока 2	% потерь потока 3
1						
2						

10). При нажатии на клавишу «Перезапуск» сбрасывается организованная конфигурация сети, исходные параметры работы, очищаются таблицы статистики. Работу с программой можно начинать заново.

#### 4.3 Подготовка отчета по лабораторной работе №2

Отчет должен выявить понимание студентом изученного теоретического материала по теме «Принципы работы транспортных сетей MPLS», приведенного в первой главе методических указаний, и продемонстрировать практические навыки, полученные в результате выполнения лабораторной работы №1.

Содержание отчета:

1). Составить с помощью программы-конструктора конфигурацию сети MPLS в соответствии со следующими вариантами задания (вариант задания назначается преподавателем):

Вариант задания	Число отправителей	Число путей коммутации
1	1	1
2	2	1
3	3	1
4	1	2
5	2	2
6	3	2
7	1	3
8	2	3
9	3	3

2). Подобрать параметры работы сети таким образом, чтобы потери пакетов были в пределах 10-15% для каждого потока, 15-20% для каждого маршрутизатора, и чтобы средняя задержка не превышала 0,4 секунд для каждого маршрутизатора.

3). Конфигурацию сети и результаты работы программы в виде таблиц статистики перерисовать в отчет, уметь объяснить значения и происхождение всех цифр при защите лабораторной работы.

## СПИСОК ЛИТЕРАТУРЫ

1. E. Rosen, Y. Rekhter, RFC-2547. BGP/MPLS VPNs. March 1999.
2. J. Malcolm, RFC-2702, Requirements for Traffic Engineering Over MPLS. September 1999
3. Y. Katsube, RFC-3063, MPLS Loop Prevention Mechanism, February 2001.
4. A. Malis, RFC-2917, A Core MPLS IP VPN Architecture, September 2000.
5. Стивенс У. Протоколы TCP/IP. В подлиннике
6. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. Второе издание. СПб, 2003
7. Браун С. Виртуальные частные сети, Апрель 2001.
8. Вегешна Ш. Качество обслуживания в сетях IP, изд. Вильямс, Январь 2003.
9. Озеров В. Советы программистов (2-е издание), изд. Символ-Плюс, Декабрь 2002.

# ОТЗЫВ

на дипломную работу студента группы СП-92

**Бочкова Романа Александровича**

тема работы: "**Разработка ПО моделирования процесса обмена разнородным трафиком в сетях MPLS. Часть 2: Сбор и анализ статистических данных**"

Интенсивный рост количества операторов, желающих внедрять сети на базе технологии MPLS, приводит к необходимости поиска новейших методов обеспечения качества обслуживания и создания программ для сбора статистики о работе сети. В данной дипломной работе разрабатываются алгоритмы регистрации различной статистической информации о функциональных элементах сети MPLS, и создается программное обеспечение, реализующее работу алгоритмов.

Наиболее положительный момент в работе дипломника - высокий уровень сложности программного обеспечения. Основываясь на исследовании современных практических и теоретических разработок в области технологии MPLS, дипломник сумел выделить и скомпоновать необходимые для создания программного обеспечения материалы и провести их анализ.

Пояснительная записка выполнена добросовестно, 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 Бочков Роман Александрович достоин присвоения квалификации инженера по специальности " Программное обеспечение вычислительной техники и автоматизированных систем ".

Начальник сектора ЛОНИИС

*Гольдштейн А. Б.*

**Подпись:**