ГОСУДАРСТВЕННЫЙ КОМИТЕТ СВЯЗИ, ИНФОРМАТИЗАЦИИ
И ТЕЛЕКОММУНИКАЦИОНЫХ ТЕХНОЛОГИЙ
РЕСПУБЛИКИ УЗБЕКИСТАН

САМАРКАНДСКИЙ ФИЛИАЛ ТАШКЕНТСКОГО
УНИВЕРСИТЕТА ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

ФАКУЛЬТЕТ “ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ И
ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ”

КАФЕДРА “ТЕЛЕКОММУНИКАЦИОННЫЙ ИНЖИНИРИНГ”

# ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

**на тему**

## Качество обслуживания в сетях ip-телефонии

**ВЫПОЛНИЛ:** студент 4-го курса по
направлению 5522200 -“Телекоммуникация”
Хатамов Ш._____

**НАУЧНЫЙ РУКОВОДИТЕЛЬ:**
Технический директор «Узи-Самарканд»
Каюмов А._____

Выпускная квалификационная работа прошла предварительную защиту.
Протокол № ____ от «___» _____ 2014 г.

Самарканд – 2014

СОДЕРЖАНИЕ

## Введение

**Актуальность темы.** Основополагающие принципы государственной политики в области информационно-коммуникационных технологий (ИКТ) подразумевают их широкое внедрение во все сферы жизни общества с тем, чтобы в нашей стране велась интенсивная работа по интеграции в мировое информационное пространство [1].

В связи с бурным развитием сетевых и коммуникационных технологий, возросшей производительностью компьютеров, и, соответственно, с необходимостью обрабатывать все возрастающее количество информации (как локальной, находящейся на одном компьютере, так и сетевой и межсетевой) возросла роль оборудования и программного обеспечения, что можно обозначить одним общим названием "person to person". Виртуальные средства обучения, удаленный доступ, дистанционное обучение и управление, а также средства проведения видеоконференций переживают период бурного расцвета и предназначены для облегчения и увеличения эффективности взаимодействия как человека с компьютером и данными, так и групп людей с компьютерами, объединенными в сеть. Несмотря на то, что экологическая ниша видеоконференций разработана не на все сто процентов, уже сейчас в мире имеется более 200 компаний, которые предлагают различное оборудование и программное обеспечение для их организации и проведения.

В целях формирования национальной системы информатизации, массового внедрения и использования во всех сферах экономики и жизни общества современных информационных технологий, средств компьютерной техники и телекоммуникаций, наиболее полного удовлетворения растущих информационных потребностей граждан, создания благоприятных условий для вхождения в мировое информационное сообщество и расширения доступа к мировым информационным ресурсам [1]. В указе президента Республики Узбекистан [1] считает важнейшими первоочередными задачами

развития и внедрения современных систем компьютеризации и информационно-коммуникационных технологий:

- создание современных надежных и безопасных национальных информационных баз данных, развитие рынка информационных ресурсов и услуг, последовательный поэтапный переход к электронным формам обмена информацией;

- широкое внедрение компьютерных и информационных технологий в отраслях реальной экономики, в сфере управления, бизнеса, науки и образования, создание условий для широкого доступа различных слоев населения к современным компьютерным и информационным системам;

- введение в учебный процесс в школах, профессиональных колледжах, академических лицеях и высших учебных заведениях прогрессивных систем обучения, основанных на овладении и активном использовании современных компьютерных и информационных технологий;

- организацию подготовки высококвалифицированного кадрового потенциала для работы в сфере информационно-коммуникационных технологий, в первую очередь, в сфере разработки программных средств, информационных баз данных, формирования республиканских, отраслевых и локальных информационно-коммуникационных сетей, разработки компьютерной и телекоммуникационной техники;

- ускоренное развитие технической инфраструктуры информационно-коммуникационных технологий на всей территории страны, включая мобильную связь, IP-технологий, других современных средств телекоммуникации и передачи данных, с учетом конвергенции информационно-коммуникационных сетей и услуг;

- внедрение высокоскоростного доступа к национальным и международным информационным сетям, обеспечение доступа к ним населенных пунктов, включая сельские;

- создание эффективного механизма по стимулированию развития отечественного производства качественных программных продуктов и их экспорта;

- содействие в организации разработки и производства отечественной компьютерной техники и комплектующих изделий к ней.

**Цель работы.** В работе обсуждается тема, связанная с качеством обслуживания в IP-сетях. Указываются определения, описаны методики определения качества в IP-сетях. Обсуждаются протоколы, с помощью которых реализуется уровень качественного обслуживания. Приведено сравнение различных технологий обеспечения качества IP-услуг. Вводится понятие очередей и "алгоритмов борьбы" с ними.

**Основные задачи исследования:**

- Обзор проблемы IP-телефонии и методы их решения;
- исследования методики определения качества в IP-сетях;
- сравнение различных технологий обеспечения качества IP-услуг;
- исследование понятие очередей.

**Структура и объем выпускной квалификационной работы.** Выпускная квалификационная работа состоит из введения, двух раздел и заключения. Содержит список использованной литературы из 12 наименований.

# Глава 1. IP технология

## 1.1. IP-технология - мир телефонии и мир Интернета

IP-технология - это технология, которая связала два абсолютно обособленных до некоторых пор мира - мир телефонии и мир Интернета [6].

Идея передачи речи по IP-сети с помощью персонального компьютера зародилась в университете штата Иллинойс (США). В 1993 году Чарли Кляйн выпустил в свет первую программу для передачи голоса в IP-сети с помощью персонального компьютера Maven..

А в феврале 1995 года израильская компания VocalTec предложила первую версию программы Internet Phone, разработанную для владельцев мультимедийных PC, работающих под операционной системой Windows. Это стало важной вехой в развитии IP-телефонии. В том же 1995 году и другие компании очень быстро оценили перспективы, которые открывали возможность разговаривать, находясь в разных полушариях Земли, и не платя при этом за международные звонки.

Конечно, качество такой связи оставляло желать лучшего, и пользовались ею лишь немногие. Но все изменилось, когда выяснилось, что при помощи не слишком дорогой технологии можно совмещать стандартные телефонные сети и сети Интернет - телефонии. В 2000 году доходы от предоставления услуг IP-телефонии разными компаниями составили уже 1800 миллионов долларов, и на эту перспективную технологию обратили внимание компании AT@T, Quest, Global One, которые начали скупку акций провайдеров и разработчиков этого вида связи. А крупнейшие производители отраслевого оборудования занялись разработкой аппаратных комплексов для IP- сетей...

Нынешний лидер по производству решений и аппаратной базы для производителей оборудования IP-телефонии - это AUDIOCODES Израиль. Именно их решения для программно-аппаратной обработки голоса TP100 позволили компании VocalTec выпустить первыми коммерческое решение

для IP-телефонии, которое стало лидирующим на несколько лет. И до настоящего момента это решение является основным для построения коммерческих сетей шлюзов IP-телефонии, распределенных в Сети Интернет.

В России Интернет - телефония развивается не менее быстро, чем, скажем, в той же Америке. И так же, как в других "компьютеризованных" странах, у нас больше всего распространена технология американской фирмы Cisco, которая занималась производством оборудования для маршрутизации компьютерных сетей во всем мире.

Но, хотя существуют другие технологии IP-телефонии, для людей "понимающих" на первом месте, бесспорно, стоит технология VocalTec, как органично развивающаяся, "родная ветвь" Интернет - телефонии. Самые первые коммерческие сети в России и МИРЕ, устойчиво и качественно работающие на реальных сетях Интернет, были построены на технологии Vocaltec. В России несколько компаний (RGC, IncomTel TG и OSS) построили свои коммерческие сети на платформе VocalTec. И, несмотря на лидирующие позиции по продажам оборудования у компании Cisco, не отказываются от этой платформы и продолжают ее развивать из-за более высокой управляемости всей сети шлюзов и более высокого качества обработки голоса и факса в условиях сети Интернет.

Что касается различия качества и цен в IP-телефонии вообще, то в данном случае можно сказать следующее: здесь, как в магазине, существуют разные сорта связи.

Пользуется спросом как "хорошая" IP-связь и подороже, так и "плохая", но дешевая. Кого-то устраивает и не слишком хорошая, но недорогая связь. Однако такая связь вряд ли подойдет, например, для ведения деловых переговоров с партнерами...

## 1.2. IP-телефони́я

Телефония — это комплекс технологий обмена голосовыми сообщениями в режиме реального времени. IP-телефония — комплекс технологий обмена голосовыми сообщениями, использующий сеть IP в качестве транспортной. Исходя из второго определения, выделим более широкое множество — комплекс технологий обмена голосовыми сообщениями и использующий сети с коммутацией пакетов в качестве транспортных. В основе всех этих технологий лежат общие технические принципы. Следовательно, IP-телефония есть подмножество более широкого понятия — пакетной телефонии. А термин «IP-телефония» прижился просто благодаря моде на Интернет и всему, что с ним связано [3,5].

**IP-телефони́я** (произносится «*айпи́-телефони́я*») — телефонная связь по протоколу IP. Под IP-телефонией подразумевается набор коммуникационных протоколов, технологий и методов, обеспечивающих традиционные для телефонии набор номера, дозвон и двустороннее голосовое общение, а также видео общение по сети Интернет или любым другим IP-сетям. Сигнал по каналу связи передаётся в цифровом виде и, как правило, перед передачей преобразовывается (сжимается) с тем, чтобы удалить избыток информации и снизить нагрузку на сеть передачи данных.

Изначально для передачи голоса использовался аналоговый сигнал — электромагнитная волна, передаваемая по медному проводу. Для одновременной передачи нескольких аналоговых сигналов по одному проводу использовалось частотное мультиплексирование (уплотнение). Основная полоса частот канала делится на некоторое число полос (подканалов) с помощью фильтров с частотами среза, сдвинутыми на 4 кГц относительно друг друга (фактическая полоса пропускания канала — 3,1…4 кГц). Полосы сдвигаются друг относительно друга методом амплитудной модуляции. Для устранения взаимного влияния подканалов используется защитная полоса, как правило, шириной 900 Гц (иногда ее можно услышать в

трубке как шипение или вой). При высоких уровнях сигнала в каналах возникает перекрестная наводка, из-за которой слышен параллельный разговор или радио (последнее — результат улавливания радиосигнала каким-либо контуром).

Если уменьшить ширину полосы, в основной диапазон можно запихнуть больше подканалов. Модем на такой линии будет работать очень плохо (или вообще не сможет), хотя голос будет вполне узнаваем (мозг способен восстанавливать нечеткий или ошибочный сигнал так, как это не снилось современным адаптивным кодекам типа CS-ACELP).

Потом придумали временное мультиплексирование, при которой для передачи сигнала каждого подканала используется фиксированный временной интервал (тайм-слот), а за ней — импульсно-кодовую модуляцию, позволившую перейти от аналогового сигнала к цифровому. Когда это случилось (довольно давно, кстати), конвергенция в традиционных сетях связи завершилась, хотя связисты об этом даже не подозревали.

Сети передачи данных создавались для обмена цифровой информацией. Основной особенностью трафика данных является его асинхронность. Когда компьютеры были большими, а процессорное время дорогим, использовалась пакетная обработка данных: формировался пакет задач, который загружал центральный процессор, а результаты раздавались всем пользователям по окончании вычисления. Поэтому временное мультиплексирование на каналах ввода-вывода было обычным делом. Кроме того, при передаче цифровых данных применяются коды с коррекцией ошибок, а также алгоритмы перезапроса пропавших при передаче пакетов.

Отдельной задачей в сетях телефонии является маршрутизация и коммутация вызовов. Сначала эти функции выполняло разумное устройство под названием «барышня». Потом некто великий, не помню кто, изобрел автоматический коммутатор. По легенде он был похоронных дел мастером, а жена его конкурента работала на телефонном узле разумным коммутатором и, первой узнавая о потенциальном покупателе, соединяла с конторой мужа.

Поэтому бизнес у нашего гробовщика шел плохо, и он решил податься в связисты.

Сейчас для маршрутизации вызовов в телефонной сети используется группа протоколов SS7 (российский аналог — ОКС №7). Самое интересное, что для передачи сигнальных сообщений в SS7 используется пакетный протокол со статической маршрутизацией (в терминах IP). Развитие сетей передачи данных привело к отказу от временного мультиплексирования в пользу пакетной коммутации с установлением соединения (X.25, Frame Relay, ATM). Эта тенденция была обусловлена необходимостью выжать из емкости физического канала как можно больше, и сети с пакетной коммутацией используют для этого асинхронность, присущую природе трафика данных. Однако маршрутизация вызовов в таких сетях строилась на основе старых добрых телефонных принципов (кстати, X.25 и ATM имеют одинаковый с телефонией стандарт адресации ITU-T E.164). Сначала по служебному каналу происходила сигнализация установления соединения (то есть всем транзитным коммутаторам сообщалось о необходимости резервирования ресурсов под канал передачи), а затем начиналась собственно передача данных. Поэтому эти сети были жестко иерархическими и централизованными. Исключением являются сети ATM, но к моменту возникновения этой технологии уже был накоплен огромный опыт динамической маршрутизации в сетях IP.

*IP-революция.* Революционность и успех протокола IP обусловлен тремя факторами. Во-первых, это протокол без установления соединения, использующий динамическую маршрутизацию пакетов. Чтобы начать передачу данных, не нужно сигнализировать приемнику и всем транзитным коммутаторам о необходимости создать канал из точки A в точку B. Сеть принимает пакет и маршрутизирует его «как фишка ляжет» [3]. Казалось бы, очень ненадежная система на деле оказалась сверхживучей (задачей разработчиков было построить сеть, которая бы функционировала при выходе из строя любого количества узлов). Во-вторых, это принцип

независимости IP-стека от физической среды передачи. И наконец, гений Джона Постела, сформировавшего такие принципы принятия технических решений в Интернет-сообществе, которые сделали эти решения открытыми и общедоступными.

Решать проблемы передачи голоса по сетям с коммутацией пакетов пришлось, когда стали массово внедряться сети передачи данных. Организация, строившая инфраструктуру с нуля, была вынуждена строить две фактически независимые сети: одну для данных, другую для телефонии. Операторы связи, до 80% оборота реинвестирущие в инфраструктуру, тоже задумались над унификацией инфраструктуры для передачи всех видов трафика. Пока трафик данных не превалировал в сетях операторов связи, этот процесс шел медленно. Все изменил Интернет, благодаря которому появилась масса приложений и решений в области передачи данных по IP-сетям. Услуги Интернета стали доступны даже там, где услуги телефонии были минимальны. Появилась возможность общаться чуть ли не со всем миром за небольшую плату, причем практически в реальном времени. А раз можно общаться в чате с помощью клавиатуры, почему не попробовать делать это с помощью микрофона и мультимедийных колонок? Сначала возникли «наколенные» разработки, потом за дело взялись стартапы, за ними встрепенулись гиганты вроде Cisco, и мир связи вздрогнул.

*ATM*. Наиболее глубоко основные проблемы передачи голоса по пакетным сетям были проработаны при создании ATM. Здесь была предпринята попытка суммировать все накопленное сообществом как в области передачи данных, так и в области традиционной телефонии. Был расширен стандарт сигнализации для установления и управления соединений широкополосных сетей (B-ISDN), разработаны технологии широковещательной трансляции для групп абонентов (механизмы IP-multicast к тому времени уже существовали, но для широкополосных глобальных сетей это было новостью), созданы хитроумные методы контроля качества передачи, опиравшиеся на природу того или иного вида

трафика. Кроме того, были разработаны технологии динамической маршрутизации с учетом качества обслуживания (QoS). Однако ATM не повезло, и, несмотря на всю комплексность и изощренность, технологию в настоящий момент можно считать мертвой. На мой взгляд, произошло это потому, что косность механизма принятия стандартов, их относительная закрытость, а также беспрерывные войны производителей за влияние на этом поле и, отчасти, сложность реализации не привели к созданию массовой индустрии решений для конечных пользователей. Оказалось, что проще инкапсулировать IP в ATM (принцип независимости от среды передачи) и использовать весь спектр IP-приложений, чем создавать приложения, «заточенные» именно под ATM [4].

*То же произошло и с телефонией.* Для стыка с унаследованными телефонными системами была разработана технология CES (circuit-emulation services), которая прозрачно транслировала TDM-каналы через сеть ATM. АТС связывались между собой по CES. При этом ATM-облако было для них совершенно прозрачно. Разумеется, это не стимулировало разработку ATM-телефонных станций и ATM-телефонов, аналогичных ISDN-продуктам.

*От реальности к виртуальности.* Следующим шагом стала оформившаяся по результатам всей этой титанической работы концепция виртуального коммутатора. Традиционная телефонная сеть жестко иерархична по уровням: зона, регион, центр агрегации (toll switch), городской коммутатор, учрежденческий коммутатор, PBX. Соответственно для организации регионального транзита телефонного трафика необходимо установить в каждом регионе мощный коммутатор и связать их всех между собой огромным количеством транковых каналов и каналов сигнализации, объединив в сеть SS7. Транзитный вызов сначала «поднимается» с помощью протоколов сигнализации по уровням, а затем «опускается» для определения конечного абонента в другом регионе. Всем коммутаторам отдается команда обеспечить соединение (выделить ячейки в коммутационной матрице). При этом число транковых каналов, а значит, количество одновременных

соединений и емкость коммутационной матрицы АТС всегда во много раз меньше, чем общее количество абонентов, подключенных к коммутатору, поскольку статистически все пользователи одновременно не разговаривают. Если такое вдруг случится, телефонная сеть захлебнется (кстати, так и происходит в Новый год, когда за пять минут до боя курантов народ кидается поздравлять друг друга) [7].

Предположим, ATM или IP-сеть с узлами доступа есть в каждом регионе. На граничном коммутаторе определяется адрес конечного абонента, а затем вызов маршрутизируется по этому адресу автоматически. При этом вся сеть работает как один большой распределенный коммутатор. Использование концепции «виртуального коммутатора» позволяет значительно сократить вложения в инфраструктуру при построении крупных сетей связи.

### 1.3. Проблемы IP-телефонии и методы их решения

Основная проблема IP-сетей — качество обслуживания при транзите трафика реального времени. IP-протокол не нуждается в установлении соединения. Его базовый принцип состоит в том, что связность (connectivity) есть фундаментальный атрибут сети, позволяющий любому абоненту осуществлять коммуникацию с любым другим абонентом без процедуры установления соединения, резервирования ресурсов на транзитных коммутаторах и т. д. Однако это означает, что приложения, основанные на IP, не должны зависеть от вариации задержек при передаче пакетов. Для HTTP-протокола не важно, скачивается веб-страница пять или пятнадцать секунд. Для голосового трафика вариация задержки даже более критична, чем потеря пакетов. Пропадание одного или нескольких пакетов с короткими голосовыми фрагментами может быть компенсировано алгоритмом кодека с помощью адаптивной экстраполяции. В конце концов, пропадание цепочки фрагментов воспринимается ухом лишь как щелчок. А вот вариация

задержки приводит к запаздыванию и плаванию звука, мешающим разговаривать. Из того же фундаментального принципа IP следует, что транзитный путь каждого конкретного пакета может быть разным. Следовательно возникает еще и проблема переупорядочивания пакетов.

Дабы решить общие проблемы качества обслуживания в IP, прикладывались колоссальные усилия. Были разработаны механизмы предупреждения и управления перегрузками транзитных коммутаторов и дифференциации классов IP-трафика. Но для обеспечения сквозного контроля качества от источника к приемнику их оказалось недостаточно. В результате был разработан протокол резервирования ресурсов для контроля качества обслуживания (RSVP). Он представляет собой протокол сигнализации всем транзитным коммутаторам о резервировании ресурсов для передачи высокоприоритетного трафика и выполняет две функции: определение оптимального (с точки зрения качества обслуживания) пути от источника к приемнику и резервирование необходимых ресурсов. Появление этого механизма фактически означает возврат к принципу предварительной сигнализации и установления соединения с заданными параметрами, как это и происходит в сетях традиционной телефонии и унаследованных пакетных сетях [8].

Другая проблема IP — избыточность заголовков. Есть такое понятие, как «задержка на пакетизацию голоса». Это время, используемое для заполнения пакета оцифрованными голосовыми фрагментами. Чем оно больше, тем больше голосовых фрагментов можно упаковать в пакет и тем эффективнее использование полосы пропускания. Однако абсолютная величина этой задержки ограничена. Если суммарная задержка в сети телефонии превышает 50 мс, возникает эхо-эффект и должны применяться алгоритмы эхоподавления. При разработке ATM было установлено, что размер полезного пространства ячейки (payload), равный 32 октетам, приводит к задержке пакетизации в 15 мс, что позволяет обойтись без эхоподавления. Однако наибольшая эффективность заполнения ячейки (с

учетом того, что ATM-заголовок содержит всего пять октетов), а значит, и эффективность использования полосы пропускания достигается при 64 октетах. После долгих споров ITU-T одобрил фиксированный полезный размер ячейки, равный 48 октетам, что является средним арифметическим между скоростью и эффективностью.

Заголовок IP-пакета составляет 24 октета. Существует также заголовок второго уровня модели OSI. Это означает, что для адекватного использования полосы необходимо увеличить эффективное пространство пакета минимум в пять раз. Кроме того, имеет место задержка транзитной передачи по сети. В реальной жизни IP-телефония с приемлемым уровнем качества живет при общей задержке в 200–250 мс (хотя некоторые умудряются разговаривать и при 400–500 мс) благодаря применению механизмов эхоподавления и умных кодеков. Тем не менее, это приводит к значительному объему ненужного трафика, да и качество не совсем коммерческое. Для передачи мультимедиа-данных был разработан протокол RTP/RTCP (Real Time (Control) Protocol), обеспечивающий определение типа трафика, секвенсирование, временные метки фрагментов, синхронизацию и контроль передачи. RTP работает поверх UDP (это еще плюс 20 октетов заголовков). Механизм такой: сначала, используя протокол TCP, посылается сигнал вызова. Абонент подтверждает соединение (снимает трубку), устанавливается контрольное соединение (RTCP) и открывается несколько UDP сессий для передачи RTP-трафика.

Дабы избежать избыточности заголовков, была разработана технология компрессии заголовков CRTP, позволяющая сократить их размер в среднем до 2–4 октетов при передаче RTP-трафика. Принцип компрессии заголовков придуман Ван Якобсоном на заре развития IP-стека и основан на том, что после установления соединения служебная информация заголовков уже не нужна, коль скоро две системы договорились о параметрах соединения. Алгоритм Ван Якобсона, описанный в RFC 1144, применим для протокола TCP, ориентированного на установление соединения. CRTP — более

продвинутая технология, обеспечивающая компрессию IP/UDP/RTP-заголовков. Идея заключается в том, что для обмена контекстом компрессии (статической информацией, содержащейся в заголовках исходных инкапсуляций, информацией о синхронизации и т. п.) выделяется специальное TCP-соединение. Тем не менее, протокол CRTP не решил всех проблем, связанных с избыточностью заголовков. На соединениях с большим количеством транзитных узлов (маршрутизаторов), а также на медленных или перегруженных каналах возникли проблемы масштабируемости. Каждый потерянный в пути компрессированный пакет вынуждает приемник сбрасывать и перезапрашивать целую цепочку, поскольку контекст компрессии рассинхронизируется на время всего цикла пути (round-trip-time — время прохождения пакета туда и обратно). Поэтому применение CRTP зачастую ограничено двумя соседними маршрутизаторами, соединенными прямыми каналами. Кроме того, реализация CRTP требует больших вычислительных ресурсов.

***Эволюция технологии.*** Попытки строительства на базе стека IP мультисервисных сетей с поддержкой QoS, а также появление технологий, позволяющих увеличить пропускную способность физической инфраструктуры передачи данных (DWDM для оптоволокна и xDSL для меди), привело к эволюции самой технологии коммутации IP-пакетов. До Интернета ни одна сеть не достигала таких масштабов без того, чтобы не рухнуть под весом комплексных архитектурных проблем. Модернизации IPv4 назрела давно, и новая версия стека IPv6 отвечает на множество системных вопросов. Но появление IPv6 не стало революционным скачком — массового перехода на новую версию не было. Интернет демонстрирует гибкость и способность эволюционировать, сохраняя преемственность приложений. Технологии, разрабатываемые в рамках решения конкретных проблем, приводят к изменениям общей архитектуры сетей связи на системном уровне. Одна из таких технологий — MPLS — технология мультипротокольной коммутации меток [7].

MPLS изначально разрабатывалась для решения задач оптимизации маршрутизации IP по сетям ATM и ускорения поиска адреса приемника по таблице маршрутизации. Принцип изоляции IP-стека от канального и физического уровня модели OSI позволяет легко переносить IP-приложения на любую физическую среду передачи, однако вызывает ряд проблем эффективности маршрутизации. Если IP-сеть построена на коммутируемых виртуальных соединениях в ATM-облаке, то при отказе одного из соединений сначала произойдет конвергенция на уровне ATM, а уж затем начнется конвергенция IP-сети. Это фундаментальная проблема, поскольку на уровне ATM могут быть приняты решения о маршрутизации, конфликтующие с решениями, принятыми на уровне IP. Предположим, в ATM-облаке возникла перегрузка одного или нескольких коммутаторов, что отразилось на качестве обслуживания виртуальных соединений. Уровень IP об этом понятия не имеет, следовательно, речи о маршрутизации приоритетных IP-пакетов с заданным качеством обслуживания быть не может.

Решая эти проблемы, разработчики MPLS предложили разделить контрольную и коммутационную компоненты при маршрутизации трафика, а также ввести фиксированный идентификатор пакета — метку. Метка представляет собой заголовок фиксированной длины, идентифицирующий множество пакетов, передаваемых определенным образом (например, одному и тому же адресату или в соответствии с некоторым классом обслуживания). Метка имеет локальное для коммутатора значение, то есть не является адресом.

Контрольная компонента архитектуры включает протокол маршрутизации третьего уровня модели OSI (в случае IP это OSPF или IS-IS), который работает согласованно с процедурами распределения и распространения меток. Она выполняет функции установления значений меток вдоль пути коммутации в соответствии с маршрутной информацией IP

(или другого протокола). Эти функции реализуются с помощью протокола распространения меток (LDP) [4].

После этого об ATM все постепенно забыли и начали разрабатывать новые возможности технологии, такие как новая концепция виртуальных частных сетей (VPN) и технологии управления потоками трафика в магистральных сетях (Traffic Engineering). Последние имеют непосредственное отношение к проблеме качества обслуживания в IP-сетях.
Протоколы маршрутизации в IP-сетях основаны на алгоритме Дейкстры — алгоритме построения кратчайшего пути в связном графе (SPF-протоколы, такие как OSPF, IS-IS). Все маршрутизаторы строят дерево кратчайшего пути к остальным узлам сети. Маршрутные таблицы строятся на основании этого дерева.

При чем здесь IP-телефония? В конце 1999 года один из подписчиков списка рассылки IETF, посвященного разработке стандартов MPLS, задал сакраментальный вопрос: почему в названии MPLS присутствует слово «мультипротокольная», ведь работа идет над проблемами коммутации IP. На что гуру ему ответили: дескать, разрабатываемая концепция может быть применена к любому маршрутизируемому протоколу, но раз уж IP является доминирующим, то ради него все и стараются. Товарищ на этом не успокоился и инициировал дискуссию о передаче голоса по MPLS-сети. Идея проста и базируется на принципах коммутации в традиционных сетях телефонии. Коль скоро сигнализация и установление пути отделены от коммутации трафика, зачем добавлять лишнюю инкапсуляцию уровня IP для передачи оцифрованных голосовых фрагментов? Дискуссия завершилась выделением этого направления из рабочей группы IETF, однако работа шла, и в конце концов MPLS Forum выпустил рекомендацию «Voice over MPLS implementation agreement». Суть этого документа — определение архитектуры, форматов заголовков для оцифрованных голосовых фрагментов, DTMF-сигналов, передачи внутриканальной сигнализации

(CAS) и т. п. Некоторые компании уже производят оборудование, позволяющее строить системы, основанные на этих принципах.

Существует множество других системных и технологических проблем в области IP-телефонии, которые в настоящее время достаточно успешно решаются Интернет-сообществом. Это проблемы общей архитектуры сети, эффективной маршрутизации телефонных вызовов (анонсирования маршрутов к абонентам и точкам шлюзования трафика и их атрибутам, таким как качество, стоимость, величина транспортной задержки и пр.), проблемы адресации, авторизации и учета пользования ресурсами сети для телефонных абонентов и т. д.

Что же делает IP-телефонию (и вообще пакетную телефонию) привлекательной и каковы ее перспективы?

Прежде всего, пакетную телефонию нельзя рассматривать в отрыве от других видов мультимедийного трафика, таких, например, как видеоконференцсвязь, пакетное телерадиовещание и т. п. Природа мультимедийного трафика единообразна для всех его видов. Поэтому IP-телефония и наработанные в этой области технологии составляют базу для мультимедийного мира будущего. Более того, уже сейчас при среднесрочном планировании ИТ-инфраструктуры нужно учитывать возможность появления этих сервисов [7].

Внедрение IP-телефонии как простой альтернативы стандартной телефонной связи для корпоративных клиентов, на мой взгляд, малоэффективно. Да, можно чуть сэкономить на междугородних переговорах и снизить затраты на инфраструктуру и сопровождение. Но если вам нужна просто учрежденческая АТС, лучше купить просто учрежденческую АТС. Многие производители подходят к IP-телефонии как к дополнительной игрушке на базе АТС, подключая к ней локальную сеть и вешая на нее модные IP-телефоны. Этот путь представляется мне тупиковым. IP-телефония ценна тем, что на базе единой технологической платформы интегрируются в единое информационное пространство два мира: мир

компьютерной обработки информации и мир услуг голосовой связи. На пересечении этих миров открываются новые возможности, которые предприятия могут использовать для повышения производительности, а компании, развивающие бизнес интегрированных ИТ-услуг, — для разработки новых бизнес-моделей. IP-телефон сейчас представляет собой универсальный терминал, работающий по технологии тонкого клиента с универсальным мультимедийным сервером. Программирование на базе открытых стандартов позволяет легко превращать этот телефон в специализированный терминал, выполняющий те или иные производственные операции, например диспетчерский пульт, получающий данные из информационной системы и используемый для экстренной связи или ввода управляющей информации. На основе мультимедийных серверов можно организовывать универсальные порталы для общекорпоративной работы, интегрируя web-технологии, видеоконференцсвязь, электронную почту и телефонию. Возможности безграничны.

### 1.4. IP-технологии в простых и понятных примерах

Маршрут по умолчанию. Подойтите к прохожему и спросите «не подскажите ли вы как пройти к моргу имени Невмировича-Данченко?». С большой долей вероятности вас пошлют на три известные буквы. Так вот это и есть маршрут по умолчанию. Другими словами, если адрес назначения не известен, то пакеты посылаются на маршрут по умолчанию (синонимы: шлюз по умолчанию, dafault gateway) [7].

Понятие TTL. Представьте себе, что вам 5 лет и вы хотите кушать. Вы идете к папе и говорите: «Папа, я хочу кушать». Ваш папа смотрит телевизор и согласно таблице маршрутизации он посылает вас к маме. Вы идете к ней и просите «Мамааа, я хочу кушать». Мама болтает с подругой по телефону и согласно своей таблице маршрутизации посылает вас к папе. И так вы ходите как дурак от папы к маме и обратно, туда-сюда, туда-сюда, а все потому, что

криворукие админы (родители папы и мамы) неправильно настроили таблицу маршрутизации. Чтобы защититься от таких ситуаций придумали понятие TTL (Time To Live), что применительно к нашей ситуации означает количество терпения у мальчика, пока он не скажет «задрало!» и не упадет перед ногами мамы или папы в беспомощном состоянии. Последний, по правилам (стандарты – это «так заведено в семье»), обязан послать короткий нелестный отзыв адрес того, кто послал мальчика кушать. Это так называемый ICMP-пакет «мальчик издох».

Ping. Вы, конечно, бывали в ситуации «кто там». Вы кричите «Карим, это ты!», а в ответ слышите: «Да, я!». Это простеший пинг. Вы только что пропинговали Васю. Не все отвечают на пинги, особо культурные, например, Microsoft.com, не утруждают себя реагированием на ваши запросы. С такими переругиваться бесполезно: мы знаем, что они слышат и злятся, но реакции добиться не можем. Тем не менее, пинг – неплохой способ узнать, жив ли хост, ведь пиная труп ногами не добьешься реакции «сам дурак».

Traceroute. Представьте себе, что вы живете на 9м этаже и хотите узнать всех жильцов, которые живут от вас до Клавки с 3-го. Берете взрывпакет и, исходя из формулы ускорения свободного падения, рассчитываете время взрыва пакета над 8-м этажом. Это TTL=1.

После того, как пакет рванет - выглянет озверевшая рожа соседа с 8-го этажа. Время реакции зависит от загруженности сервера, т.е. от занятости соседа и от шейпов, т.е. в воздухе ли ваша система или вы живете на планете, где атмосфера - жидкий азот. Так вот, если вообще не дождетесь ответа - ваш сосед глухой, то есть у него запрещены ICMP-ответы либо он запретил их только для вас, если его уже заколебали ваши финты и он научился вас игнорировать. Дальше выставляете TTL=2 и т.д. Не забывайте, что если Клавка живет выше вас – это no route to host.

# Глава 2. Сравнение различных технологий обеспечения качества ip-услуг

## 2.1. Понятие QoS

Сети с коммутацией пакетов на основе протокола IP не обеспечивают гарантированной пропускной способности, поскольку не гарантируют доставку.

Для приложений, где не важен порядок и интервал прихода пакетов, время задержек между отдельными пакетами не имеет решающего значения. IP-телефония является одной из областей передачи данных, где важен порядок прихода пакетов и важна динамика передачи сигнала, которая обеспечивается современными методами кодирования и передачи информации. Транспортные протоколы стека TCP/IP, функционирующие поверх протокола IP, не обеспечивают высокого качества обслуживания трафика, чувствительного к задержкам. Протокол TCP, хоть и гарантирует достоверную доставку информации, но переносит ее с непредсказуемыми задержками. Протокол UDP, который, как правило, используется для переноса информации в реальном времени, обеспечивает меньшее, по сравнению с протоколом TCP, время задержки, но, как и протокол IP, не содержит никаких механизмов обеспечения качества обслуживания [4].

Вместе с тем необходимо обеспечить механизмы, по которым в периоды перегрузки пакеты с информацией, чувствительной к задержкам (например, речь), не будут простаивать в очередях или получат более высокий приоритет, чем пакеты с информацией, не чувствительной к задержкам. Для этой цели в сети должны быть реализованы механизмы, гарантирующие нужное качество обслуживания (Quality of Service - QoS).

Объективными, измеряемыми или рассматриваемыми показателями качества являются:

- изменение задержки в сети;
- пропускная способности сети.

Время отклика оценивается по:

- промежутку времени от момента передачи пакета до момента приема подтверждения;
- времени задержки однонаправленного сквозного соединения, также называемой временем запаздывания (latency);
- пропускной способности.

Готовность и надежность оценивается по:

- возможности получения доступа к ресурсам сети или коэффициенту использования;
- результатам контроля уровня обслуживания 24/7 (при режиме работы 24 часа в сутки, 7 дней в неделю).

Меры обеспечения QoS, применяемые в IP- сетях:

- Резервирование ресурсов (на время соединения запрашиваются и резервируются необходимые для выполнения приложения ресурсы).
- Приоритезация трафика (разделение трафика в сети на классы с приоритетным порядком обслуживания некоторых из них).
- Перемаршрутизация (позволяет при перегрузке в сети перевести трафик на резервный маршрут; именно этим способом обеспечивается QoS в подавляющем большинстве контроллеров SBC).

В современных IP-сетях перечисленные меры реализуются с помощью технологий IntServ, DiffServ и MPLS с использованием протокола RSVP.

### 2.2. Трафик реального времени в IP-сетях

Как правило, большую часть VoIP-трафика составляют потоки информации, чувствительной к задержкам. Максимальная задержка не должна превышать 250 мс, причем сюда входит и время обработки информации на конечной станции. Вариацию задержки (джиттер) также необходимо свести к минимуму. Кроме того, необходимо учитывать, что при сжатии информация становится более чувствительной к ошибкам,

возникающим при передаче, и их нельзя исправлять путем переспроса именно из-за необходимости передачи в реальном времени [5,7].

Общая задержка речевой информации делится на две основные части - задержка при кодировании и декодировании речи в шлюзах или терминальном оборудовании пользователей и задержка, вносимая самой сетью. Уменьшить общую задержку можно двумя путями: во-первых, спроектировать инфраструктуру сети таким образом, чтобы задержка в ней была минимальной, и, во-вторых, уменьшить время обработки речевой информации шлюзом [10].

Для уменьшения задержки в сети нужно сокращать количество транзитных маршрутизаторов и соединять их между собой высокоскоростными каналами. А для сглаживания вариации задержки можно использовать такие эффективные методы, как, например, механизмы резервирования сетевых ресурсов.

Одним из способов избежать того, чтобы речь и другая информация, требующая передачи в режиме реального времени, не простаивала в очередях наравне со статической информацией (обычные, не голосовые данные), является выделение и сортировка пакетов, содержащих голосовую информацию.

### 2.3. Дифференцированное обслуживание разнотипного трафика - Diff-Serv

Опция DiffServ позволяет классифицировать пакеты из трафика, идущего в локальную сеть. Работа DiffServ основывается на идентификаторе DSCP, представляющем собой первые 6 бит поля TOS. DSCP определяет, как будут перенаправляться пакеты в DiffServ-сети (PHB, Per-hop Behavior). Изменяя значение этого идентификатора, различные виды трафика можно распределить по приоритетам в очереди.

Модель Diff-Serv описывает архитектуру сети как совокупность пограничных участков и ядра. Пример сети согласно модели Diff-Serv приведен на рисунке 1.

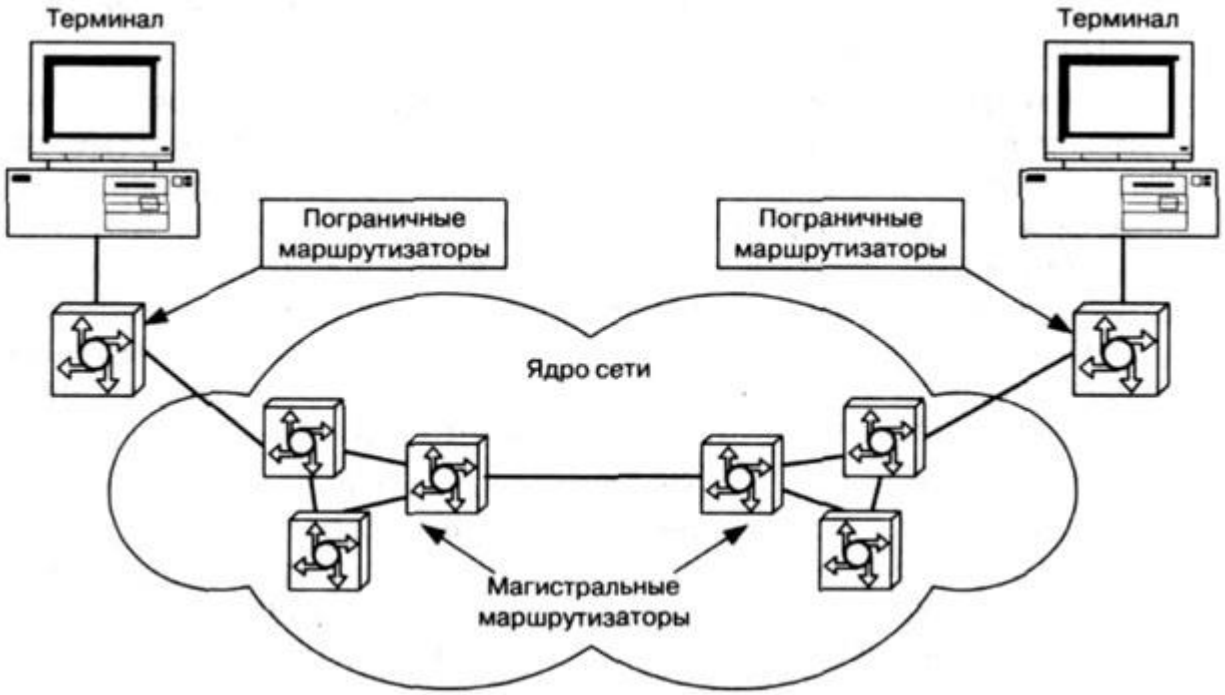


Рис. 1. *Модель Diff-Serv*

Поступающий в сеть трафик классифицируется и нормализуется пограничными маршрутизаторами. Нормализация трафика предусматривает измерение его параметров, проверку соответствия заданным правилам предоставления услуг, профилирование (при этом пакеты, не укладывающиеся в рамки установленных правил, могут быть отсеяны) и другие операции. В ядре сети магистральные маршрутизаторы обрабатывают трафик в соответствии с классом PHB, код которого указан в поле DS.

Достоинства модели Diff-Serv:

1. обеспечивает единое понимание того, как должен обрабатываться трафик определенного класса;
2. позволяет разделить весь трафик на относительно небольшое число классов и не анализировать каждый информационный поток отдельно;

3. нет необходимости в организации предварительного соединения и в резервировании ресурсов;
4. не требуется высокая производительность сетевого оборудования.
5. К настоящему времени для Diff-Serv определено два класса трафика:
6. класс срочной пересылки пакетов (Expedited Forwarding PHB Group);
7. класс гарантированной пересылки пакетов (Assured Forwarding PHB Group).

Механизм обеспечения QoS на уровне сетевого устройства, применяемый в Diff-Serv, включает в себя следующие операции. Сначала пакеты классифицируются на основании их заголовков. Затем они маркируются в соответствии с произведенной классификацией (в поле приоритета Diff-Serv в зависимости от маркировки выбирается алгоритм передачи, при необходимости - с выборочным удалением пакетов), позволяющий избежать заторов в сети. Заключительная операция чаще всего состоит в организации очередей с учетом приоритетов [13].

### 2.4. Интегрированное обслуживание IntServ

IntServ (Integrated Services) больше подходит для концентрации трафика в пограничной сети IP и не рекомендована для применения в транзитных сетях IP (из-за проблем с масштабируемостью).

Модель с интеграцией услуг была предложена в начале 90-х годов и разрабатывалась для обслуживания единичных потоков, которым предоставляется два вида услуг: гарантированные и с управляемой нагрузкой. Гарантированные услуги позволяют обеспечить определенному объему трафика поддающееся количественному вычислению максимальное значение задержки при прохождении пакетов из конца в конец. Услуги с управляемым уровнем нагрузки предоставляют определенному объему трафика обслуживание best-effort при виртуальной низкой сетевой нагрузке без строгих гарантий.

Рассмотрим структурную схему IntServ (рис. 2).

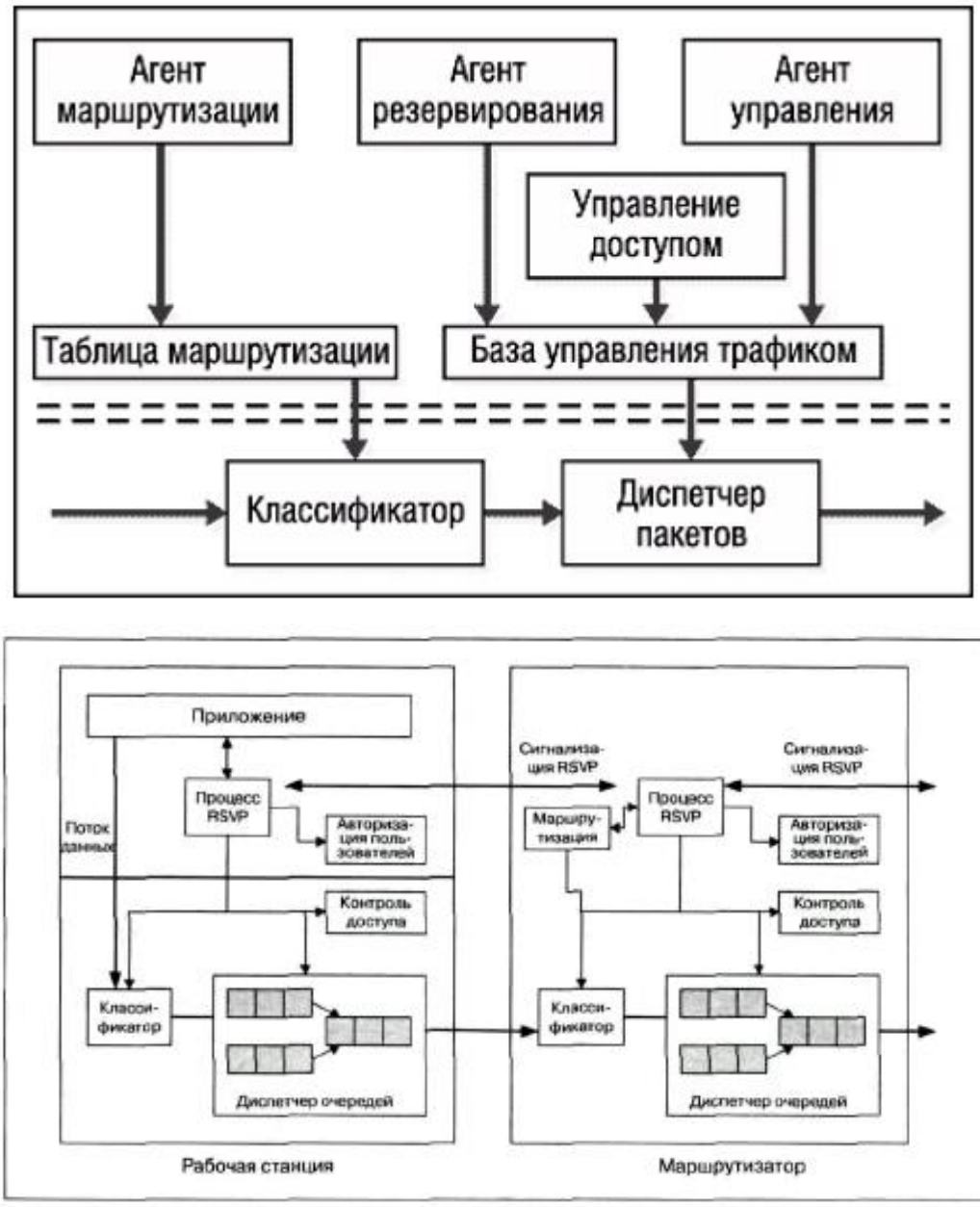


Рис.2. *Модель IntServ*

В каждом узле, поддерживающем IntServ, должно быть несколько обязательных элементов:

1. классификатор - направляет поступающий пакет в один из классов обслуживания согласно информации, полученной из заголовков (сетевого и транспортного уровней) пакета. Класс обслуживания реализуется в виде отдельной очереди. Все пакеты в пределах одного класса обслуживания должны получать одинаковый QoS;

2. диспетчер пакетов - извлекает из каждой очереди пакеты и направляет их на канальный уровень. Для IntServ предложен двухступенчатый диспетчер пакетов. Все поступающие пакеты обрабатываются в соответствии с дисциплиной обслуживания WFQ для изоляции потоков, получающих гарантированные услуги, от всех остальных. Потоки с управляемой нагрузкой и потоки best-effort разделяются с помощью приоритетов;
3. блок управления доступом (admission control) - принимает решения о возможности получения трафиком требуемого количества ресурсов, не влияя при этом на ранее предоставленные гарантии. Управление доступом выполняется на каждом узле для принятия или отклонения запроса на выделение ресурсов по всему пути прохождения потока;
4. протокол резервирования ресурсов - информирует участников соединения (отправителя, получателя, промежуточные маршрутизаторы) о требуемых параметрах обслуживания. Для модели IntServ рекомендуется использовать протокол RSVP.

Сервисная модель IntServ в сочетании с RSVP (см. далее) позволяет организовать гибкое обслуживание разнотипного трафика, максимально учитывая потребности каждого приложения, а использование WFQ для обслуживания пакетов гарантирует максимально допустимое значение задержки. Эта особенность делает IntServ идеальной для обслуживания мультимедийного трафика [7].

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

Но самый большой недостаток IntServ связан с масштабируемостью RSVP, особенно в высокоскоростных магистральных сетях. Действительно, объем ресурсов, которые необходимы маршрутизатору для обработки и хранения информации RSVP, увеличивается пропорционально количеству потоков QoS. Измерения трафика показывают, что большинство соединений IP "из конца в конец" существует очень недолго, и в каждый момент времени магистральным маршрутизатором поддерживается несколько тысяч активных соединений. Следовательно, многочисленные потоки IntServ в канале с большой пропускной способностью значительно увеличивают нагрузку на маршрутизаторы. Более того, каждый раз при изменении топологии все зарезервированные пути необходимо прокладывать заново.

### 2.5. Интегро-дифференцированное обслуживание трафика

Опубликованный в 2000 г. стандарт RFC2998 описывает принципы организации взаимодействия IntServ/RSVP и DiffServ для предоставления QoS из конца в конец. Слабые места одной модели компенсируются соответствующими решениями другой. С одной стороны, плохо масштабируемая IntServ на магистральных участках сети может быть заменена на более простую DiffServ, с другой стороны, с помощью RSVP может решаться (если не полностью, то в большей степени) проблема с неопределенностью получаемого сервиса в "чистой" DiffServ-сети.

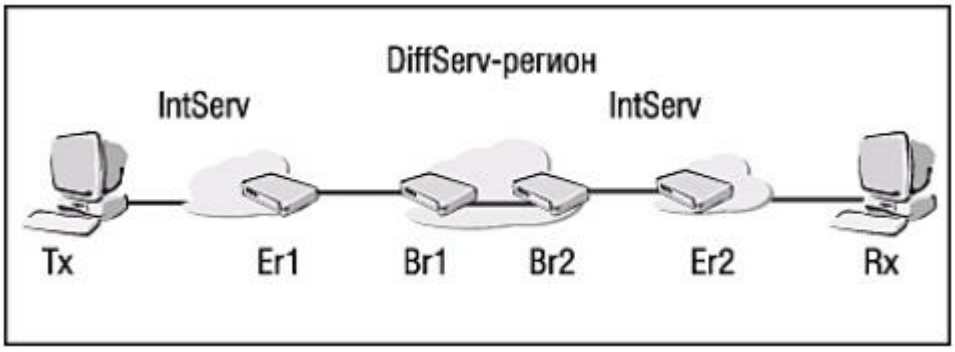


Рис. 3. *Модель DiffServ + IntServ*

Основная проблема при взаимодействии - соответствие ресурсов, запрашиваемых с помощью RSVP и предоставляемых в DiffServ-регионе (так называется непрерывная последовательность DiffServ-доменов, в пределах которых могут предоставляться дифференцированные услуги). Для реализации отображения ресурсов был предложен ряд решений.

Возможна организация двух вариантов взаимодействия протоколов качества обслуживания:

1. DiffServ-регион не поддерживает RSVP-сигнализацию, и ресурсы выделяются на статической основе;
2. обработка RSVP-сообщений производится в DiffServ-регионе.

В первом случае совместная работа основана на статическом соглашении клиента с оператором SLS (спецификация уровня сервиса). В простейшей ситуации оно описывает значение пропускной способности, получаемое трафиком пользователя, в DiffServ-сети. В этом случае (рис. 7.3) Tx (отправитель) генерирует сообщения Path, которые направляются к узлу Rx (получатель) через DiffServ-регион.

При прохождении через DiffServ-регион содержимое RSVP-сообщений игнорируется, и они пересылаются как обычный пакет с данными. При получении узлом Rx сообщения Path генерируется запрос на резервирование RESV, который затем направляется обратно к узлу Tx. В случае успешной обработки запроса каждым RSVP-совместимым маршрутизатором и прохождения через DiffServ-регион сообщение RESV достигает маршрутизатора Er1. Er1 на основании SLS производит сравнение ресурсов, запрашиваемых в сообщении RESV, и ресурсов, доступных в DiffServ-регионе. Если Er1 подтверждает запрос, сообщение RESV отсылается далее по направлению к узлу Tx. В ином случае сообщение отвергается, и узлу Rx отправляется сообщение об ошибке. В полученном узлом Tx сообщении может содержаться информация о маркировании соответствующим кодом пакетов, адресуемых в узел Rx. Значение кода определяется по умолчанию или из сообщения RESV.

Во втором варианте предполагается, что пограничные маршрутизаторы в DiffServ-регионе (например, маршрутизатор Br1) поддерживают протокол RSVP. Отметим, что, несмотря на поддержку RSVP-сигнализации, обрабатываются только агрегированные потоки, а не единичные, как в сети IntServ/RSVP. Порядок обмена RSVP-сообщениями такой же, как и в предыдущем случае. Однако благодаря поддержке RSVP в DiffServ-регионе блок управления доступом является частью DiffServ-сети. В результате маршрутизатор Br1 имеет возможность непосредственно обработать RSVP-запрос, исходя из доступности ресурсов.

По-видимому, совместная работа IntServ и DiffServ является оптимальным вариантом для предоставления требуемого QoS из конца в конец. Реализация такой модели позволит ликвидировать причину низкого качества мультимедийных услуг на основе IP-протокола и повысить производительность традиционных сервисов.

### 2.6. Протокол резервирования ресурсов - RSVP

Одним из средств обеспечения качества IP-телефонии и особенно интернет-телефонии является использование протокола резервирования ресурсов (Resource Reservation Protocol, RSVP), рекомендованного комитетом IETF. С помощью PSVP мультимедиа-программы могут потребовать специального качества обслуживания (specific quality of service - QoS) посредством любого из существующих сетевых протоколов - главным образом IP, хотя возможно использовать и UDP, - чтобы обеспечить качественную передачу видео- и аудиосигналов. Протокол RSVP предусматривает гарантированное QoS благодаря тому, что через каждый компьютер, или узел, который связывает между собой участников телефонного разговора, может передаваться определенное количество данных.

Протокол RSVP предназначен только для резервирования части пропускной способности. Используя RSVP, отправитель периодически

информирует получателя о свободном количестве ресурсов сообщением RSVP Path (рис. 4). Транзитные маршрутизаторы по мере прохождения этого сообщения также анализируют имеющееся у них количество свободных ресурсов и подтверждают его соответствующим сообщением RSVP Resv, передаваемым в обратном направлении. Если ресурсов достаточно, то отправитель начинает передачу. Если ресурсов не достаточно, получатель должен снизить требования или прекратить передачу информации.

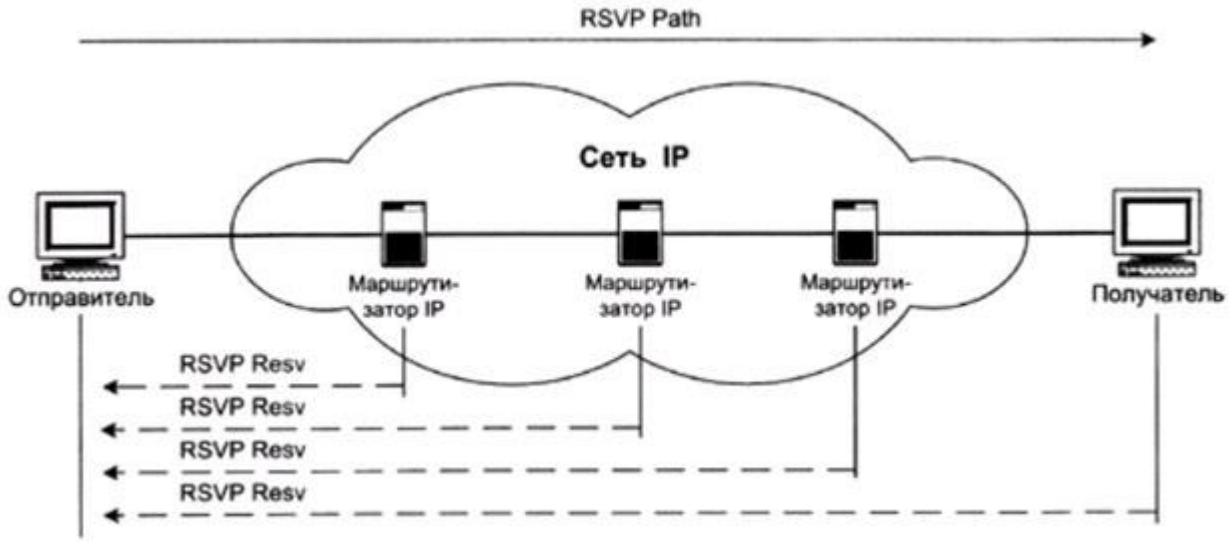


Рис. 4. *Применение протокола RSVP*

RSVP - это протокол сигнализации, который обеспечивает резервирование ресурсов для предоставления в IP-сетях услуг эмуляции выделенных каналов. Протокол позволяет системам запрашивать, например, гарантированную пропускную способность такого канала, предсказуемую задержку, максимальный уровень потерь. Но резервирование выполняется лишь в том случае, если имеются требуемые ресурсы [5].

Одной из особенностей RSVP является то, что запросы на резервирование ресурсов направляются только от получателей данных отправителям, а не наоборот. Такой подход обусловлен тем, что лишь устройство-получатель знает, с какой скоростью оно должно получать данные, чтобы надежно декодировать аудио- или видеосигналы. Другая особенность RSVP - резервирование производится лишь для одного

направления. Кроме того, RSVP не допускает смешения аудио- и видеосигналов на зарезервированном канале.

Когда RSVP-программы закончат сеанс связи, они должны вызвать функцию отмены, предусмотренную этим протоколом. Отмена аннулирует все запросы на ресурсы, сделанные программой, и позволяет другим прикладным программам использовать коммуникационные возможности Интернета. Если программе не удается выполнить отмену, то предусмотренные протоколом средства по истечении некоторого промежутка времени обнаружат это и автоматически отменят запрос на ресурсы.

Недостатком протокола RSVP является то, что полоса пропускания, выделяемая источнику информации, при снижении активности источника не может быть использована для передачи другой информации. Поскольку для реализации QoS протокол RSVP требует резервирования ресурсов или каналов связи, небрежные или безответственные пользователи могут захватить ресурсы сети, инициируя несколько сеансов QoS подряд. Как только канал зарезервирован, он становится недоступным для других пользователей, даже если тот, кто его затребовал, ничего не передает. К сожалению, в RSVP отсутствует четкий механизм предотвращения подобных ситуаций, и решение этой проблемы возлагается на сетевых администраторов. Очевидно, что необходимо предусмотреть более жесткий контроль, чтобы RSVP имел успех.

### 2.7. Технология MPLS

MPLS (Multiprotocol Label Switching) - это технология быстрой коммутации пакетов в многопротокольных сетях, основанная на использовании меток. MPLS разрабатывается и позиционируется как способ построения высокоскоростных IP-магистралей, однако область применения технологии 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.

Архитектура MPLS обеспечивает построение магистральных сетей, имеющих практически неограниченные возможности масштабирования, повышенную скорость обработки трафика и высокую гибкость с точки зрения организации дополнительных сервисов. Кроме того, технология MPLS позволяет интегрировать сети 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 [10].

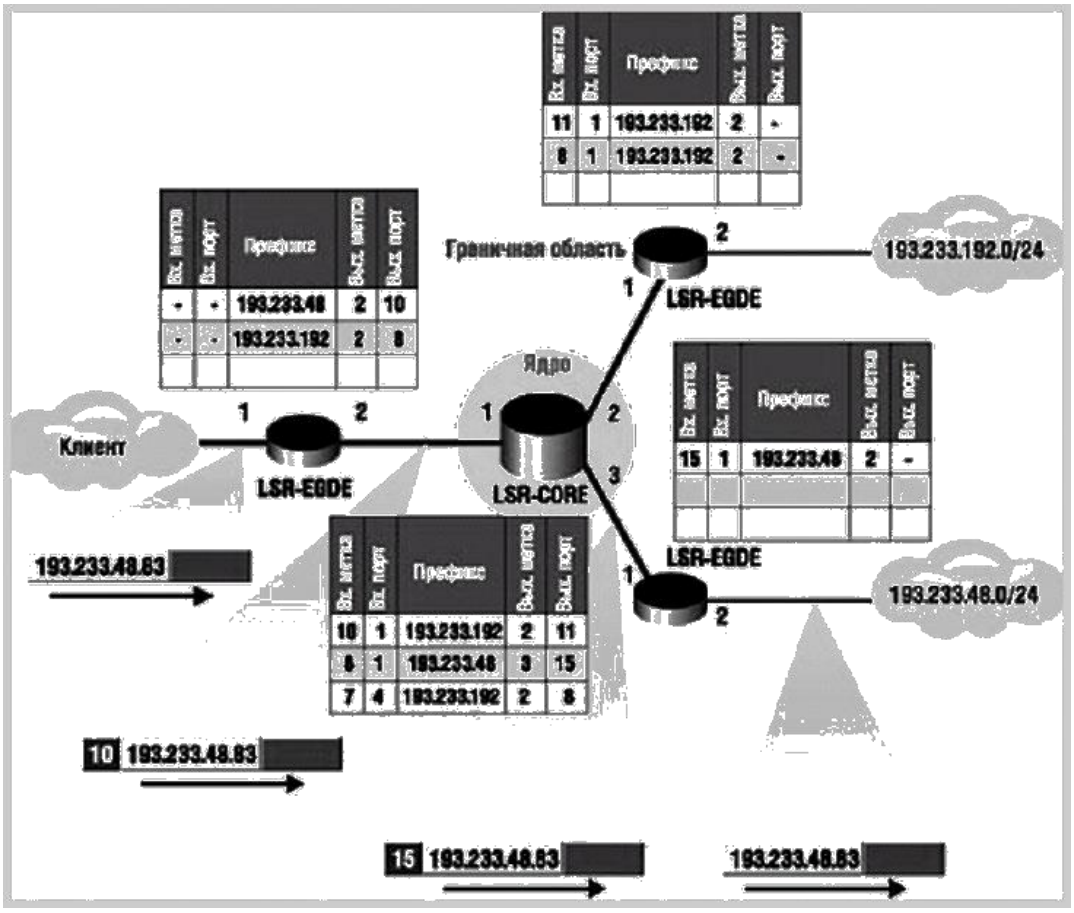


Рис. 5. Схема коммутации MPLS

Принцип коммутации. В основе MPLS лежит принцип обмена меток. Любой передаваемый пакет ассоциируется с тем или иным классом сетевого уровня (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 (LSR). Метка передается в составе любого пакета, причем способ ее привязки к пакету зависит от используемой технологии канального уровня [8].

Маршрутизатор LSR получает топологическую информацию о сети. 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 (LDP), так и модифицированных версий других протоколов сигнализации в сети.

Распределение меток между 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, LSR по номеру интерфейса, на который пришел пакет, и по значению привязанной к пакету метки определяет для него выходной интерфейс. Старое значение метки заменяется новым, содержавшимся в поле "выходная метка" таблицы, и пакет отправляется к следующему устройству на пути 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.

Преимущества технологии MPLS:

- отделение выбора маршрута от анализа IP-адреса (дает возможность предоставлять широкий спектр дополнительных сервисов при сохранении масштабируемости сети);

- ускоренная коммутация (сокращает время поиска в таблицах);
- гибкая поддержка QoS , интегрированных сервисов и виртуальных частных сетей;
- эффективное использование явного маршрута;
- сохранение инвестиций в установленное ATM-оборудование;
- разделение функциональности между ядром и граничной областью сети.

Сеть MPLS подразделяется на две функционально различные области - ядро и граничную область (см. рис. 5). Ядро образуют устройства, минимальным требованием к которым является поддержка MPLS и участие в процессе маршрутизации графика для того протокола, который коммутируется с помощью MPLS. Маршрутизаторы ядра занимаются только коммутацией. Все функции классификации пакетов по различным FEC, а также реализацию таких дополнительных сервисов, как фильтрация, явная маршрутизация, выравнивание нагрузки и управление трафиком, берут на себя граничные LSR. В результате интенсивные вычисления приходятся на граничную область, а высокопроизводительная коммутация выполняется в ядре, что позволяет оптимизировать конфигурацию устройств MPLS в зависимости от их местоположения в сети.

Таким образом, главная особенность 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. Поскольку на установление соответствия пакетов определенным классам FEC могут влиять не только IP-адреса, но и другие параметры, можно реализовать, например, назначение различных LSP пакетам, относящимся к различным потокам RSVP или имеющим разные приоритеты обслуживания. Конечно, подобный сценарий удается

осуществить и в обычных маршрутизируемых сетях, но решение на базе MPLS 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 LSR таких механизмов управления буферизацией и очередями, как WRED, WFQ или CBWFQ, 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.

## 2.8. Сравнение технологий IntServ, DiffServ, MPLS

Так как для обеспечения качества только анализируется поле заголовка пакета IP и не используются никакие вспомогательные протоколы сигнализации, то проблема совместимости оборудования разных производителей неактуальна.

Так как для обеспечения качества только анализируется поле заголовка пакета IP и не используются никакие вспомогательные протоколы сигнализации, то проблема совместимости оборудования разных производителей неактуальна.

Технология DiffServ может использоваться в транзитной сети. Но в условиях однородного трафика, например только голосового, принцип применения приоритетов теряет смысл и сеть начинает работать в режиме Best Effort.

MPLS (многопротокольная коммутация по меткам) предназначена для ускорения коммутации пакетов в транспортных сетях. Основное отличие этой технологии от рассмотренных ранее в том, что MPLS изначально не является технологией обеспечения качества и становится таковой только при использовании протокола RSVP-TE.

| Параметр | IntServ | DiffServ | MPLS |
|---|---|---|---|
| Метод обеспечения QoS | Резервирование | Приоритезация | Перемаршру-тизация |
| Число обслуживаемых классов QoS | 3 | 3 | 0 |
| Перечень задаваемых показателей качества | Полоса пропускания | Скорость передачи трафика | - |
| | Максимальная сетевая задержка | Сетевая задержка | |
| | Джиттер | Коэффициент потери пакетов | |
| Необходимость использования дополнительных протоколов | RSVP | Нет | LDP, CR-LDP, RSVP |
| Требования к производительности маршрутизаторов | Высокие | Низкие | Средние |
| Эффективность масштабирования сети | Невысокая | Высокая | Высокая |
| Совместимость оборудования разных производителей | Средняя | Высокая | Средняя |
| Гарантированность обеспечения качества | Высокая | Средняя | Высокая с использованием RSVP |

На границе сети MPLS маршрутизаторы помечают пакеты специальными метками, определяющими дальнейший маршрут следования пакета к месту назначения. В результате анализируются не адреса IP, а короткие цифровые метки, что существенно снижает сетевую задержку и

требования к производительности маршрутизаторов. Для корректного взаимодействия их между собой и обмена информацией о создаваемых метках используются протоколы распределения меток (LDP, CR-LDP, RSVP-TE и др.).

Маршрут может также задаваться административно. В этом случае заранее определяется весь перечень узлов, через которые он будет проходить. Если для соединения требуется гарантия определенного уровня качества, то для распределения меток применяется протокол RSVP-TE, и на маршруте резервируются необходимые ресурсы. В RSVP-TE предусмотрены контроль и обновление установленного соединения, так что в случае повреждения в сети можно динамически перевести потоки трафика на резервный маршрут.

Технология MPLS характеризуется высокой масштабируемостью и рассматривается в качестве наиболее перспективной для передачи трафика IP. Она стандартизована IETF, поэтому, как и в случае с IntServ, при отклонении от спецификаций могут возникнуть проблемы с совместимостью оборудования разных производителей.

## 2.9. Обслуживание очередей

Алгоритмы обслуживания очередей позволяют предоставлять разный уровень QoS трафику разных классов. Обычно используется несколько очередей, каждая из которых занимается пакетами с определенным приоритетом. Требуется, чтобы высокоприоритетный трафик обрабатывался с минимальной задержкой, но при этом не занимал всю полосу пропускания, и чтобы трафик каждого из остальных типов обрабатывался в соответствии с его приоритетом.

Обслуживание очередей включает в себя алгоритмы:

- организации очереди;
- обработки очередей.

***Алгоритмы организации очереди.*** Существует два основных алгоритма организации очереди: Tail Drop и Random Early Detection.

Алгоритм Tail Drop. Tail drops - отсечения конца очереди. Задается максимальный размер очереди (в пакетах или в байтах). Когда очередь полна, ни один вновь поступивший пакет туда уже не помещается и потому отбрасывается. Такое управление очередью приводит к повторной синхронизации параметров соединения. После синхронизации TCP сразу посылает столько пакетов, сколько допускает размер окна подтверждения. Подобный всплеск нагрузки опять приводит к отсечению конца очереди, что опять порождает необходимость повторной синхронизации [5,7].

Чтобы избежать возникновения заторов, на маршрутизаторах зачастую организуются очереди большого размера. К сожалению, несмотря на то что увеличение размеров очереди благоприятно сказывается на пропускной способности, большие очереди могут приводить к увеличению времени задержки, что становится причиной нестабильного поведения TCP-соединений.

Алгоритм Random Early Detection (RED). RED позволяет более "справедливо" разделить канал между TCP-соединениями. Он позволяет контролировать нагрузку с помощью выборочного случайного уничтожения некоторых пакетов до того, как очередь будет заполнена полностью и протоколы, подобные TCP, начнут снижать скорость передачи, а также предотвращает повторную синхронизацию. Кроме того, выборочная "потеря" пакетов помогает TCP быстрее найти подходящую скорость передачи данных и удерживать размер очереди и время задержки на разумном уровне. Вероятность "потери" пакета конкретного соединения прямо пропорциональна пропускной способности, используемой этим соединением, а не числу пакетов, т. е. большие пакеты уничтожаются чаще маленьких, что дает достаточно справедливое распределение полосы пропускания.

При работе с RED пользователю необходимо определиться со значениями трех параметров: минимум (min), максимум (max) и превышение (burst). Минимум - это минимальный размер очереди в байтах, выше которого начнется выборочная потеря пакетов. Максимум - это "мягкий"

максимум, алгоритм будет пытаться удержать размер очереди ниже этого предела. Превышение - максимальное число пакетов, которые могут быть приняты в очередь сверх установленного максимального предела.

Минимальный размер очереди рассчитывается, исходя из максимально допустимого времени задержки в очереди и пропускной способности канала. Если установить минимальный предел слишком маленьким, это приведет к снижению пропускной способности, слишком большим - к увеличению времени задержки.

Максимальный размер очереди нужно задавать по меньшей мере в два раза больше минимального, чтобы снизить вероятность повторной синхронизации. На медленных линиях, с небольшим минимальным пределом размера очереди, максимальный предел следует задавать в четыре, а иногда и более раз больше минимального.

Предел превышения отвечает за поведение RED на пиковых нагрузках. Кроме того, необходимо будет определиться с предельным размером очереди (limit) и средним размером пакета (avpkt). Когда очередь достигает предельного размера, RED переходит к алгоритму "отсечения конца".

При малых размерах очередей метод RED более эффективен, чем другие методы. Он также более устойчив к трафику, имеющему "взрывной" характер.

***Алгоритмы обработки очередей.*** Стратегия FlFO. Алгоритм обслуживания очередей First-In-First-Out (FIFO), также называемый First Come First Served, является самым простым. Пакеты обслуживаются в порядке поступления без какой-либо специальной обработки.

Такая схема приемлема, если исходящий канал имеет достаточно большую свободную полосу пропускания. Алгоритм FIFO относится к так называемым неравноправным схемам обслуживания очередей, так как при его использовании одни потоки могут доминировать над другими и захватывать несправедливо большую часть полосы пропускания. В связи с этим применяются равноправные схемы обслуживания, предусматривающие

выделение каждому потоку отдельного буфера и равномерное разделение полосы пропускания между разными очередями.

Очередь с приоритетами. Очередь с приоритетами (Priority Queuing) - это алгоритм, при котором несколько очередей FIFO (могут использоваться алгоритмы Tail Drop, RED и т. д.) образуют одну систему очередей.

При приоритетной организации очередей (PQ) важный трафик получает самую быструю обработку в каждом пункте, в котором она используется. Этот метод назначает строгий приоритет важного трафика и может обеспечить гибкое задание уровня приоритета в соответствии с сетевыми протоколами. При приоритетной организации очереди каждый пакет помещается в одну из четырех очередей - с высоким, средним и низким приоритетом ожидания - на основе присвоенного приоритета. Назначение разным потокам нескольких разных приоритетов производится по ряду признаков, таких как источник и адресат пакета, транспортный протокол, номер порта. Пакеты, которые не подверглись классификации этим механизмом занесения в список приоритетов, по умолчанию направляются в нормальную очередь. Во время передачи этот алгоритм предоставляет очередям с более высоким уровнем приоритета преференциальный режим по сравнению с очередями с низким уровнем приоритета.

Class-Based Queuing (CBQ). Классовые дисциплины широко используются в случаях, когда различные виды трафика необходимо обрабатывать по-разному. Примером классовой дисциплины может служить CBQ.

Когда трафик передается на обработку классовой дисциплине, он должен быть отнесен к одному из классов (классифицирован). Определение принадлежности пакета к тому или иному классу выполняется фильтрами [7].

Фильтры, присоединенные к дисциплине, возвращают результат классификации (класс пакета), после чего пакет передается в очередь, соответствующую заданному классу. Каждый из классов в свою очередь может состоять из подклассов и иметь свой набор фильтров для выполнения

более точной классификации свой доли трафика. В противном случае пакет обслуживается дисциплиной очереди класса.

Кроме того, в большинстве случаев классовые дисциплины выполняют шейпинг (формирование) трафика, с целью переупорядочивания пакетов и управления скоростью их передачи. Это совершенно необходимо в случае перенаправления трафика с высокоскоростного интерфейса (например, Ethernet) на медленный (например, модем).

Это позволяет различным приложениям совместно использовать одну и ту же сеть, причем каждое из них предъявляет свои специфические минимальные требования к ширине полосы или к задержке.

Взвешенные очереди. Для резервирования полосы пропускания в сети IP может использоваться метод WFQ (Weighted Fair Queuing). Метод WFQ позволяет для каждого вида трафика выделять определенную часть полосы пропускания. Оператор через систему административного управления может задать количество очередей. В случае если одна очередь не использует полностью выделенную ей полосу пропускания, то свободный резерв полосы пропускания может задействоваться для передачи информации из следующей очереди.

Стратегия справедливых (взвешенных) очередей WFQ используется по умолчанию для интерфейсов низкого быстродействия. WFQ делит трафик на несколько потоков, используя в качестве параметров (для IP-протокола) IP-адреса и порты получателя и отправителя, а также поле IP-заголовка ToS (Type of Service). Значение ToS служит для квалификации части выделяемой полосы потока. Для каждого из потоков формируется своя очередь. Максимально возможное число очередей равно 256. Очереди обслуживаются в соответствии с карусельным принципом (round-robin). Более высокий приоритет имеют потоки с меньшей полосой, например, Telnet. По умолчанию каждая из очередей имеет емкость 64 пакета (но допускается значение и менее 4096 пакетов).

В сетях существует 8 уровней приоритета. Следует иметь в виду, что WFQ не поддерживается в случае туннелирования или шифрования. Поток с низким весом получает более высокий уровень обслуживания, чем поток с высоким уровнем. Когда задействованы биты ToS, WFQ реализует приоритетное обслуживание пакетов согласно значению этого кода. Весовой фактор обратно пропорционален уровню приоритета.

Справедливые очереди, базирующиеся на классах (CBWFQ). Дальнейшим развитием технологии WFQ является формирование классов потоков, задаваемых пользователем. Алгоритм CBWFQ предоставляет механизм управления перегрузкой. Параметры, которые характеризуют класс, те же, что и в случае WFQ (только вместо ToS используется приоритет). В отличие от WFQ здесь можно в широких пределах перераспределять полосу пропускания между потоками. Для выделения класса могут привлекаться ACL (Access Control List) или даже номер входного интерфейса. Каждому классу ставится в соответствие очередь. В отличие от RSVP данный алгоритм гарантирует полосу лишь в условиях перегрузки. Всего может быть определено 64 класса. Нераспределенная полоса может использоваться потоками согласно их приоритетам.

Очереди с малой задержкой (LLQ). В некоторых случаях, например, в случае VoIP, важнее обеспечить малую задержку, а не широкую полосу пропускания. Для таких задач разработан алгоритм LLQ (Low Latancy Queuing), который является модификацией CBWFQ. В этом алгоритме пакеты всех приоритетов, кроме наивысшего, вынуждены ждать, пока очередь более высокого приоритета будет опустошена. Разброс задержки в высокоприоритетном потоке может быть связан только с ожиданием завершения передачи пакета низкого приоритета, начавшейся до прихода приоритетного кадра. Такой разброс определяется диапазоном длин кадров.

Как работают маршрутизаторы?

В маршрутизаторе, реализующем архитектуру с интеграцией услуг IETF, алгоритмы обслуживания очередей сортируют трафик в таком порядке,

чтобы данные гарантии были выполнены. Часто маршрутизаторы, не поддерживающие QoS, реализуют подобные алгоритмы в целях управления трафиком. FIFO - первым пришел, первым ушел

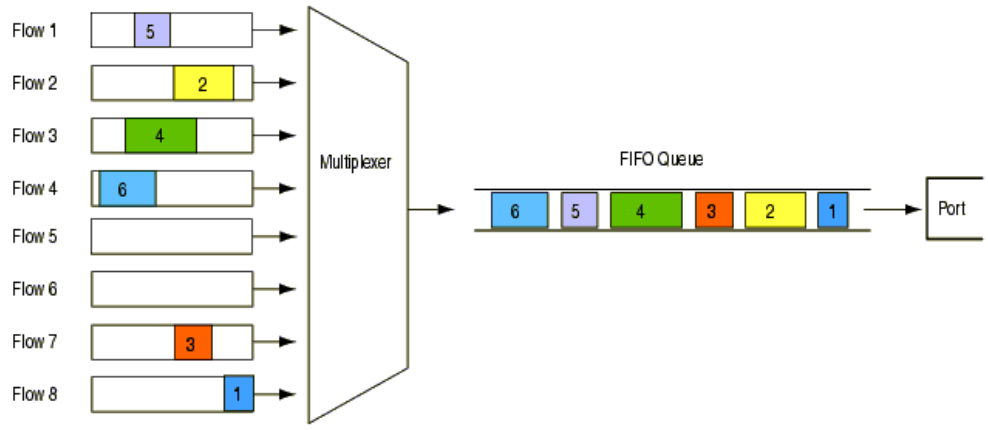


Figure 2.2.1

Стандартные реализации очереди FIFO первыми отправляют наиболее раннее из полученных сообщений и отбрасывают все последующие, если очередь уже полна. Недавние исследования показывают, что удаление сообщений, по крайней мере для TCP/IP, имеет серьезные побочные эффекты. Например, когда сообщение потеряно, приложение-отправитель может рассматривать это как сигнал о том, что оно посылает пакеты слишком быстро. TCP реагирует на такой сигнал замедлением отправки сообщений. Но когда очередь полна, то часто несколько сообщений отбрасываются друг за другом - в результате целый ряд приложений решает замедлить передачу. После этого приложения зондируют сеть для определения ее загруженности и буквально через несколько секунд возобновляют передачу с прежним темпом, что опять приводит к перегрузке.

Случайное раннее обнаружение (Random Early Detection, RED) представляет альтернативу очередям FIFO. Оно позволяет смягчить эффект от потери трафика даже при очень больших нагрузках, так что приложения не синхронизированы друг с другом, как это имело место в предыдущем случае. Такая очередь по-прежнему использует принцип FIFO, но, вместо того чтобы отбрасывать сообщения из конца очереди, RED отбрасывает трафик

статистически, когда средняя длина очереди за данный промежуток времени превосходит некоторое значение. Таким образом, заполнение очереди оптимизировано для обеспечения большей устойчивости алгоритма. Этот процесс был придуман специально для TCP, но те, кто его изобрел, считают, что он применим к любому трафику, когда сеть не гарантирует доставки.

Очередь с приоритетами - это алгоритм, при котором несколько очередей FIFO или RED образуют одну систему очередей. Трафик распределяется между данными очередями в соответствии с некоторыми заданными критериями, например в соответствии с приложением или получателем. Однако трафик отправляется в порядке строгой очередности: сначала трафик с высоким приоритетом, затем со средним и т. д. При всей простоте понимания и реализации этот алгоритм не очень хорошо работает при высоких нагрузках, потому что очереди с низким приоритетом оказываются блокированными в течение продолжительного периода времени или низкоприоритетный трафик имеет такую большую задержку в результате следования по окружному пути, что становится бесполезным.

Очереди в соответствии с классом (Class-Based Queuing, CBQ) - это алгоритм, при котором трафик делится на несколько классов. Определение класса трафика в значительной мере произвольно. Класс может представлять весь трафик через данный интерфейс, трафик определенных приложений, трафик к заданному подмножеству получателей, трафик с качеством услуг, гарантированным RSVP. Каждый класс имеет собственную очередь, и ему гарантируется, по крайней мере, некоторая доля пропускной способности канала. Если какой-либо класс не исчерпывает предоставленный ему лимит пропускной способности, то остальные классы увеличивают свою долю пропорциональным образом.

Взвешенная справедливая очередь (Weighted Fair Queuing, WFQ) является частным случаем CBQ, когда отдельному классу соответствуют независимые потоки. Как и в случае CBQ, каждому классу WFQ соответствует одна очередь FIFO и гарантируется некоторая часть

пропускной способности канала. Если некоторые потоки используют предоставленную им пропускную способность не полностью, то другие потоки увеличивают свою долю соответственно. Так как каждый класс - это отдельный поток, то гарантия пропускной способности эквивалентна в данном случае гарантии максимальной задержки. Зная параметры сообщения, вы можете по известной формуле вычислить его максимальную задержку при передаче по сети. Выделение дополнительной пропускной способности позволяет уменьшить максимальную задержку.

Входные и выходные драйверы - это программы и чипы для приема и отправки сообщений из системы. Вообще говоря, они могут рассматриваться естественным образом в рамках протоколов сетевого уровня. Однако протоколы маршрутизации должны учитывать топологические соображения. По этой причине они рассматривают классы компонентов канального уровня по-иному. Обычно компоненты канального уровня характеризуются такими терминами, как локальные сети, каналы точка-точка, сети множественного доступа с виртуальными соединениями, каналы нерегулярного доступа и коммутируемые каналы.

Локальная сеть, вероятно, наиболее известный для сообщества Internet компонент канального уровня. Примерами могут служить сети Ethernet, Token Ring, FDDI и (несколько парадоксально) Switched Multimegabit Data Service. Предназначение локальных сетей не в обеспечении высокой загруженности, а в обеспечении высокой доступности; в результате, когда локальная сеть загружена, ее производительность менее предсказуема и далека от оптимальной. Локальную сеть можно реализовать, используя различные комбинации кабеля, концентраторов и коммутаторов. Но системы в них - как хосты, так и маршрутизаторы - имеют целый ряд общих характеристик. Если вы не занимаетесь написанием драйверов, то тогда отношение к локальной сети как средству предоставления высокодоступных сервисов некоторому множеству систем с заданной скоростью, вполне достаточно.

Каждая система имеет MAC-адрес, идентифицирующий систему в пределах данной сети. Когда какая-либо система отправляет сообщение, адрес сетевого уровня системы-получателя должен быть переведен сначала в MAC-адрес. Как это делается, зависит от протокола: в NetWare MAC-адрес является частью адреса сетевого уровня, в то время как в AppleTalk и IP протокол определения адреса запрашивает системы об их адресах для установления соответствия между адресами канального и сетевого уровня.

Ввиду необходимости такой трансляции каждой системе в локальной сети необходим уникальный адрес сетевого уровня, благодаря которому сообщение может быть доставлено ей по сети; адрес должен содержать достаточную топологическую информацию (обычно в виде номера сети или префикса адреса), чтобы маршрутизаторы знали, куда направлять сообщение. Подобная система идентификации позволяет последнему маршрутизатору передать сообщение непосредственно системе-получателю.

Организация очередей в локальных сетях сопряжена с определенными трудностями, так как системы не знают о поведении своих соседей. Протоколы локальных сетей имеют механизмы, с помощью которых системы могут договариваться об использовании среды передачи для каждого конкретного сообщения. Это согласование осуществляется обычно посредством обнаружения коллизий или передачи маркера. Такой процесс отнимает иногда немало времени, однако ввиду высокой пропускной способности длинные очереди для локальной сети не характерны.

Каналы точка-точка, например PPP или HSSI, представляют полную противоположность локальным сетям, поскольку здесь мы имеем дело только с двумя участниками. Некоторые архитектуры маршрутизации рассматривают их как внутренние интерфейсы между двумя половинками маршрутизатора, в то время как другие - как вырожденный случай локальной сети.

Такие каналы обычно не имеют адресов, потому что маршрутизаторы с обоих концов могут идентифицировать друг друга непосредственно, не

беспокоясь о формальном имени. Данная конфигурация имеет определенные достоинства при распределении адресов: нет нужды присваивать каналу номер сети. Кроме того, преобразование адресов производить тоже не надо.

В конфигурации точка-точка очередь, кроме того, проще организовать, так как незачем договариваться об использовании канала. Таким образом, система полностью контролирует характеристики трафика.

# 3. Безопасность жизнедеятельности на предприятиях связи в чрезвычайных ситуациях

## 3.1. Чрезвычайные ситуации и их классификация

Экология и безопасность жизнедеятельности — это дисциплина, рассматривающая вопросы о сохранении здоровья и безопасности человека в среде обитания [11].

Чрезвычайная ситуация — это состояние, при котором в результате возникновения источника ЧС на объекте, определенной территории или акватории нарушаются нормальные условия жизни и деятельности людей, возникает угроза их жизни и здоровью, наносится ущерб имуществу населения, народному хозяйству и природной среде.

Под источником чрезвычайных ситуаций понимают опасное природное явление, аварию или опасное техногенное происшествие, широко распространенные инфекционные болезни людей, сельскохозяйственных животных и растений, а также применение современных средств поражения в результате чего происходит или может произойти ЧС.

Все чрезвычайные ситуации (ЧС) классифицируются как конфликтные и бесконфликтные, характеризующиеся скоростью и масштабами распространения

К конфликтным ситуациям относятся военные столкновения, экономические кризисы, социальные взрывы, национальные и религиозные конфликты, разгул уголовной преступности, террористические акты и др.

К бесконфликтным ЧС относятся техногенные, экологические и природные явления, вызывающие ЧС.

По скорости распространения все ЧС делятся на внезапно возникшие, быстро, умеренно и медленно распространяющиеся.

По масштабам распространения все ЧС делятся на локальные, местные, территориальные, региональные, федеральные и трансграничные.

К локальным относятся ЧС, в результате которых пострадало не более 10 человек, либо нарушены условия жизнедеятельности не более 100 человек,

либо материальный ущерб составляет не более 1 тыс. МРОТ на день возникновения ЧС и зона ЧС не выходит за пределы территории объекта производственного или социального значения.

**ЧС техногенного характера.** ЧС техногенного характера — это ситуации, которые возникают в результате производственных аварий и катастроф на объектах, транспортных магистралях и продуктопроводах; пожаров, взрывов на объектах; загрязнения местности и атмосферы сильнодействующими ядовитыми веществами (СДЯВ), отравляющими веществами (ОВ), биологически (бактериологически) опасными и радиоактивными веществами.

Аварии и катастрофы на объектах характеризуются внезапным обрушением зданий, сооружений, авариями на энергетических сетях (ТЭЦ, АЭС, ЛЭП и др.), авариями в коммунальном жизнеобеспечении, авариями на очистных сооружениях, технологических линиях и т. д. Все эти аварии могут сопровождаться выбросами в окружающую среду, в атмосферу СДЯВ, ОВ, биологически вредных и радиоактивных веществ [11].

**ЧС природного характера.** К ЧС природного характера относятся: гидрометеорологические (тайфуны, наводнения, смерчи, нагоны морской воды, вызывающие наводнения, пылевые бури, засухи, ливневые дожди, град, гололед, обледенение, стихийные пожары, морские бури, ураганы, сильные морозы, сильная жара, сильные туманы); гидрогеоморфологические (лавины, сели, оползни, карст) и эндогенные (землетрясения, вулканизм, цунами) явления.

**ЧС экологического характера.** К ЧС экологического характера относится изменения состояния почв, недр Земли, ландшафтов, состояния атмосферы, гидросферы, биосферы. Все эти ЧС происходят в результате техногенных и природных чрезвычайных ситуаций.

***Стихийные бедствия***. К стихийным бедствиям относятся природные явления или процессы геофизического, геологического, атмосферного, биосферного и другого происхождения такого масштаба, которые вызывают

катастрофические ситуации, характеризующиеся внезапным нарушением безопасности жизнедеятельности населения, разрушением и уничтожением материальных ценностей, поражением или гибелью людей. Стихийные бедствия могут быть причиной аварий и катастроф. К стихийным бедствиям следует отнести: землетрясения, наводнения, бури, ураганы, снежные заносы, обледенения, селевые потоки, оползни, пожары, извержения вулканов, длительные засухи, ливневые дожди и т. д.

Опасность селей заключается не только в их разрушительной силе, но и во внезапности появления.

По составу переносимого твердого материала селевые потоки могут быть грязевыми — смесь воды с мелкоземом при небольшой концентрации камней, грязекаменными — смесь воды, гальки, гравия, небольших камней и водокаменными — смесь воды с преимущественно крупными камнями. Скорость селевого потока составляет 2,5–4,0 м/с, а при прорыве заторов на реках достигает 8,0–10 м/с. С течением времени скорость селевого потока увеличивается с увеличением объемного веса.

Способы борьбы с селевыми потоками:

- возведение плотин для задержки твердого стока и пропуска воды с мелкими фракциями пород и подпорных стенок для укрепления откосов;
- создание каскадов запруд для разрушения селевого потока и освобождения его от твердого материала и горных стокоперехватывающих и водосборных канав для отвода стоков в ближайшие водотоки, водоемы и т. д.

Точных методов прогнозирования возникновения селевых потоков нет, но для опасных селевых районов установлены критерии, позволяющие оценивать вероятность их возникновения. С этой целью определяются критические сумма осадков в течении 1–3 суток и температура за 10–15 суток для ледников или сумма этих показателей, по которым и прогнозируют возможность возникновения селевого потока.

***Аварии и катастрофы.*** Авария — это непреднамеренный выход из строя машин, механизмов, устройств, коммуникаций, линий связи, продуктопроводов вследствие нарушения технологии производства, правил эксплуатации, мер безопасности, ошибок, допущенных при проектировании, строительстве, изготовлении, низкой трудовой дисциплины и, как следствие стихийных бедствий.

Наиболее характерными авариями являются взрывы, пожары, заражения атмосферы и местности химическими, биологическими (бактериальными) и радиоактивными веществами.

Катастрофы — это внезапные бедствия, аварии, влекущие за собой разрушения зданий, сооружений, уничтожение материальных ценностей, сопровождаемые массовой гибелью людей и животных.

Пожары на предприятиях могут возникать в результате повреждения электропроводки и электрооборудования, находящегося под током, повреждения отопительных систем, емкостей с легковоспламеняющимися жидкостями и в результате нарушений техники безопасности. На характер и масштаб пожаров существенное влияние оказывают огнестойкость зданий и сооружений, пожарная опасность объектов, плотность застройки на территории, метеорологические условия, состояние систем и средств пожарной сигнализации и пожаротушения.

Аварии с истечением (выбросом) химически опасных веществ и, вследствие этого, загрязнения окружающей среды, могут происходить на предприятиях химической, нефтеперерабатывающей, целлюлозно-бумажной, масломолочной и пищевой промышленности, водопроводных и очистных сооружениях, а также при транспортировке вредных веществ. Так, в 1984 г. произошла утечка 40 т метализоциата с химического завода в Бхполе (Индия), где погибло 2,5 тыс. человек, и около 180 тыс. получили отравления разных степеней.

Могут происходить аварии на железнодорожном транспорте при перевозках взрывчатых веществ. Так, в 1986 г. на станции Арзамас

произошел взрыв двух вагонов с взрывчаткой. В результате взрыва погибло 88 человек, и свыше 200 человек получили ранения.

Наиболее опасными по масштабам своего действия являются аварии на атомных электростанциях (АЭС) и ядерных реакторах с выбросом в атмосферу радиоактивных веществ, что ведет к длительному радиоактивному загрязнению местности на огромных территориях. В результате аварии на ЧАЭС (1986) большое количество людей получили радиационные поражения различной степени тяжести, 200 тыс. человек были эвакуированы из зоны заражения, площадь радиоактивного загрязнения охватила 11 областей с населением в 17 млн человек.

Биологическое (бактериологическое) заражение вызывает различные эпидемические заболевания: холера, чума, сибирская язва, сап и др. Такие заражения могут вызываться нарушениями безопасности на биологических предприятиях, нарушениями работы санитарно-эпидемической службы, размываниями старых чумных, холерных захоронений при разливах рек, строительстве, переносе болезнетворных микроорганизмов грызунами, насекомыми и т. д.

### 3.2. Чрезвычайные ситуации как результат конфликтных событий

Чрезвычайные ситуации возникают в результате военных действий, межнациональных, религиозных конфликтов, в случаях диверсионных актов и т. д.

История войн говорит о том, что в военных конфликтах в основном страдает мирное население, и чем совершеннее становятся средства поражения, тем больше гибнет мирных граждан. Так, в первую мировую войну потери среди мирного населения составили 5 % от всех потерь, во вторую мировую войну — уже 48 %, война в Корее унесла жизнь 84 % мирных жителей, а во Вьетнаме — 90 %.

В современных условиях могут быть использованы:

- оружие массового поражения (ядерное, химическое, бактериологическое);
- обычные средства поражения (артиллерийское, ракетное, стрелковое, авиационное);
- современные средства поражения.

*Современные средства поражения*. В результате научно-технической революции произошло накопление новых знаний, развитие фундаментальных наук. Открытия во многих областях науки и техники привели к созданию новых систем, направленных не только на благо человека, но и против него. В результате появились новые виды оружия; лучевое, радиочастотное, инфразвуковое, радиологическое, геофизическое.

## Заключение

В работе обсуждены тема, связанная с качеством обслуживания в IP-сетях. Указываются определения, описаны методики определения качества в IP-сетях. Рассмотрено протоколы, с помощью которых реализуется уровень качественного обслуживания. Приведено сравнение различных технологий обеспечения качества IP-услуг. Вводится понятие очередей и "алгоритмов борьбы" с ними.

Выполнены следующие задачи исследования: обзор проблемы IP-телефонии и методы их решения; исследования методики определения качества в IP-сетях; сравнение различных технологий обеспечения качества IP-услуг; исследование понятие очередей.

Алгоритмы обслуживания очередей позволяют предоставлять разный уровень QoS трафику разных классов. Обычно используется несколько очередей, каждая из которых занимается пакетами с определенным приоритетом. Требуется, чтобы высокоприоритетный трафик обрабатывался с минимальной задержкой, но при этом не занимал всю полосу пропускания, и чтобы трафик каждого из остальных типов обрабатывался в соответствии с его приоритетом.

Сети с коммутацией пакетов на основе протокола IP не обеспечивают гарантированной пропускной способности, поскольку не гарантируют доставку. Для приложений, где не важен порядок и интервал прихода пакетов, время задержек между отдельными пакетами не имеет решающего значения. IP-телефония является одной из областей передачи данных, где важен порядок прихода пакетов и важна динамика передачи сигнала, которая обеспечивается современными методами кодирования и передачи информации.

Вместе с тем необходимо обеспечить механизмы, по которым в периоды перегрузки пакеты с информацией, чувствительной к задержкам, не

будут простаивать в очередях или получат более высокий приоритет, чем пакеты с информацией, не чувствительной к задержкам. Для этой цели в сети должны быть реализованы механизмы, гарантирующие нужное качество обслуживания.

## Литература


1. Ислам Каримов. О мерах по дальнейшему совершенствованию процедур, связанных с осуществлением предпринимательской деятельности и предоставлением государственных услуг. Ташкент, 15 апреля 2014 года. http://www.press-service.uz/ru/news/4943/
2. Постановления Президента Республики Узбекистан принятие ПП №1730 от 21 марта 2012 года «О мерах по дальнейшему внедрению и развитию современных информационно-коммуникационных технологий». http://lex.uz/ru/online
3. Бакланов И.Г. ISDN и IP-телефония / Вестник связи, 1999, №4.
4. Фокин В.Г. Управление телекоммуникационными сетями: Учеб.пособие. – Новосибирск.: СибГУТИ, 2011. -110.
5. Крук Б.И., Полантонопуло В.Н., Шувалов В.П. Телекоммуникационные системы и сети. Учеб.пособие. – Изд. 3-е, испр. И доп. –М.:Горячая линия – Телеком, 2003. -647 с.:ил.
6. Гейер Дж. - Беспроводные сети. Первый шаг, 2004г.
7. Бройдо В.Л. Вычислительные системы, сети и телекоммуникации: Учебник для вузов. 2-е изд. - СПб.: Питер, 2006 - 703 с.
8. Крухмалев В. В., Гордиенко В. Н., Мочанов А. Д. и др. Основы построение телекоммуникационных систем и сетей: 0-75. Учебник для вузов. .- М.: Радио и связь, 1998.
9. Васильев И. И., Птичников М. М. Измерение в цифровых сетях связи. М.: Пастмеркет, 2004.
10. Гольдштейн Б.С., Пинчук А.В., Суховицкий А.Л. IP-телефония. – М.:Радио и связь, 2001.
11. Кукин П.П., Лапин В.Л., Подгорных Е.А. Безопасность жизнедеятельности. Безопасность технологических процессов и производств: Учебное пособие для вузов/. – М. Высш. шк., 1999.
12. www.aci.uz

13.http://lib.tuit.uz

14.www.bookfi.org