Министерство образования и науки Российской Федерации
Московский Государственный институт электроники и математики
(технический университет)

Кафедра «Вычислительные системы и сети» (ВСиС)

Отчет

по преддипломной практике

Выполнение:
Никитин А. А.

Руководитель:
Панфилов П. Б.

Группа: С-112

МОСКВА 2004

Содержание

1. Введение

На современных российских коммерческих предприятиях все чаще и чаще возникает задача передачи по локальной вычислительной сети мультимедийного трафика, например, IP-телефонии или цифрового видео. Специфика таких информационных потоков заключается в том, что они требуют от среды передачи данных соблюдения жестких правил качества обслуживания, от которого, в свою очередь, зависит качество звукового сигнала или видеосигнала. Нередко решение этой непростой задачи влечет за собой полную реорганизацию всей вычислительной сети предприятия с закупкой дорогостоящего оборудования. Аналитический расчет параметров узлов и каналов проектируемой сети, обеспечивающей качественную передачу мультимедиа-информации чрезвычайно сложен, а в некоторых случаях — и вовсе невозможен.

В связи с этим актуальной становится разработка программных средств имитационного моделирования локальных вычислительных сетей с учетом особенностей мультимедийного трафика, задача которых — повысить эффективность вложений в модернизацию локальной вычислительной сети. Такие программные средства позволят произвести оценку загруженности каналов проектируемыми информационными потоками, в том числе и мультимедийными потоками группового вещания (multicast), выявить «узкие места» в телекоммуникационной структуре, а также визуализировать результаты имитационного моделирования для дальнейшего анализа.

2. Технологии обеспечения QoS в сетях IP/Ethernet

Качество обслуживания (QoS) — это способность сетевых средств обеспечить требуемый сервис для определенных классов трафика в различных сетевых средах, включая ретрансляцию кадров (Frame Relay), режим асинхронной передачи (Asynchronous Transfer Mode, ATM), Ethernet, сети 802.1, SONET, а также в IP-сетях, которые могут использовать любую из вышеперечисленных технологий. Под классом трафика здесь подразумевается тип транспортируемых данных: голосовые пакеты, видео, HTTP/FTP, трафик баз данных и т. д.

Основное назначение QoS-технологий состоит в том, чтобы обеспечить гарантированное соблюдение следующих параметров:

- приоритет;
- необходимую полосу пропускания;
- контролируемую задержку;
- контролируемую вариацию задержки — jitter (это требование связано с передачей интерактивного трафика и работой некоторых приложений реального времени);
- минимальный процент потерь пакетов при передаче.

Кроме того, важно обеспечить приоритетность обслуживания для одного или нескольких потоков с одновременной возможностью передачи других потоков.

Технологии QoS включают широкий спектр инструментальных средств, которые, при правильном их применении, могут значительно повысить эффективность использования существующей полосы пропускания и избавить от необходимости ее расширения (а значит,

и от дополнительных расходов), причем не только в территориально распределенных сетях (WAN) и сетях ISP, но и в небольших корпоративных сетях.

Основные преимущества, обеспечиваемые механизмом QoS:

- **Контроль и более эффективное использование сетевых ресурсов**. Имея широкие возможности контроля и управления ресурсами, можно, например, в качестве приоритетного выбрать трафик баз данных и ограничить пропускную способность для трафика FTP. При помощи специального программного обеспечения можно определить, какой поток занимает большую часть полосы пропускания и где возникают заторы.
- **Специализированные услуги**. Высокий уровень контроля и надежность, обеспечиваемые QoS, позволяют ISP предлагать своим клиентам специализированные дифференцированные услуги.
- **Сосуществование критически важных приложений**. QoS-технологии позволяют эффективно регулировать использование полосы пропускания, что особенно актуально при наличии критически важного трафика. Так, например, они гарантируют выделение необходимой полосы пропускания мультимедийным и голосовым приложениям, соответствующим образом уменьшая задержки. В то же время данное соединение может использоваться и другими приложениями, которые будут обслуживаться по своей схеме, не влияя на критически важный трафик.
- **Основа для построения интегрированной сети**. Внедрение QoS-технологий в действующие сети — это первый шаг на пути к созданию интегрированных мультимедийных сетей, которые в недалеком будущем станут фундаментом для любых коммуникаций.

Такие технологии, как ATM или Frame Relay, изначально предусматривают использование механизмов QoS, поэтому органы стандартизации больше внимания уделяют IP, Ethernet и другим технологиям, требующим поддержки качества сервиса. В данной области IETF разрабатывает два направления: *Differential Services (DiffServ)* и *Multiprotocol Label Switching (MPLS)*. Эти технологии по-разному подходят к проблеме обеспечения качества обслуживания.

DiffServ — это решение 3-го уровня, позволяющее внедрить QoS в среде, не ориентированной на соединение (connectionless environment). Основная задача, требующая решения, — это стандартизация набора блоков для построения QoS, используя которые провайдеры могут улучшить IP-сервис. DiffServ предполагает внедрение QoS-механизма в конечных сетях с помощью устройств доступа и последующую его транспортировку по магистрали с помощью маршрутизаторов, поддерживающих DiffServ. Поскольку технологии работают на 3-м уровне, DiffServ можно развернуть на любой инфраструктуре 2-го уровня. Маршрутизаторы и сервисы DiffServ и non-DiffServ способны совместно работать в одной среде.

В ближайшее время технология DiffServ может получить широкое распространение, поскольку обеспечивает IP QoS и включает в себя механизм предоставления QoS как на оборудовании доступа, так и на магистралях.

MPLS — технология, упрощающая транспортировку IP-пакетов по магистрали с помощью активных сетевых устройств уровня 2/3. Хотя технология MPLS и обеспечивает QoS, это не главная ее задача. MPLS сфокусирована, в основном, на повышении масштабируемости Internet с использованием механизма инжиниринга трафика. Магистральные сети, построенные при помощи MPLS, лучше поддерживают QoS-трафик, но применение этой технологии влечет за собой существенные изменения в архитектуре сетей. MPLS, по

сути являющаяся гибридом сетевой (Уровень 3) и транспортной (Уровень 2) структур, предлагает качественно новый путь построения магистральных IP-сетей.

DiffServ и MPLS — это независимые разработки, которые могут функционировать как вместе, так и раздельно. Однако сети MPLS должны обладать способностью определять состояние QoS в трафике DiffServ. В дальнейшем планируется совместное использование этих технологий.

2.1. Базовая архитектура QoS

Базовая архитектура QoS включает 3 основных компонента:

- механизмы идентификации и маркировки, предназначенные для координирования QoS между оконечными сетевыми элементами;
- QoS в пределах одного элемента сети (например, инструментарий для организации очередей и формирования трафика);
- политики, управление и учет QoS, необходимые для контроля и администрирования трафика между оконечными элементами сети.

2.1.1. Идентификация и маркировка трафика

Чтобы обеспечить приоритет обслуживания для определенного типа трафика, его следует идентифицировать. Далее, в случае необходимости, пакеты могут быть маркированы. (Классификация подразумевает выполнение именно этих двух задач.) Трафик может быть идентифицирован по различным характеристикам пакета, например по значениям полей заголовка любого уровня (MAC-адрес, IP-адрес, IP-протокол верхнего уровня); по ToS-байту (Type of Service) в IP-заголовке — это биты IP Precedence поля DSCP (DiffServ Code Point) — или по битам CoS (Class of Service) в 802.1p/q-заголовке; по типу приложения и т. п.

К общепринятым методам идентификации потоков данных относятся:

- списки доступа (access control list, ACL);
- маршрутизация, основанная на политиках (policy-based routing, PBR);
- гарантированный уровень доступа (committed access rate, CAR);
- распознавание сетевых приложений (network-based application recognition, NBAR).

Идентификация по спискам доступа выполняется для таких механизмов управления заторами, как очереди с приоритетами (priority queuing, PQ), индивидуальные очереди (custom queuing, CQ), а в некоторых случаях — и для взвешенной справедливой очереди на базе классов (CBWFQ). Поскольку в каждом из маршрутизаторов создаются свои очереди PQ или CQ, идентификация пакета в данном случае действительна только в пределах того устройства, на которое поступил данный пакет, и установки приоритета для QoS не передаются последующим транзитным маршрутизаторам в сети.

Прямо противоположный подход — установка битов приоритета: в этом случае одна и та же маркировка пакетов действует по всей IP-сети. Для маркировки могут использоваться CoS-биты User Priority в 802.1p-части заголовка 802.1Q или биты IP Precedence поля DSCP в байте ToS заголовка IPv4-пакетов.

Класс сервиса для каждого пакета задается тремя битами приоритета. На основе IP Precedence трафик может быть разбит на 6 классов сервиса. Другими словами, эти три бита позволяют назначить IP-пакету приоритет от 0 до 7 (значения 6 и 7 зарезервированы). Технологии организации очередей, действующие в сети, обеспечивают обслуживание пакетов в соответствии с этим показателем. Спецификация DiffServ (RFC-2475) расширяет возможности использования байта ToS, увеличивая число битов до 6. Определение поля ToS заменяется определением байта DS в протоколе IPv4, как описано в документе RFC-1349. Шесть битов поля DS используются в качестве кодов для определения вида предоставляемых дифференцированных услуг (DSCP). Они служат для выбора необходимого класса обработки трафика на каждом транзитном узле.

Такие возможности, как маршрутизация на базе политик (PBR) и гарантированный уровень доступа (CAR), могут быть использованы для установки приоритета на основе классификации по расширенным спискам доступа. Это обеспечивает гибкость в назначении приоритета, в том числе по приложениям или пользователям, по адресу сегмента назначения или источника и т. д.Как правило, эти функциональные средства разворачиваются как можно ближе к границе сети или автономной системы, так чтобы каждый последующий сетевой элемент мог обеспечивать сервис в соответствии с заданной политикой. Следует отметить, что обе технологии — и PBR, и CAR — кроме маркирования, выполняют и ряд других функций, в частности, определение политик.

Распознавание сетевых приложений (NBAR) допускает более глубокий анализ трафика при классификации. Так, например, может быть выполнена идентификация по URL или MIME-типу HTTP-пакета. Как только такой пакет идентифицирован, он может быть маркирован с указанием соответствующего приоритета.

2.1.2. QoS-средства в пределах одного сетевого элемента

В пределах одного узла сети QoS обеспечивается с помощью следующих механизмов:

- управление заторами (congestion management);
- организация очередей (queuing) и предотвращение заторов (congestion avoidance);
- эффективное использование канала (link efficiency);
- формирование трафика (shaping);
- определение политик (policing).

Управление заторами. Из-за пульсирующей (bursty) природы трафика голоса, видео и данных объем трафика может превысить возможности его передачи. В этом случае потребуется применить какие-либо технологии управления заторами, такие например, как очереди с приоритетами (priority queuing, PQ), индивидуальные очереди (custom queuing, CQ), взвешенная справедливая очередь (weighted fair queuing, WFQ) и взвешенная справедливая очередь на базе классов (class-based weighted fair queuing, CBWFQ), которые будут подробно рассмотрены ниже. Каждый из алгоритмов организации очередей разрабатывался для решения проблем определенного класса сетевого трафика и отчасти влияет на производительность сети, поэтому если канал не перегружен, то нет необходимости помещать пакеты в очередь.

Предотвращение заторов. Методики предотвращения заторов основаны на отслеживании состояния сетевого трафика. Они дают возможность спрогнозировать заторы в

потенциально узких местах сети и избежать их возникновения, в противоположность методам управления заторами, которые нацелены на устранение уже возникшего переполнения канала. Как правило, в TCP/IP-средах для этих целей используются алгоритмы случайного раннего обнаружения (random early detection, RED): при возрастании нагруженности канала пакеты отбрасываются в случайном порядке.

Однако при наличии высокоприоритетного трафика возникает, так называемая, проблема «tail drops» — отсечения конца очереди. Когда очередь полна, ни один вновь поступивший пакет туда уже не помещается, а потому отбрасывается. Чтобы обеспечить целостность высокоприоритетного трафика, необходимо, во-первых, следить за тем, чтобы очередь, по возможности, не переполнялась (в ней должно оставаться место для высокоприоритетных пакетов); во-вторых, используя некоторый критерий, отбрасывать пакеты с меньшим приоритетом, прежде чем будут отброшены пакеты с более высоким приоритетом. Оба этих механизма реализует алгоритм взвешенного случайного раннего обнаружения (weighted random early detection, WRED).

WRED объединяет возможности RED-алгоритма и IP Precedence, благодаря чему предпочтение при обслуживании получает высокоприоритетный трафик. Алгоритм WRED избирательно отбрасывает пакеты с меньшим приоритетом, если в интерфейсе возникает угроза затора, и обеспечивает дифференцированные передаточные характеристики для различных классов сервиса.

Эффективное использование канала. Интерактивный трафик (Telnet, VoIP и т. п.) весьма чувствителен к растущим значениям задержки и вариации задержки, когда сеть обслуживает пакеты большого размера (например, при FTP-передаче LAN-to-LAN через WAN-канал), особенно если очереди организуются на низкоскоростных каналах. Так, например, задержка сериализации (serialization delay — время физической побитовой передачи пакета через интерфейс; определяется отношением размера пакета к ширине полосы пропускания) для 1500-байтового пакета в канале с пропускной способностью 56 кбит/с составляет 214 мс.

Если какому-либо голосовому пакету придется ожидать отправки, задержка может превысить любые нормы еще до того, как этот пакет покинет маршрутизатор, поскольку к задержке сериализации голосового пакета добавятся еще и эти 214 мс.

Специальные механизмы, такие как фрагментация соединения и чередование (link fragmentation and interleave, LFI), позволяют разбивать большой пакет на пакеты меньшего размера и при отправке чередовать их с голосовыми. Алгоритм фрагментации и чередования описан в Multiclass Extensions to Multilink PPP (MCML), предложении по стандарту IETF. В среде Frame Relay фрагментация выполняется согласно спецификации FRF.12.

Другой способ повышения эффективности передачи состоит в использовании меньшего числа служебных битов. Например, протокол Real-Time Transport Protocol (RTP) предусматривает использование пакетов с 40-байтовым заголовком. Как правило, задействованными оказываются только 20 байт, поэтому в некоторых случаях издержки удваиваются. Сжатие RTP-заголовков (Compressed Real-Time Protocol, CRTP) позволяет сократить заголовок до 2–5 байт. Особенно выгодно использовать этот метод для небольших пакетов (таких, как голосовой IP-трафик) на низкоскоростных каналах (384 Кбит/с и ниже). Компрессия RTP-заголовков поддерживается на последовательных каналах с использованием Frame Relay, High-Level Data Link Control (HDLC) или PPP-инкапсуляции. Реализован этот механизм и на ISDN-интерфейсах. Соответствующий проект спецификации IETF называется Compressed RTP (CRTP).

Формирование трафика и определение политик. Методы формирования трафика (traffic shaping, формирование полосы) применяются для создания полосы, выделенной

из потенциально доступной полосы пропускания, в тех случаях, когда наблюдается несоответствие скоростей каналов. Так, при использовании hub-and-spoke, самой популярной топологии Frame Relay, в центральном узле, как правило, предусматривается высокоскоростное соединение (скажем, T1), а удаленные узлы передают данные через сравнительно «медленные» каналы (например, 128 кбит/с). Поэтому возможны заторы трафика на пути между центральным и удаленными узлами.

Формирование трафика — это действенный метод, позволяющий приблизить трафик к отметке 128 кбит/с во избежание переполнения низкоскоростного канала. Трафик, скорость которого выше заданной, буферизуется, с тем чтобы можно было отправить его позднее и тем самым поддержать заданный темп передачи.

Определение политик (policing) по своей сути близко к формированию трафика, но есть одно существенное отличие: трафик, скорость которого превышает указанное пороговое значение, не буферизуется, а, как правило, отбрасывается. Хотя основная задача средств определения политик — отбрасывать трафик, скорость передачи которого превышает заданную, этот механизм используется также для перемаркировки «непрофильных» пакетов и последующего уведомления устройств, находящихся на пути их следования, о том, что такие пакеты должны отбрасываться в первую очередь.

2.2. Управление QoS

Поддержка качества обслуживания требует взаимодействия всех сетевых уровней, а также всех сетевых элементов на пути следования пакетов от отправителя к получателю, поэтому несогласованная работа одного узла может свести на нет усилия всех остальных звеньев этой цепочки. Отсюда вытекает необходимость централизованного управления средствами QoS, особенно в крупных сетях.

Управление QoS помогает определить задачи и оценить действенность политики QoS. Общепринятая методология включает следующие шаги:

- Определение характеристик трафика с помощью таких устройств, как RMON-зонды (probe). Кроме того, необходимо оценить (в плане времени отклика) приложения, которым требуется QoS.
- После получения характеристик трафика и определения приложений, которым требуется определенный уровень QoS, выбирается политика и реализуются технологии для предоставления такого сервиса. Политика QoS — это набор правил, позволяющий активным сетевым устройствам (коммутаторам, маршрутизаторам, серверам доступа) опознавать различные типы трафика и обслуживать их, используя те или иные механизмы QoS.
- Оценка результатов. Протестировав (с помощью специальных средств мониторинга) время отклика определенных приложений, необходимо убедиться в том, что необходимые параметры QoS обеспечены.

Следует иметь в виду, что в изменяющейся сетевой среде поддержка QoS — это не разовая процедура, а неотъемлемая часть сетевого сопровождения. Постоянный контроль сетевого трафика поможет выявить намечающиеся тенденции и позволит сетевым администраторам оперативно отреагировать на изменение требований к сетевым ресурсам.

2.3. Уровни сервиса при обмене между оконечными элементами сети

Уровень сервиса соответствует реальным возможностям QoS, то есть определяет способность сети обеспечить затребованный сервис при передаче трафика определенного класса между оконечными точками. Сервисы различаются по уровню ограничений, которые описывают связь между полосой пропускания, задержками, вариацией задержки и характеристиками потерь.

Различают три основных уровня сервиса:

- Сервис «без гарантии доставки» (Best-effort service), известный как сервис без QoS. Это базовый уровень для соединений без гарантированной скорости передачи.
- Дифференцированный сервис, мягкий QoS (Differentiated service, soft QoS). Определенному классу трафика отдается предпочтение при обслуживании (в плане скорости обработки, выделяемой полосы пропускания и средней величины потерь пакетов). Статическая схема обеспечивается классификацией трафика, а также использованием инструментальных средств QoS, таких как PQ, CQ, WFQ и WRED.
- Гарантированный сервис, жесткий QoS (Guaranteed service/ hard QoS) — полное (абсолютное) резервирование сетевых ресурсов для трафика определенного класса. Обеспечивается такими средствами QoS, как RSVP и CBWFQ.

Рассмотрим эти уровни сервиса подробнее.

2.3.1. Сервис «без гарантии доставки»

Характеризуется очередями FIFO (первым пришел — первым отправлен), при формировании которых все потоки имеют равные права. Простейшая форма FIFO-очереди предполагает буферизацию пакетов в случае перегруженности сети; когда сеть становится доступной, пакеты отправляются в том порядке, в котором прибыли. Такой метод формирования очереди во многих случаях принят по умолчанию, поэтому не требует специального конфигурирования устройств.

Главный недостаток очередей FIFO состоит в том, что пакеты всех потоков рассматриваются как равноправные (приоритеты пакетов не анализируются); основным критерием остается очередность поступления пакетов, которая и определяет последовательность их размещения в буфере, а также быстроту обработки. Немаловажно и то, что транспортный сервис «без гарантии доставки» не предусматривает никаких механизмов защиты от источников трафика, характеризующегося высокой степенью непредсказуемости, поэтому при наличии в сети мощного источника подобного «пульсирующего» трафика (burst) пакеты критически важных приложений могут доставляться с большими задержками.

Кроме того, при переполнении очереди пакеты попросту отбрасываются, вне независимости от приоритета. Маршрутизатор не может предотвратить отбрасывания пакетов (к тому же механизм FIFO не в состоянии отличить пакет с высоким приоритетом от пакета с низким). Таким образом, FIFO-очереди — это первый шаг в контролировании сетевого трафика, однако современные интеллектуальные сети требуют более продуктивных и надежных алгоритмов.

2.3.2. Дифференцированный сервис

Реализуется путем организации разного рода очередей. Очереди накапливают избыточный трафик и передают его в сеть небольшими порциями согласно порядку поступления по мере рассасывания затора. Если очередей несколько, коммутатор или маршрутизатор может реализовать приоритетное обслуживание в зависимости от способа дифференциации трафика.

Управление очередями должно быть тщательно продумано, чтобы избежать непредсказуемых задержек и, как следствие, сильной вариации задержки. Один из возможных методов управления заторами — использование алгоритмов создания очередей для сортировки трафика и выбора метода определения его приоритета на выходном соединении. Подразумевается, что сеть «знает» параметры передачи для определенных классов трафика и обеспечивает обслуживание пакетов исходя из их характеристик. Такими характеристиками могут быть адреса отправителя и получателя, порт транспортного уровня получателя, значение приоритета. Рассмотрим наиболее распространенные методы организации очередей.

Очереди с приоритетами (Priority queuing, PQ). Этот метод гарантирует, что важный трафик будет обрабатываться в первую очередь на всем пути следования. Приоритет назначается пакетам в зависимости от сетевого протокола (IP, IPX, AppleTalk, ...), номера порта TCP/UDP, входного интерфейса, размера пакета, адреса отправителя и получателя и т. д.Метод PQ позволяет организовать четыре очереди с разными приоритетами: высоким (high), средним (medium), обычным (normal) и низким (low). Пакеты из очереди с наивысшим приоритетом транспортируются первыми. Если эта очередь оказывается пустой, передаются пакеты из очереди с меньшим приоритетом и т. д.Этот механизм гарантирует, что высокоприоритетный трафик будет обслуживаться с минимальными задержками. Недостаток данного алгоритма состоит в том, что в случае постоянного наличия потока с высшим приоритетом трафик с более низким приоритетом не будет транспортироваться вообще. Поэтому PQ рекомендуется использовать только для низкоскоростных WAN-соединений и (в редких случаях) на интерфейсах 1,544 Мбит/с или выше. PQ целесообразно применять в тех сетях, где трафик имеет иерархию по приоритету и поток с высшим приоритетом не должен задерживаться менее важным трафиком. Например, для голосового трафика можно установить более высокий приоритет, чем для FTP.

Индивидуальные очереди (Custom queuing, CQ). Метод используется в тех сетях, где необходимо гарантировать определенный минимальный уровень сервиса для каждого класса трафика. Технология формирования индивидуальных очередей позволяет администратору резервировать для каждого класса некоторую часть полосы пропускания. Таким образом, критически важным приложениям и трафику, чувствительному к задержкам, может быть выделена большая часть доступной полосы, а низкоприоритетному трафику — меньшая. Администратор может сконфигурировать до 17 очередей, включая нулевую — очередь системных пакетов, которая обслуживается первой. Маршрутизатор обслуживает очереди с 1-й по 16-ю, используя циклический метод (round-robin), и в каждом цикле освобождает предварительно заданное число байт в каждой очереди. Если какой-либо класс трафика в данный момент времени не занимает отведенную ему полосу пропускания, то она передается в распоряжение остальным классам. В пределах очереди для данного класса трафика применяется метод FIFO. На практике индивидуальные очереди используются при передаче голоса, видео, а также при работе протоколов, требующих, чтобы время ответа было предсказуемо (например, IBM Systems Network Architecture, SNA). Как и очереди с приоритетами, CQ конфигурируется статически и не может автоматически адаптироваться к изменению ситуации в сети.

Взвешенная справедливая очередь на базе потоков (Flow-based weighted fair queuing, FBWFQ), или просто взвешенная справедливая очередь (WFQ). Алгоритм, позволяющий динамически разделить полосу пропускания между потоками согласно весу каждого потока. Каждая очередь обслуживается «справедливо» с точки зрения количества передаваемых байт. Согласно этой схеме, потоки низкообъемного трафика обслуживаются «быстрее», однако в действительности передается такое же число байт, как и в случае потоков большого объема. Например, если очередь 1 состоит из 100-байтовых пакетов, а очередь 2 — из 50-байтовых, алгоритм WFQ будет обрабатывать по два пакета из очереди 2 на каждый пакет из очереди 1. Таким образом, WFQ позволяет снизить задержки при передаче такого рода трафика даже при изменении условий передачи. Алгоритм справедливых очередей подходит для передачи данных большинства приложений и поэтому используется по умолчанию на последовательных интерфейсах с полосой пропускания E1 (2,048 Мбит/с) и ниже. В рамках FBWFQ потоки создаются в зависимости от характеристик пакета (адресов отправителя и получателя, идентификаторов сеанса (порт/socket), типа протокола). Для каждого потока организуется своя собственная очередь, в которой буферизуются пакеты при возникновении заторов.

«Взвешенность» WFQ напрямую связана с использованием битов старшинства (IP Precedence), что позволяет предоставить лучший сервис для конкретных очередей. Алгоритм WFQ в состоянии выявить пакеты с более высоким приоритетом и обеспечить для этого трафика предпочтительное обслуживание. Поле IP Precedence может содержать значения от 0 (по умолчанию) до 7 (биты 6 и 7 зарезервированы). При возрастании значения алгоритм расширяет полосу для потока, гарантируя его быстрое обслуживание при возникновении затора. WFQ-алгоритм присваивает вес каждому потоку, что и определяет порядок обработки пакетов в очереди (здесь, согласно схеме вычисления веса, реализуется обратная зависимость: меньший вес — более высокий уровень обслуживания). Например, пакеты со значением 7 в поле IP Precedence имеют меньший вес, чем пакеты со значением 3, и поэтому передаются как более приоритетные. WFQ работает также с протоколом резервирования ресурсов (Resource Reservation Protocol, RSVP), описанным ниже, и позволяет обеспечить как дифференцированное качество обслуживания, так и гарантированное. Кроме того, WFQ эффективно решает проблему вариаций задержек циклического обхода.

2.3.3. Гарантированный сервис

Метод абсолютного резервирования сетевых ресурсов для специфического трафика. Обеспечивается такими инструментами QoS, как взвешенная справедливая очередь на базе классов (Class-based weighted fair queuing, CBWFQ). CBWFQ гарантирует сервис в пределах отдельного интерфейса.

Взвешенная справедливая очередь на базе классов (Class-based weighted fair queuing, CBWFQ) — метод управления заторами, предложенный Cisco. Позволяет обеспечить минимальную гарантированную полосу пропускания и используется как для управления гарантированным уровнем доступа (CAR), так и для формирования трафика. Согласно схеме CBWFQ, вместо создания очередей для каждого индивидуального потока, определяется класс, который включает один или несколько потоков. Для каждого класса может быть гарантирована минимальная ширина полосы.

Примером использования возможностей CBWFQ может служить предотвращение захвата полосы пропускания несколькими низкоприоритетными потоками при передаче высокоприоритетных данных. Например, если видеопоток нуждается в половине полосы E1,

то при использовании WFQ это требование будет выполнено лишь в том случае, если таких потоков два. При увеличении количества потоков полоса, выделенная видеопотоку, будет уменьшаться, поскольку WFQ-механизм действует по принципу «справедливости». При наличии 10 потоков видеопотоку будет отведена 1/10 полосы. Проблема не будет решена даже в том случае, если установить бит приоритетности равным 5 ($1 \cdot 9 + 6 = 15$, видеопоток получит 6/15 полосы). Чтобы обеспечить видеопотоку половину полосы, необходим такой механизм, как CBWFQ. Администратор определяет класс, к которому принадлежит видеопоток, и конфигурирует для данного класса сервис 1024 кбит/с (половина E1). Теперь видеопоток получит половину полосы, а остальные классы трафика (обслуживаемого по схеме FBWFQ), по умолчанию будут делить оставшуюся полосу.

Можно также использовать очередь с минимальными задержками (Low-latency queue, LLQ), или, что то же самое, очередь по приоритету (Priority queue class-based weighted fair queuing, PQCBWFQ). Этот способ применяется главным образом в мультисервисных сетях для передачи данных, голоса и видео. Метод LLQ аналогичен методу CBWFQ, за исключением того, что он позволяет создать очередь для классов трафика, имеющую абсолютный приоритет над другими очередями CBWFQ, т.е. LLQ — это комбинация PQ и CBWFQ. Следует также отметить, что, согласно алгоритму CBWFQ, для определенного класса резервируется полоса минимальной ширины, а если доступны дополнительные ресурсы, класс вправе их использовать. Верно и другое: если класс не использует гарантируемую выделенную полосу, ею могут воспользоваться другие потоки.

3. Принципы передачи мультимедиа-трафика в сетях IP/Ethernet

3.1. Передача мультимедийной информации и IGMP

Передача мультимедийных данных по сетям IP является одним из наиболее перспективных направлений развития сетевых технологий. Этот вид информации передается обычно в режиме без установления соединения (протокол UDP/RTP). Наиболее типичной схемой в этом случае является наличие одного передатчика и большого числа приемников (multicast-группа). Эта схема реализуется с использованием *multicast-адресации*. Multicast-адресация может осуществляться на IP- и MAC-уровнях. В IP для групповой рассылки используется диапазон адресов класса D — `224.0.0.1` – `249.255.255.254`. В Ethernet для этих целей зарезервирован блок адресов в диапазоне от `01:00:5E:00:00:00` до `01:00:5E:7F:FF:FF`. Первый байт адреса, равный `01`, указывает на то, что адрес является групповым. Данная схема резервирования адресного пространства позволяет использовать 23 бита MAC-адреса для идентификации группы рассылки при групповой рассылке IP (см. Рис. 1).

Область из 5 бит в IP-адресе, отмеченная `*****`, не используется при формировании Ethernet-адреса. Так как соотношение IP- и MAC-адресов не является однозначным, драйверы должны обеспечивать обработку адресов с тем, чтобы интерфейсы получали только те кадры, которые действительно им предназначены. Для того чтобы информировать маршрутизатор о наличии участников multicast-группы в подсети, связанной с тем или иным интерфейсом, используется *протокол IGMP*.

Протокол IGMP (Internet Group Management Protocol, RFC-1112) используется для видеоконференций, передачи звуковых сообщений, а также группового исполнения команд различными ЭВМ. Этот протокол использует групповую адресацию.

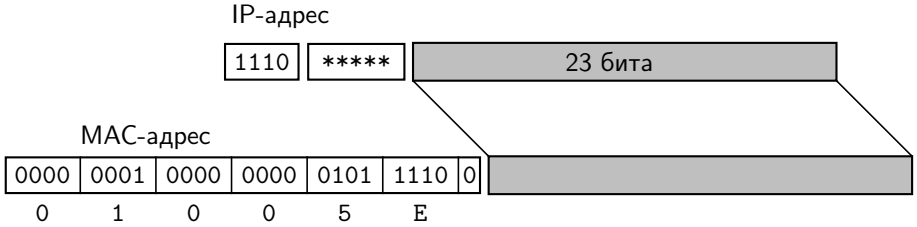

Рис. 1. Соотношение IP-адресов класса D и MAC-адресов

Групповая форма адресации нужна тогда, когда какое-то сообщение или последовательность сообщений необходимо послать нескольким (но не всем) адресатам одновременно. При этой форме адресации ЭВМ имеет возможность выбрать, следует ли участвовать в этой процедуре. Когда группа ЭВМ хочет взаимодействовать друг с другом, используется один групповой (multicast) адрес. Групповая адресация может рассматриваться как обобщение обычной системы адресов, а традиционный IP-адрес — частный случай группового обращения при числе ЭВМ, равном 1.

При групповой адресации один и тот же пакет может быть доставлен заданной группе ЭВМ. Членство в этой группе может динамично меняться со временем. Любая ЭВМ может войти в группу и выйти из группы в любое время по своей инициативе. В то же время ЭВМ может быть членом большого числа таких групп. ЭВМ может посылать пакеты членам группы, не являясь им сама. Каждая группа имеет свой адрес класса D.

Адрес `224.0.0.1` предназначен для обращения ко всем группам. Ряд других multicast-адресов зарезервирован строго для определенных целей:

Адрес группы	**Описание**
`224.0.0.0`	Зарезервирован
`224.0.0.1`	IGMP-совместимые системы данной подсети
`224.0.0.2`	Маршрутизаторы данной подсети
`224.0.0.4`	DVMRP-маршрутизаторы
`224.0.0.5` – `224.0.0.6`	OSPFIGP (MOSPF)
`224.0.0.9`	Маршрутизаторы RIP2
`224.0.0.10`	IGRP-маршрутизаторы
`224.0.1.0`	VMTP-группа менеджеров
`224.0.1.1`	NTP — Network Time Protocol
`224.0.1.6`	NSS — сервер имен
`224.0.1.7`	Audio News Multicast
`224.0.1.9`	MTP — Multicast Transport Protocol
`224.0.1.10`	IETF-1 low-audio
`224.0.1.11`	IETF-1 audio
`224.0.1.12`	IETF-1 video
`224.1.0.0` – `224.1.255.255`	ST-группы
`224.2.0.0` – `224.2.255.255`	Вызовы при мультимедиа-конференциях
`232.0.0.0` – `232.255.255.255`	VMTP переходные группы

Для того чтобы участвовать в коллективных обменах в локальной сети, ЭВМ должна быть снабжена программой, которая поддерживает этот режим. При этом сервер локальной сети (шлюз) информируется о намерении локального узла подключиться к группе.

Шлюз передает эту информацию другим внешним серверам IP-сети. Режим групповой рассылки не загружает локальную сеть так же, как и широковещательный, если сеть построена на коммутаторах с поддержкой IGMP-snooping (отслеживания IGMP-запросов). IGMP для передачи своих сообщений использует IP-дейтаграммы, в которые инкапсулированы пакеты IGMP. Для подключения к группе сначала посылается IGMP-сообщение «всем ЭВМ» о включении в группу, при этом локальный multicast-сервер (шлюз) подготавливает маршрут. Шлюз время от времени проверяет ЭВМ и определяет, не покинули ли они группу, поскольку ЭВМ не подтверждает свое членство в группе. Все обмены между ЭВМ и шлюзом производятся в режиме ip-multicast, то есть любое сообщение адресуется всем ЭВМ группы. ЭВМ, не принадлежащая группе, IGMP-сообщений не получает, что сокращает загрузку сети.

3.2. Протокол реального времени RTP

В Интернет и в сетях меньшего масштаба, возможна потеря пакетов изменение их порядка в процессе транспортировки, а также вариация времени доставки в достаточно широких пределах. Мультимедийные приложения накладывают достаточно жесткие требования на транспортную среду. Для согласования таких требований с возможностями Интернет был разработан *протокол RTP*. Протокол RTP базируется на идеях, предложенных Кларком и Тенненхаузом [5], и предназначен для доставки данных в реальном масштабе времени (например, мультимедиа). При этом определяется тип поля данных, производится нумерация посылок, присвоение временных меток и мониторинг доставки. Приложения обычно используют RTP поверх протокола UDP для того, чтобы использовать его возможности мультиплексирования и контрольного суммирования, но RTP может использоваться и поверх любой другой сетевой транспортной среды. RTP поддерживает одновременную доставку по многим адресам.

Следует иметь в виду, что сам по себе RTP не обеспечивает своевременной доставки и не предоставляет каких-либо гарантий уровня сервиса (QoS). Этот протокол не может гарантировать также корректного порядка доставки данных. Правильный порядок выкладки информации может быть обеспечен принимающей стороной с помощью порядковых номеров пакетов. Такая возможность крайне важна практически всегда, но особое внимание этому уделяется при восстановлении передаваемого изображения или звука.

На практике протокол RTP используется вместе с протоколом RTCP (RTP control protocol). Последний служит для мониторинга QoS и для передачи информации об участниках обмена в ходе сессии.

RTP — гибкий протокол, который может доставить приложению нужную информацию, его функциональные модули не образуют отдельный слой, а чаще встраиваются в прикладную программу. Протокол RTP не является жестко регламентирующим.

Рассмотрим принцип работы протокола RTCP на примере аудио-конференции. При организации аудио-конференции каждый участник должен иметь адрес и два порта: один для звуковых данных, другой — для управляющих RTCP-пакетов. Эти параметры должны быть известны всем участникам конференции. При необходимости соблюдения конфиденциальности информация и пакеты управления могут быть зашифрованы. При аудио-конференциях каждый из участников пересылает небольшие закодированные звуковые фрагменты длительностью около 20 мкс. Каждый из таких фрагментов помещается в поле данных RTP-пакета, который, в свою очередь, вкладывается в UDP-дейтаграмму.

Заголовок пакета RTP определяет, какой используется метод кодирования звука (PCM, ADPCM или LPC), что позволяет отправителю при необходимости сменить метод коди-

рования, если к конференции подключился новый потребитель с определенными ограничениями или сеть требует снижения скорости передачи.

При передаче звука весьма важным становится взаимное положение закодированных фрагментов во времени. Для решения задачи корректного воспроизведения заголовки пакетов RTP содержат временную информацию и порядковые номера. Порядковые номера позволяют не только восстановить правильный порядок фрагментов, но и определить число потерянных пакетов-фрагментов.

Так как участники конференции могут появляться и исчезать по своему усмотрению, полезно знать, кто из них присутствует в сети в данный момент, и как до них доходят передаваемые данные. Для этой цели периодически каждый из участников транслирует через порт RTCP multicast-сообщение, содержащее имя участника и диагностические данные. Узел-участник конференции шлет пакет BYE (RTCP), если он покидает сессию.

Если в ходе конференции передается не только звук но и изображение, то используются два независимых потока и, соответственно, две пары UDP-портов. RTCP-пакеты посылаются независимо для каждой из этих двух сессий.

На уровне RTP не существует какой-либо взаимосвязи между аудио- и видео-сессиями. Только RTCP-пакеты несут в себе одни и те же канонические имена участников.

В некоторых случаях можно столкнуться с ситуацией, когда один из участников конференции подключен к сети через канал с небольшой скоростью. Было бы не слишком корректно требовать от всех участников перехода на кодировку, соответствующую этой малой полосе. Для того чтобы этого избежать, можно установить преобразователь, называемый смесителем, в непосредственной близости от узкополосной области.

Смеситель преобразует поток аудио-пакетов в последовательность пакетов, которая соответствует возможностям низкоскоростного канала. Эти пакеты могут быть типа unicast (адресованными одному получателю) или multicast. Заголовок RTP включает в себя средства, которые позволяют мультиплексорам идентифицировать источники потока данных, так что получатель может правильно идентифицировать источник звукового сигнала.

Некоторые участники конференции, использующие широкополосные каналы, не доступны для групповой рассылки IP (например, находятся за межсетевым экраном). Для таких узлов смесители не нужны, здесь используется другой RTP-уровень передачи, называемый трансляцией. Устанавливается два транслятора по одному на каждой из сторон межсетевого экрана. Внешний транслятор передает multicast-пакеты по безопасному каналу внутреннему транслятору. Внутренний же транслятор рассылает их подписчикам локальной сети обычным образом.

Смесители и трансляторы могут выполнять и другие функции, например, преобразование IP/UDP пакетов в ST-II при видео-конференциях.

Абсолютное время представляется с помощью временных меток в соответствии с форматом NTP (Network Time Protocol), который характеризует время в секундах от начала суток (UTC) 1 января 1970 г. Полное разрешение временной метки NTP определяется 64-битовым числом с фиксированной запятой без знака. Целочисленная часть задается первыми 32 битами, а дробная — часть последними. В некоторых полях, где допустимо более компактное представление, используются только средние 32 бита (16 бит целочисленная часть и 16 бит дробная).

3.3. Протокол резервирования ресурсов RSVP

Протокол RSVP используется ЭВМ для того, чтобы запросить для приложения определенный уровень качества сетевых услуг QoS (Quality of Service, например, определенный

уровень полосы пропускания). RSVP используется также маршрутизаторами для доставки QoS-запросов всем узлам вдоль пути информационного потока, а также для установки и поддержания необходимого уровня услуг. RSVP-запросы обеспечивают резервирование определенных сетевых ресурсов, которые нужны, чтобы обеспечить конкретный уровень QOS вдоль всего маршрута транспортировки данных.

Функция этого протокола крайне важна и многообразна, именно по этой причине он один из самых сложных протоколов.

RSVP запрашивает ресурсы только для одного из направлений трафика и только по указанию получателя. RSVP работает поверх IPv4 или IPv6. Протокол относится к числу управляющих, а не транспортных.

RSVP предназначен для работы с существующими и будущими маршрутными протоколами, которые управляют как обычными, так и групповыми потоками. В последнем случае ЭВМ сначала посылает IGMP-запрос, для того чтобы подключиться к мультикастинг-группе, а затем уже RSVP-сообщение для резервирования ресурсов по маршруту доставки.

Протокол RSVP:

- выполняет резервирование полосы для unicast- и multicast-приложений, динамически адаптируясь к изменениям членства в группе вдоль маршрута;
- является симплексным протоколом, т. е. он выполняет резервирование для однонаправленного потока данных;
- ориентирован на получателя, т. е., получатель данных инициирует и поддерживает резервирование ресурсов для потока;
- поддерживает динамическое членство в группе и автоматически адаптируется к изменениям маршрутов;
- не является маршрутным протоколом, но зависит от существующих и будущих маршрутных протоколов;
- транспортирует и поддерживает параметры управления трафиком и политикой, которые остаются непрозрачными для него;
- обеспечивает несколько моделей резервирования или стилей, для того чтобы удовлетворить требованиям различных приложений;
- обеспечивает прозрачность операций для маршрутизаторов, которые его не поддерживают;
- может работать с IPv4 и IPv6.

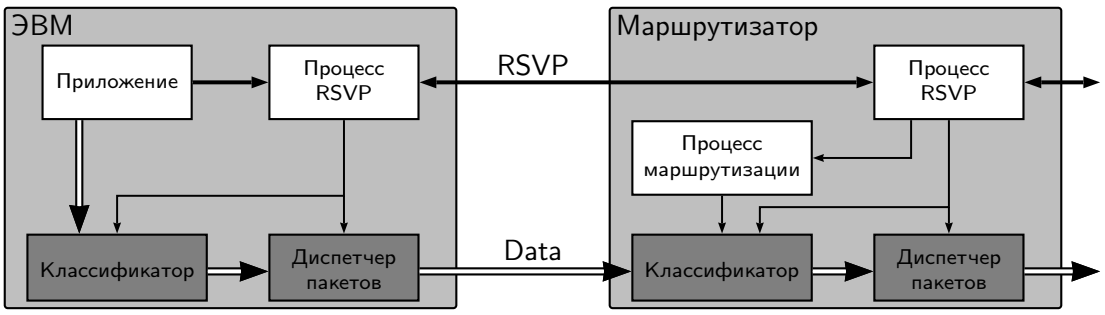

Рис. 2. RSVP в ЭВМ и маршрутизаторе

4. Обоснование выбора темы дипломного проектирования

Целью настоящего дипломного проектирования является создание прикладной программы, имитирующей передачу данных по локальной вычислительной сети, построенной на базе технологии Ethernet. Ethernet на сегодняшний день — самая распространенная технология ЛВС. Более того: кадры Ethernet могут быть инкапсулированы в другие протоколы, например, протоколы семейства xDSL, но это никак не изменит алгоритма функционирования программы, потребуется лишь указать соответствующую скорость работы канала.

Имитационное моделирование — это метод, позволяющий строить модели, учитывающие время выполнения функций. Полученную модель можно «проиграть» во времени и получить статистику происходящих процессов так, как это было бы в реальности. В имитационной модели изменения процессов и данных ассоциируются с событиями. «Проигрывание» модели заключается в последовательном переходе от одного события к другому.

Программ имитационного моделирования сетей Ethernet на сегодняшний день существует много, однако передаче мультимедийной информации в них внимания практически не уделено, если не говорить о крупных и дорогостоящих программных пакетах. Если перед проектировщиком ЛВС стоит задача расчета параметров сети на предмет передачи мультимедийного трафика, и при этом он ограничен в финансовых и технических ресурсах, то ему потребуется специализированное приложение, выполняющее этот расчет.

Разработка такого приложения и была выбрана в качестве дипломного проекта. Таким образом, тема настоящего дипломного проектирования следующая: «Программа имитационного моделирования ЛВС на базе Ethernet с учетом особенностей мультимедийного трафика».

5. Анализ источников информации

5.1. Литературные источники

5.1.1. Б. Столлингс. Современные компьютерные сети

Эта книга посвящена современным аспектам развития высокоскоростных объединенных TCP/IP и ATM сетей. В ней рассматривается широкий круг вопросов: от обработки одиночного пакета или ячейки в очереди на маршрутизаторе или коммутаторе до универсальных методов резервирования сетевых ресурсов для определенного типа трафика; от определения характеристик потока данных до способов их сжатия, позволяющих снизить нагрузку на сеть.

В книге подробно описаны алгоритмы качества обслуживания, такие как PQ, CBQ и WFQ.

5.1.2. Б. Страуструп. Язык C++

Книга Бьерна Страуструпа является каноническим изложением возможностей C++, написанным автором этого языка программирования. Помимо подробного описания самого языка, на страницах книги можно найти множество эффективных подходов к решению разнообразных задач программирования и проектирования.

В последнем издании были добавлены такие главы как стандартная библиотека шаблонов (STL), пространства имен (namespaces), механизм идентификации типов во время исполнения (RTTI), явные приведения типов (cast-операторы) и другие.

5.2. Электронные источники

В сети Internet можно найти практически любую информацию, касающуюся протоколов глобальных и локальных сетей.

5.2.1. Сайт IETF

IETF — Internet Engineering Task Force — организация, непосредственно отвечающая за разработку протоколов и архитектуры Интернет. Конкретная работа ведется в рамках рабочих групп, руководители которых вместе с председателем IETF образуют так называемый IESG (Internet Engineering Steering Group), иным словом, «президиум» IETF.

IETF отвечает за текущие эксплуатационные и назревающие технические проблемы. Рабочие группы имеют различные функции: это может быть выпуск документации, выработка стратегии действий при возникновении проблем, стратегические исследования, разработка новых стандартов и протоколов, доработка уже существующих (например, изменение значений отдельных полей). Рабочая группа обычно выпускает доклад — RFC (Request for Comment). В зависимости от вида рекомендации, это может быть просто документацией и быть доступной для любого желающего, что может быть принято добровольно как здравая идея, или же рекомендация может быть послана в качестве заявки в вышестоящий институт стандартов.

На Web-сайте организации (*http://www.ietf.org/*) опубликованы все документы RFC, некоторые из них приведены в списке литературы отчета.

5.2.2. Сайт IEEE

IEEE — Institute of Electrical and Electronics Engineers — Институт инженеров по электротехнике и электронике.

Эта общественная некоммерческая ассоциация профессионалов ведет свою историю с 1884 года, объединяющая 380 тыс. индивидуальных членов из 150 стран. IEEE издает третью часть технической литературы, касающейся применения компьютеров, управления, электроинженерии, издает более 100 журналов, популярных в среде профессионалов, проводит в год более 300 крупных конференций. За годы своей деятельности IEEE принял около 900 действующих стандартов.

На Web-сайте организации (*http://www.ieee.org/*) лишь небольшая часть стандартов находится в свободном доступе, среди них — все документы, описывающие физический и канальный уровень кабельных и беспроводных сетей Ethernet.

В состав IEEE входит 37 крупных технических обществ, объединяющих индивидуальных членов IEEE по их профессиональной принадлежности. Одно из сообществ — IEEE Communications Society (*http://www.comsoc.org*).

Список литературы

[1] Олифер В. Г., Олифер Н. А. *Компьютерные сети. Принципы, технологии, протоколы* — СПб.: "Питер", 2002.

[2] Столлингс В. *Современные компьютерные сети. 2-е изд.* — СПб.: "Питер", 2003.

[3] Страуструп Б. *Язык программирования C++, Специальное изд.* — М.: "Издательство Бином", СПб.: "Невский диалект", 1999.

[4] В. Орлов *Качество обслуживания, или многоликий QoS* — Сети и телекоммуникации, № 5, 2002.

[5] D. D. Clark, D. L. Tennenhouse *Architectural considerations for a new generation of protocols* — in SIGCOMM Symposium on Communications Architectures и Protocols (Philadelphia, Pennsylvania), pp. 200–208, IEEE, Sept. 1990. Computer Communications Review, Vol. 20(4), Sept. 1990.

[6] Семенов Ю. А. *Протокол IGMP и передача мультимедиа по Интернет.* — ГНЦ ИТЭФ, *http://book.itep.ru/*

[7] Семенов Ю. А. *Протокол реального времени RTP.* — ГНЦ ИТЭФ, *http://book.itep.ru/*

[8] Семенов Ю. А. *Протокол резервирования ресурсов RSVP.* — ГНЦ ИТЭФ, *http://book.itep.ru/*

[9] L. Zhang, R. Braden, Ed., S. Berson, S. Herzog, S. Jamin. *Resource ReSerVation Protocol, RFC-2205.* — *http://www.ietf.org*

[10] S. E. Deering. *Internet Group Management Protocol, RFC-1112.* — *http://www.ietf.org*

[11] H. Schulzrinne, S. Casner, R. Frederick, V. Jacobson *RTP: A Transport Protocol for Real-Time Applications, RFC-2205, 2209, 2210, 1990, 1889* — *http://www.ietf.org*