Непрекращающийся рост Internet и частных сетей предъявляет новые требования к пропускной способности. World Wide Web привел к гигантскому увеличению трафика графической информации. Сегодня еще и голосовые, а также видеоприложения выдвигают свои специфические требования к и без того перегруженным сетям.

Чтобы удовлетворить все эти запросы, одного увеличения емкости сети недостаточно. Что действительно необходимо, так это разумные эффективные методы управления трафиком и контроль загруженности.

Исторически сети на базе IP предоставляли всем приложениям только простейшую услугу по доставке данных по мере возможности. Однако потребности изменились со временем. Организации, потратившие миллионы долларов на установку сети на базе IP для передачи данных между локальными сетями, сталкиваются теперь с тем, что такие конфигурации не способны эффективно поддерживать новые мультимедийные приложения реального времени с многоадресной рассылкой.

ATM - единственная сетевая технология, изначально разрабатывавшаяся для поддержки обычного трафика TCP и UDP наряду с трафиком реального времени. Однако ориентация на ATM означает либо создание новой сетевой инфраструктуры для трафика реального времени, либо замену имеющейся конфигурации на базе IP, причем обе альтернативы обойдутсявесьма недешево.

Поэтому потребность в поддержке нескольких типов трафика с различными требованиями к качеству услуг в рамках архитектуры TCP/IP весьма насущна. Эту задачу призваны решить два ключевых инструмента: транспортный протокол реального времени (Real-Time Transport Protocol, RTP) и протокол резервирования ресурсов (Resource Reservation Protocol, RSVP).

RTP гарантирует доставку данных одному или более адресатам с задержкой в заданных пределах. Это означает, что данные могут быть воспроизведены в реальном времени. RSVP позволяет конечным системам резервировать сетевые ресурсы для получения необходимого качества услуг, в особенности ресурсы для трафика реального времени по протоколу RTP.

Наиболее широко используемый протокол транспортного уровня - это TCP. Несмотря на то что TCP позволяет поддерживать множество разнообразных распределенных приложений, он не подходит для приложений реального времени.

В приложениях реального времени отправитель генерирует поток данных с постоянной скоростью, а получатель(-и) должен предоставлять эти данные приложению с той же самой скоростью. Такие приложения включают аудио- и видеоконференции, распространение живого видео (для немедленного воспроизведения), разделяемые рабочие области, удаленную диагностику в медицине, компьютерную телефонию, распределенное интерактивное моделирование, игры и мониторинг в реальном времени.

Использование TCP в качестве транспортного протокола для этих приложений невозможно по нескольким причинам. Во-первых, этот протокол позволяет установить соединение только между двумя конечными точками, следовательно, он не подходит для многоадресной передачи. Он предусматривает повторную передачу потерянных сегментов, прибывающих, когда приложение реального времени уже их не ждет. Кроме того, у TCP нет удобного механизма привязки информации о синхронизации к сегментам - другое требование приложений реального времени.

Другой широко используемый протокол транспортного уровня UDP не имеет первых двух ограничений (соединение точка-точка и передача потерянных сегментов), но и он не предоставляет критической информации о синхронизации. Таким образом, UDP не предоставляет сам по себе каких-либо инструментов общего назначения для приложений реального времени.

Несмотря на то что каждое приложение реального времени может иметь свои собственные механизмы для поддержки передачи в реальном времени, они имеют много общих черт, а это делает определение единого протокола весьма желательным. Стандартный протокол такого рода - RTP, определенный в RFC1889.

В типичной среде реального времени отправитель генерирует пакеты с постоянной скоростью. Они отправляются им через одинаковые интервалы времени, проходят через сеть и принимаются получателем, воспроизводящим данные в реальном времени по их получении.

Однако ввиду вариации задержки при передаче пакетов по сети они прибывают через нерегулярные интервалы времени. Для компенсации этого эффекта поступающие пакеты буферизуются, придерживаются на некоторое время и затем предоставляются с постоянной скоростью программному обеспечению, генерирующему вывод. Чтобы такая схема работала, каждый пакет получает отметку о времени - таким образом получатель может воспроизвести поступающие данные с той же скоростью, что и отправитель.

RTP поддерживает передачу данных в реальном времени между несколькими участниками сеанса. (Сеанс - это логическая связь между двумя и более пользователями RTP, поддерживаемая в течение всего времени передачи данных. Процесс открытия сеанса выходит за рамки RTP.).

Хотя RTP может использоваться и для одноадресной передачи в реальном времени, его сила в поддержке многоадресной передачи. Для этого каждый блок данных RTP содержит идентификатор отправителя, указывающий, кто из участников генерирует данные. Блоки данных RTP содержат также отметку о времени, чтобы данные могли быть воспроизведены с правильными интервалами принимающей стороной.

Кроме того, RTP определяет формат полезной нагрузки передаваемых данных. С этим напрямую связана концепция синхронизации, за которую частично отвечает микшер - механизм трансляции RTP. Принимая потоки пакетов RTP от одного или более источников, он комбинирует их и посылает новый поток пакетов RTP одному или более получателям. Микшер может просто комбинировать данные, а также изменять их формат.

Пример приложения для микшера - комбинирование нескольких источников звука. Например, предположим, что часть систем данного аудиосеанса генерирует каждая свой собственный поток RTP. Большую часть времени только один источник активен, хотя время от времени одновременно "говорят" несколько источников.

Если новая система хочет принять участие в сеансе, но ее канал до сети не имеет достаточной емкости для поддержки всех потоков RTP, то микшер получает все эти потоки, объединяет их в один и передает последний новому члену сеанса. При получении нескольких потоков микшер просто складывает значения импульсно-кодовой модуляции. Заголовок RTP, генерируемый микшером, включает идентификатор(-ы) отправителя(-ей), чьи данные присутствуют в пакете.

Более простое устройство создает один исходящий пакет RTP для каждого поступающего пакета RTP. Этот механизм, называемый транслятором, может изменить формат данных в пакете или использовать иной комплект низкоуровневых протоколов для передачи данных из одного домена в другой. Например, потенциальный получатель может оказаться не в состоянии обрабатывать высокоскоростной видеосигнал, используемый другими участниками сеанса. Транслятор конвертирует видео в формат более низкого качества, требующий не такой высокой скорости передачи данных.

Протокол RTP используется только для передачи пользовательских данных - обычно многоадресной - всем участникам сеанса. Отдельный протокол управления передачей в реальном времени (Real-Time Transport Control Protocol, RTCP) работает с несколькими адресатами для обеспечения обратной связи с отправителями данных RTP и другими участниками сеанса.

RTCP использует тот же самый базовый транспортный протокол, что и RTP (обычно UDP), но другой номер порта. Каждый участник сеанса периодически посылает RTCP-пакет всем остальным участникам сеанса. RFC 1889 описывает три функции, выполняемые RTCP.

Первая функция состоит в обеспечении качества услуг и обратной связи в случае перегрузки. Так как RTCP-пакеты являются многоадресными, все участники сеанса могут оценить, насколько хороши работа и прием других участников. Сообщения отправителя позволяют получателям оценить скорость данных и качество передачи. Сообщения получателей содержат информацию о проблемах, с которыми они сталкиваются, включая утерю пакетов и избыточную неравномерность передачи. Например, скорость передачи для аудио/видеоприложения может быть снижена, если линия не обеспечивает желаемого качества услуг при данной скорости передачи.

Обратная связь с получателями важна также для диагностирования ошибок при распространении. Анализируя сообщения всех участников сеанса, администратор сети может определить, касается данная проблема одного участника или носит общий характер.

Вторая основная функция RTCP - идентификация отправителя. Пакеты RTCP содержат стандартное текстовое описание отправителя. Они предоставляют больше информации об отправителе пакетов данных, чем случайным образом выбранный идентификатор источника синхронизации. Кроме того, они помогают пользователю идентифицировать потоки, относящиеся к различным сеансам. Например, они дают пользователю возможность определить, что одновременно открыты отдельные сеансы для аудио и видео.

Третья функция состоит в оценке размеров сеанса и мастшабировании. Для обеспечения качества услуг и обратной связи с целью управления загруженностью, а также с целью идентификации отправителя, все участники периодически посылают пакеты RTCP. Частота передачи этих пакетов снижается с ростом числа участников.

При небольшом числе участников один пакет RTCP посылается максимум каждые 5 секунд. RFC 1889 описывает алгоритм, согласно которому участники ограничивают частоту RTCP-пакетов в зависимости от общего числа участников. Цель состоит в том, чтобы трафик RTCP не превышал 5% от общего трафика сеанса.

Назначение любой сети состоит в доставке данных получателем с гарантированным качеством услуг, включающих пропускную способность, задержку и допустимый предел вариации задержки. С ростом числа пользователей и приложений обеспечить качество услуг становится все труднее

Просто реагировать на перегрузку уже недостаточно. Необходим инструмент, с помощью которого перегрузок можно было бы избежать вообще, т. е. сделать так, чтобы приложения могли резервировать сетевые ресурсы в соответствии с требуемым качеством услуг.

Превентивные меры полезны как при одноадресной, так и при многоадресной передаче. При одноадресной передаче два приложения договариваются о конкретном уровне качества услуг для данного сеанса. Если сеть сильно загружена, то она может оказаться не в состоянии предоставить услуги необходимого качества. В этом случае приложениям придется отложить сеанс до лучших времен или попробовать снизить требования к качеству услуг, если это возможно.

Решение в данном случае состоит в резервировании одноадресными приложениями ресурсов для обеспечения требуемого уровня услуг. Тогда маршрутизаторы на предполагаемом пути выделяют ресурсы, например место в очереди и часть емкости исходящей линии. Если маршрутизатор не имеет возможности выделить ресурсы вследствие ранее взятых на себя обязательств, то он извещает об этом приложение. В этом случае приложение может попытаться инициировать другой сеанс с меньшими требованиями к качеству услуг или перенести его на более поздний срок.

Многоадресная рассылка ставит гораздо более сложные задачи по резервированию ресурсов. Она ведет к генерации огромных объемов сетевого трафика в случае, например, таких приложений, как видео, или большой и рассредоточенной группы получателей. Однако трафик от источника многоадресной рассылки может быть в принципе значительно снижен.

Для этого есть два основания. Во-первых, некоторые члены группы могут не нуждаться в доставке данных от конкретного источника в определенный период времени. Например, члены одной группы могут получать информацию одновременно по двум каналам (от двух источников), но при этом получатель может быть заинтересован в приеме только одного канала.

Многоадресный трафик можно снизить и вследствие того, что некоторые члены группы в состоянии обрабатывать только часть передаваемой отправителем информации. Например, видеопоток может состоять из двух компонентов: один с низким качеством картинки, а другой - с высоким. Такой формат имеет ряд алгоритмов сжатия видео: они генерируют базовый компонент с картинкой низкого качества и дополнительный компонент с повышенным разрешением.

Некоторые получатели могут не иметь достаточной вычислительной мощи для обработки компонентов с высоким разрешением или быть подключены к сети через подсеть или канал, не имеющие достаточной емкости, чтобы пропустить полный сигнал.

Резервирование ресурсов позволяет маршрутизаторам заранее определить, в состоянии ли они осуществить доставку многоадресного трафика всем получателям.

В предыдущих попытках реализации резервирования ресурсов и в принятых во frame relay и ATM подходах необходимые ресурсы запрашивает источник потока данных. Этот метод достаточен в случае одноадресной передачи, потому что передающее приложение передает данные в определенном темпе, а необходимы уровень качества услуг заложен в схему передачи.

Однако такой подход нельзя использовать для многоадресной рассылки. У разных членов группы могут быть неодинаковые требования к ресурсам. Если исходный поток может быть разделен на подпотоки, то некоторые члены группы, вполне возможно, пожелают получать только один из них. Например, некоторые получатели могут быть в состоянии обрабатывать только компонент видеосигнала низкого разрешения. Или если несколько отправителей вещают на одну группу, то получатель может выбрать только одного отправителя или некоторое их подмножество. Наконец, требования различных получателей к качеству услуг могут меняться в зависимости от оборудования вывода, мощности процессора и скорости канала.

По этой причине резервирование ресурсов получателем представляется предпочтительным. Отправители могут предоставить маршрутизаторам общие характеристики трафика (например, темп передачи данных и вариабельность), но получатели должны сами определить требуемый уровень качества услуг. Маршрутизаторы сводят затем воедино запросы на выделение ресурсов на общих участках дерева распространения.

В основе RSVP лежат три концепции, касающиеся потоков данных: сеанс, спецификация потока и спецификация фильтра. Сеанс - это поток данных, идентифицируемый по адресату. Отметим, что эта концепция отличается от концепции сеанса RTP, хотя сеансы RSVP и RTP могут иметь взаимооднозначное соответствие. После резервирования маршрутизатором ресурсов для конкретного адресата он рассматривает это как начало сеанса и выделяет ресурсы на время этого сеанса.

Запрос на резервирование от конечной системы-получателя, называемый описателем потока, состоит из спецификаций потока и фильтра. Спецификация потока определяет требуемое качество услуг и используется узлом для задания параметров планировщика пакетов. Маршрутизатор передает пакеты с заданным набором предпочтений, опираясь на текущую спецификацию потока.

Спецификация фильтра определяет набор пакетов, под которые запрашиваются ресурсы. Вместе с сеансом она определяет набор пакетов (или поток), для которых требуемое качество услуг должно быть обеспечено. Любые другие пакеты, направляемые этому адресату, обрабатываются постольку, поскольку сеть в состоянии это сделать.

RSVP не определяет содержание спецификации потока, он просто передает запрос. Спецификация потока включает обычно класс услуг, Rspec (R означает резерв) и Tspec (Т означает трафик). Два других параметра представляют собой набор чисел. Параметр Rspec определяет требуемое качество услуг, а параметр Tspec описывает поток данных. Содержимое Rspec и Tspec прозрачно для RSVP

В принципе спецификация фильтра описывает произвольное подмножество пакетов одного сеанса (т. е. пакетов, адресат которых определяется данным сеансом). Например, спецификация фильтра может определять только конкретных отправителей или протоколы либо пакеты, поля протокольных заголовков которых совпадают с заданными.

С точки зрения хоста работа протокола состоит из следующих этапов (первые два этапа в этой последовательности имеют иногда обратную очередность)

1. Получатель вступает в группу многоадресной рассылки посредством отправки сообщения по протоколу IGMP соседнему маршрутизатору.

2. Потенциальный отправитель отправляет сообщение по адресу группы.

3. Получатель принимает сообщение Path, идентифицирующее отправителя.

4. Теперь, когда получатель имеет информацию об обратном пути, он может отправлять сообщения Resv с дескрипторами потока.

5. Сообщения Resv передаются по сети отправителю.

6. Отправитель начинает передачу данных.

7. Получатель начинает прием пакетов данных.

Механизм установка соединения с резервированием полосы пропускания.

Процедура установки соединения с резервированием полосы пропускания проходит следующим образом:

Конечный пользователь, заинтересованный в передаче чувствительного к задержкам трафика, передает в сеть сообщение с указанием информации о данных, которые он собирается передавать (сюда включается IP адрес источника и номер UDP/TCP порта),а так же информацию о типе трафика.

Эта информация применяется при настройке механизмов управления потоком данных в промежуточных узлах сети для осуществления резервирования полосы пропускания, а так же для предотвращения избыточного резервирования ресурсов для данного типа трафика.

При прохождении по сети этот информационный пакет “запоминает” маршрут по которому он дошел до получателя.

При получении информационного пакета приемник анализирует его содержание и, в случае своей заинтересованности в данной информации, передает в сеть запрос на резервирование полосы пропускания.

Данный запрос, описывающий необходимый тип сервиса и сетевого соединения, передается по сети от приемника к передатчику по тому же маршруту, что и информационный пакет.

Каждый промежуточный узел сети проводит анализ полученного запроса на основании описанных ниже правил.

При получении запроса на установку соединения с резервированием ресурса в узле сети включаются два механизма: контроллер ресурсов канала, определяющий наличие запрашиваемого ресурса и контроллер доступа, сверяющий права данного пользователя с полученным запросом.

Если при отработке обоих механизмов был получен положительный результат, то резервирование, в данном узле, считается установленным и соответствующая информация передается в модули, отвечающие за классификацию потоков и формирование выходных очередей.

Если же хотя бы один из механизмов возвращает отрицательный результат, то протокол информирует источник запроса о невозможности его осуществления.

Обработка запроса на установление соединения с резервированием ресурса проходит по отдельности для каждого типа сетевого соединения так как протокол RSVP способен различать типы соединения.

Тип сетевого соединения определяется тремя параметрами: IP адрес получателя, тип протокола и тип порта назначения.

Если полученный запрос удовлетворяет всем требованиям, то узел производит резервирование необходимой полосы пропускания и передает запрос дальше, в направлении к передатчику.

Как только передатчик получает запрос на резервирование полосы пропускания от приемника соединение считается установленным и начинается обмен информацией.

Во время сеанса связи приемник и передатчик периодически подтверждают дальнейшую необходимость в осуществлении резервирования полосы пропускания путем посылки информационных пакетов передатчиком и запросов на резервирование приемником.

Узел сети в праве прекратить резервирование полосы пропускания как только он не получает очередного подтверждения от приемника или передатчика.

Резервирование полосы пропускания так же может быть прекращено после передачи приемником или передатчиком запроса на отмену соединения.

**Качество услуг**. Качество услуг (QoS) - это ключевая фраза для обозначения сетей передачи данных без потери ячеек с предсказуемой задержкой из конца в конец и доставкой в реальном времени после установления соединения. Высококачественное мультимедиа в сети как в реальном времени, так и при воспроизведении аудио- и видеофайлов с сервера предполагает наличие сети с обеспечением качества услуг. Такие протоколы, как ATM, разрабатывались специально для предоставления нескольких уровней услуг. Обеспечение качества услуг в случае IP возможно только при использовании специальных протоколов, таких как RSVP, для резервирования пропускной способности на промежуточных устройствах (маршрутизаторах).

**Компьютерная телефония.** Термин “компьютерная телефония” (Computer-Telephony Integration, CTI) относится к реализации традиционных аудио- (иногда и видео-) сервисов в сети передачи данных. Системы компьютерной телефонии могут быть реализованы как в сетях с гарантированной пропускной способностью (типа ATM), так и в сетях передачи кадров (типа Ethernet или frame relay).

**CIF.** Общий промежуточный формат (Common Intermediate Format) с разрешением 352 пиксела по горизонтали на 288 пикселов по вертикали является наиболее популярным форматом изображений в видеоконференциях. При меньшей пропускной способности видеосистемы используют, как правило, либо QCIF (Quarter CIF) с разрешением 176х144 пиксела, либо SQCIF (Sub-Quarter CIF) с разрешением 128х96 пикселов. Видео с высокой пропускной способностью описывается форматом 4CIF (704х576 пикселов) или 16CIF (1408х1152 пиксела).

**G.711.** Один из основных стандартов ITU-T для аудиокодеков (кодировщиков-декодировщиков голоса и музыки). G.711 является частью более общих мультимедийных стандартов, таких как H.320 и H.323, кроме того, он используется в компьютерной телефонии и сам по себе. G.711 определяет аудиосигнал с шириной полосы 3,4 КГц (иными словами, обычный аналоговый голосовой сигнал) по информационным каналам в 64 Кбит/с. Стандарт G.722 описывает аудиопоток с шириной полосы 7,0 КГц по каналу в 64 Кбит/с, а стандарт G.728 - аудиопоток с шириной полосы 3,4 КГц по каналу в 16 Кбит/с. Стандарт G.723 определяет передачу компьютерной аудиоинформации по узкополостным телефонным линиям. Он описывает уплотненный сигнал в 3,4 КГц для обычных телефонных линий и используется в мультимедийном стандарте H.324.

**H.233.** Стандарт шифрования данных ITU-T для мультимедийной информации реального времени. H.233 поддерживается целым рядом стандартных служб, в том числе H.320, H.323 и H.324. Стандарт H.234 определяет, каким образом обрабатываются ключи шифрования.

**H.261.** Стандарт ITU-T на кодек со сжатием видео. Поддерживаемый H.320, H.323 и H.324, H.261 совместим с форматами изображений CIF и QCIF. H.261 разрабатывался для спользования с ISDN и допускает скорости передачи данных, кратные 64 Кбит/с. Новый стандарт H.263 (поддерживаемый H.324) повышает эффективность H.261 и совместим с изображениями в форматах SQCIF, 4CIF, 16CIF.

**H.320.** Один из основных стандартов ITU-T для мультимедиа в реальном времени. H.320 - это стандарт для видеоконференций в узкополосных глобальных сетях с коммутацией каналов, таких как ISDN. Он включает спецификации для данных (T.120), голоса (G.711 и G.728), видео (H.261) и шифрования (H.233 и H.234). H.323 представляет собой усовершенствованный стандарт H.320 для основных сетей с коммутацией пакетов. Родственные стандарты для мультимедиа реального времени, не рассматриваемые отдельно в этом словаре, включают H.321 для широкополосного ISDN и ATM, H.322 для сетей коммутации пакетов с гарантированной полосой пропускания и H.310 для мультимедиа высокого разрешения поверх ATM.

H.323. В настоящее время шлюзы и клиентское программное обеспечение являются по большей части нестандартными. Если оба компонента не представлены одной компанией, то, скорее всего, вы не сможете использовать IP-телефонию для звонка другому абоненту.

Здесь приходит на помощь стандарт Н.323, определяющий передачу видео и аудио по сетям с негарантированным качеством услуг, таким как Ethernet и IP.Н.323 описывает несколько элементов, в том числе аудио- и видеокодеки (кодеры/декодеры), коммуникационные протоколы и синхронизацию пакетов. Первоначально стандарт разрабатывался для рынка видеоконференций в качестве альтернативы сеансов по ISDN, но теперь сообщество IP-телефонии адаптировало стандарт для своих собственных нужд.

Но из-за того, что Н.323 разрабатывался для видеоконференций, далеко не всякий шлюз и клиент IP-телефонии поддерживает стандарт. Тем не менее эта ситуация постепенно меняется, так как число производителей, высказывающихся в пользу стандартов и работающих над их оптимизацией для IP-телефонии, неуклонно растет. Среди компаний, заявивших о поддержке Н.323, - VocalTec, Clarent, Dialogic, Array Telecom, Micom, Microsoft, Intel, Brooktrout. В сентябре 1997 года на конференции "Голос по сети" в Бостоне производители из всех областей рынка IP-телефонии

приняли участие в крупнейшей публичной демонстрации интероперабельности Н.323.

**H.324.** Стандарт ITU-T для передачи мультимедиа в реальном времени по обычным телефонным линиям с помощью модемов V.34 на 28,8 Кбит/с или более быстрых. Подобно H.320, H.324 включает стандарт T.120 для разделения данных, сжатие видео по стандарту H.261, а также стандарты шифрования H.233 и H.234. В отличие от H.320, H.324 использует аудиостандарт G.723.

**MMX.** По утверждению Intel, акроним “MMX” не имеет какого-либо конкретного значения, но обычно он расшифровывается как “Мультимедийные расширения”. Более конкретно MMX реализуется как набор новых команд для микропроцессоров Pentium с MMX и Pentium II. Однако MMX занимается не только Intel: так, например, компания Advanced Micro Devices, конкурирующий производитель процессоров, выпустила новое MMX-совместимое семейство процессоров. Многие новые мультимедийные продукты под Windows для компьютерной телефонии и видеоконференций пишутся с учетом преимуществ новых команд MMX.

**RTP.** Транспортный протокол реального времени - это стандарт IETF для передачи данных, таких как голос или видео, в реальном времени по пакетной сети, не гарантирующей качества услуг. Связанный с ним стандарт - протокол управления передачей в реальном времени (Real-Time Transport Control Protocol, RTCP) - обеспечиваетобратную связь между двумя устройствами или группой. Такие мультимедийные стандарты ITU-T для сетей без обеспечения качества услуг, как H.323 и H.324, опираются на RTP/RTCP.

**T.120.** Этот стандарт ITU-T касается разделения мультимедийных данных по сети в реальном времени. Он служит базисом для таких приложений, как совместная работа над проектами при двусторонних или многосторонних сеансах. T.120 является составной частью некоторых стандартов видеоконференций, например H.320, H.323 и H.324.

РЕЗЮМЕ.

Вчерашние методы работы с большими объемами трафика совершенно непригодны для современных систем. Удовлетворить растущим требованиям к передаче данных в связи с ростом их объема, распространением приложений реального времени и многоадресной рассылки без новых инструментов невозможно. RTP и RSVP обеспечивают надежный фундамент для сетей следующего поколения.