План

Введение

Каждый день в мире происходят миллионы телефонных разговоров, сотни тысяч подписчиков онлайновых игр проводят часы в виртуальных мирах, множество людей проводят видеоконференции, находясь в разных уголках планеты. Требования к сетевым службам у данных приложений имеют различный характер. Но в большинстве случаев многие мультимедийные приложения весьма чувствительны к длительности сквозной задержки (сумма ожидания передачи, обработки и ожидания пакета). При этом, однако, важно отметить некритичность данных приложений к потере небольшого количества пакетов. Это обусловлено тем, что потеря пакета оказывает незначительный сбой при воспроизведении аудио- и видеоданных и часто потери могут быть частично или полностью замаскированы (например с использованием интерполяции). Также отметим, что с передачей мультимедиа информации встает вопрос о её сжатия т.к. несжатые видео- и аудиоданные требуют весьма большой пропускной способности. В данном реферате кратко рассмотрены вопросы сжатия мультимедийной информации, приведен небольшой обзор мультимедийных приложений, рассмотрены протоколы мультимедийной направленности: RTP, RTSP, RTCP, SIP, H.323.

Сетевые мультимедийные приложения

На данный момент в Интернете распространено множество приложений мультимедийного характера: это программы IP-телефонии (сюда относятся программы позволяющие звонить не только между ПК, но и обычными телефонами посредством карточек IP телефонии ставшими последнее время весьма популярными), примером может служить программа Net2Phone, и набравшая большую популярность (в силу бесплатности) Skype. К мультимедийным программам принадлежат приложения для организации видеосвязи, например входящий в стандартную поставку ОС Windows Microsoft NetMeeting©.

Целый класс составляют программы воспроизведения потокового видео и аудио: продукты RealNetworks – RealPlayer, QuickTime фирмы Apple, Windows Media Player от Microsoft, Nullsoft с технологией SHOUTcast и проигрывателем Winamp.

Сжатие изображения и звука

Перед тем как данные передавать их необходимо сжать, это обусловлено тем, что в несжатом виде данные занимают очень много места на носителе и для передачи в приемлемые сроки требуют большой пропускной способности. Ради примера можно привести, что секунда несжатого видеопотока с разрешением 800x600 пикселей и глубиной цвета 24 бита и частотой кадров 30 к/с, требует канала с пропускной способностью в 41,2Мбайта/с что при сопоставлении с максимальной скоростью канала который имеет конечный пользователь при использовании ADSL соединения – 1Мбайт/с (8Мбит/с) указывает на необходимость сжатия. Про звук можно привести пример, когда используется кодово-импульсная модуляция при записи звука, на аудио компакт диски там соотношение составляет 650Мбайт на 74 минуты записи. Отсюда вытекает необходимость в сжатии изображения и звука. Само сжатие бывает двух типов: без потери качества (lossless сжатие) и с потерей (lossy сжатие). При использовании сжатия без потери качества редко удается значительно сжать изображение или звук. Поэтому широкое применение получили методы использующие сжатие с потерями.

Для сжатия голоса применяются кодеки GSM (одноименно называемый стандарт в сотовой связи, также его использует) , G.729, G.723.3. Имеются также некоторые проприетарные кодеки например от RealNetworks. Для сжатия музыки широкое распространение получил формат MP3 или MPEG1 Layer 3 разработанный институтом Фраунгофера и фирмой THOMPSON. Также продвигаются стандарты Ogg Vorbis (имеющий лучшее соотношения объема информации к секунде воспроизведения при сходном качестве звука (приблизительно 2 к 1, хотя так говорить не совсем корректно т.к. он использует переменный битрейт))

Для сжатия видео имеется стандарт MPEG (1/2/4). Данный стандарт сжатия основан на свойствах видеопотока: пространственной и временной избыточности. Пространственная избыточность представляет

собой повторение пикселов одного цвета в какой-либо ограниченной области. Временная – заключается в малом изменении картинки в пределах некоторого промежутка времени, что дает нам возможность кодировать не всю картинку целиком, а только её изменения. Помимо стандартов MPEG в Интернете распространены и другие методы сжатия видео: QuickTime, RealVideo и FLV(Macromedia/Adobe). Весьма распространенным стал формат DivX который произошел от кодека MPEG4.

Протоколы для мультимедийных приложений

Протокол реального времени RTP

В Интернет, также как и в некоторых других сетях, 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 (RFC-2205, -2209, -2210, -1990, -1889,-3989, -3952; "RTP: A Transport Protocol for Real-Time Applications" H. Schulzrinne, S. Casner, R. Frederick, V. Jacobson) предназначен для доставки данных в реальном масштабе времени (например, аудио- или видео). При этом определяется тип поля данных, производится нумерация посылок, присвоение временных меток и мониторирование 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, если мультикастинг поддерживается нижележащим сетевым уровнем.

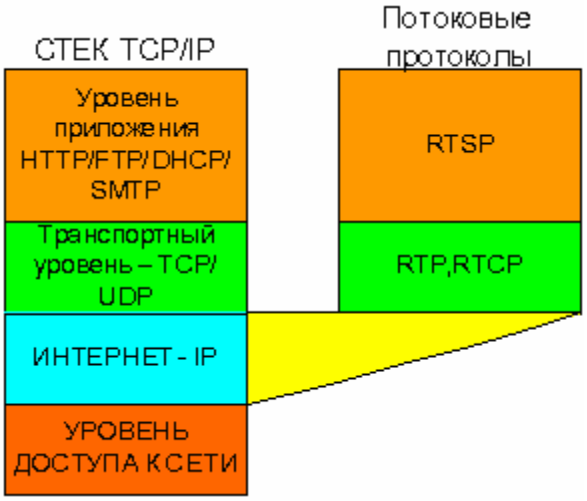

Рис. 1 Соотношения между уровнями протокола TCP/IP и мультмедийными потоковыми протоколами

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.

На практике протокол RTP не отделим от протокола 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.

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 порядка 20 мсек. Каждый из таких фрагментов помещается в поле данных RTP-пакета, который в свою очередь вкладывается в UDP-дейтаграмму.

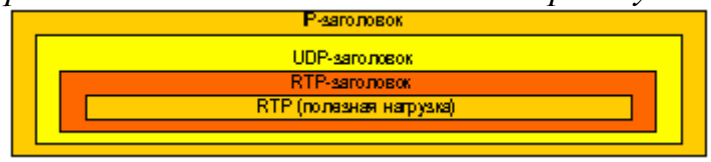

Рис. 2 Структура пакета с полезной нагрузкой

Заголовок пакета RTP определяет, какой вид кодирования звука применен (PCM, ADPCM или LPC), что позволяет отправителю при необходимости сменить метод кодирования, 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 мультикастинг-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, они передаются как два независимых потока с использованием двух пар 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.

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

Протокол RTSP

Для многих пользователей Интернета активно потребляющих мультимедиа требуется управление получаемым контентом (перемотка вперед/назад, остановка/воспроизведение). Для управления процессом воспроизведения проигрыватель, должен обмениваться информацией с сервером управляющей информацией по специальному протоколу. Таким протоколом является RTSP (Real-Time Streaming Protocal, RFC 2326, протокол разработан фирмами RealNetworks и Netscape)

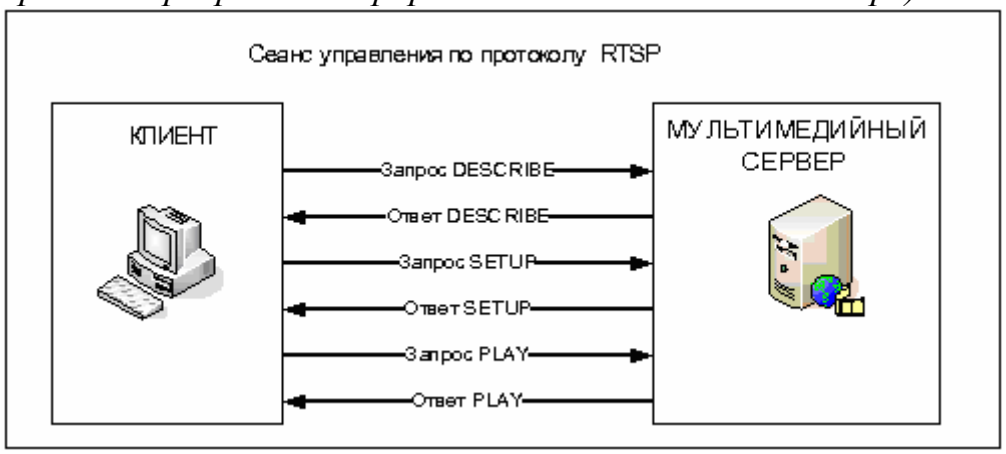

Рис 3 Сеанс управления по протоколу RTSP

RTSP – это протокол прикладного уровня, подобный HTTP и FTP в стеке протоколов TCP/IP. Данный протокол предназначен для управления мультимедиа потоком. Для него протоколами нижнего уровня могут быть RTP, TCP/UDP.

Также как и HTTP протокол RTSP обладает свойствами масштабируемости и взаимодействия. Каждая презентация, каждый мультимедиа поток в нем идентифицируются своим URL. Свойства презентаций и другие спецификации хранятся в файле дескриптора презентации, также имеющем свой URL.

Не смотря на существенное сходство протоколов RTSP и HTTP, они обладают некоторыми различиями. Самое важное отличие заключается в том, что в протоколе RTSP и сервер, и клиент могут генерировать запросы. К примеру, видео сервер может послать запрос на установку параметров воспроизведения определенного видео потока. Также протоколом RTSP

предусматривается, что управление состоянием и связью осуществляет сервер.

Третье отличие заключается в возможности передачи данных вне основной полосы (out-of-band) другими протоколами (например, протоколом RTP).

Сервис RTSP содержит набор инструкций, которыми обмениваются сервер и клиент, они отсылаются в виде RTSP пакетов, содержащих установочные параметры для мультимедиа потока.

Приведем некоторые из инструкций:

DESRIBE, клиентский запрос на описание презентации/мультимедиа потока

ANNOUNCE, серверная инструкция на обновление описания сессии в режиме реального времени

SETUP, клиент запрашивает у сервера ресурсы и начинает RTSP сессию

PLAY, запрос на начало передачи данных в потоке, выделенном командой SETUP

PAUSE, запрос на временную приостановку доставки данных без освобождения ресурсов

TEARDOWN, клиентский запрос на прекращение передачи данных и освобождение связанных с потоком данных

Протокол RTCP

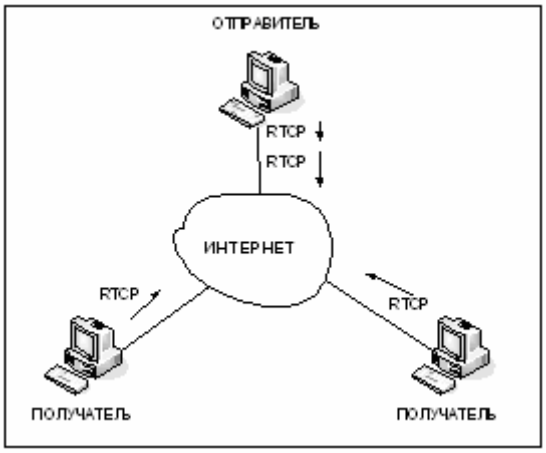

Рис 4. Взаимодействие узлов по протоколу RTCP

Управляющий протокол RTCP базируется на периодической передаче управляющих пакетов всем участникам сессии, используя тот же механизм рассылки, что и для пакетов данных. Этот протокол не имеет самостоятельного значения и используется лишь совместно с RTP. Нижележащий протокол должен обеспечивать мультиплексирование пакетов данных и управления, используя разные номера портов. RTCP выполняет четыре функции:

1. Главной задачей данного протокола является обеспечение обратной связи для контроля качества при рассылке данных. Обратная связь может быть непосредственно полезна при адаптивном кодировании, но эксперименты с

IP мультикастингом показали, что для получателей крайне важно диагностировать ошибки при рассылке пакетов. Посылка сообщений-отчетов о приеме данных всем участникам позволяет тому, кто обнаружил какие-то проблемы, разобраться в том, являются ли эти трудности локальными или глобальными. При механизме рассылки типа IP-мультикастинга, сервис провайдер, который непосредственно не вовлечен в сессию, получив обратную связь, может независимо мониторировать ситуацию в сети.

2. RTCP имеет постоянный идентификатор транспортного уровня для RTP источника, который называется каноническим именем или cnate. Так как SSRC-идентификатор может быть изменен, если будет зафиксировано столкновение или источник будет вынужден рестартовать, получатели нуждаются в cnate, для того чтобы отслеживать каждого из участников. Получателям также нужно Cnate, чтобы установить соответствие между многими потоками данных от одного участника при реализации нескольких сессий одновременно, например, чтобы синхронизовать аудио- и видео-каналы.

3. Первые две функции требуют, чтобы все участники посылали RTCP-пакеты, следовательно скорость передачи должна контролироваться для того, чтобы RTP мог работать с большим числом участников. При посылке каждым участником своих управляющих пакетов всем остальным любой партнер может независимо определить полное число участников сессии. Это число используется при вычислении частоты посылки пакетов.

4. Четвертая опционная функция служит для передачи минимальной управляющей информации, например идентификаторов участников, для графического интерфейса пользователя. Это полезно для "слабо управляемых" сессий, когда участники входят и выходят без должного контроля и без согласования параметров. RTCP выполняет функции удобного канала для контакта со всеми участниками, но он необязательно поддерживает все коммуникационные требования приложения.

Функции 1-3 являются обязательными, когда RTP используется в среде с IP мультикастингом, и рекомендательными для всех остальных сред. Разработчикам приложений RTP рекомендуется избегать механизмов, которые могут работать только в уникастном режиме.

Формат пакетов RTCP

Стандарт определяет несколько типов RTCP пакетов, которые предназначены для переноса управляющей информации:

sr:	*Отчет отправителя. Для статистики приема и передачи участников, которые являются активными отправителями*
rr:	*Отчет получателя. Для получения статистики от участников, которые не являются активными отправителями*

sdes:	*Элементы описания источника, включая cnate*
bye:	*Отмечает прекращение участия в группе*
app:	*Специфические функции приложения*

Каждый RTCP-пакет начинается с фиксированной части, сходной с той, которая используется RTP-пакетами, за ней следуют структурные элементы, которые могут иметь переменную длину в зависимости от типа пакета, но кратную 32 бит. Требования выравнивания и поле длины в фиксированной части заголовка введены для того, чтобы сделать RTCP-пакеты объединяемыми. Несколько RTCP-пакетов могут быть соединены друг с другом без введения каких-либо сепараторов, для того чтобы получить составной RTCP-пакет, который посылается в рамках транспортного протокола низкого уровня, например UDP. Не существует специального счетчика индивидуальных RTCP-пакетов, так как протокол низкого уровня задаст общую длину и определит конец составного пакета.

Каждый индивидуальный RTCP пакет в составном пакете может обрабатываться независимо без каких-либо требований к порядку или комбинации пакетов. Однако, для того чтобы выполнить функции протокола накладываются следующие ограничения:

- *Статистика приема (в SR или RR) должна посылаться так часто, как это позволяют ограничения пропускной способности, так что каждый периодически посылаемый составной пакет включает в себя пакет отчета.*
- *Новые получатели должны приобрести cnate для источника как можно быстрее, каждый составной RTCP-пакет должен включать в себя SDES Cname.*
- *Число типов пакетов, которые могут впервые появиться в составном пакете, должно быть ограничено.*

Таким образом, все RTCP-пакеты должны посылаться в составных пакетах (не менее 2) и иметь следующий рекомендованный формат:

Префикс шифрования. Если составной пакет должен быть зашифрован, он снабжается 32-битным случайным числом-префиксом, которое копируется для каждого передаваемого составного пакета.

SR или RR. Первый RTCP-пакет в составном пакете должен быть всегда сообщением-отчетом. Это справедливо, даже если не было послано или получено никаких данных, в этом случае посылается пустой пакет RR. Это справедливо, даже если другим RTCP -пакетом в составной дейтограмме является Bye.

Дополнительные RR. Если число источников, для которых приводится статистика приема, превышает 31, в первый пакет помещается информация по части источников, остальная часть размещается в следующих RR-пакетах.

SDES. SDES-пакет, содержащий Cname, должен быть включен в каждый составной RTCP-пакет. Другие элементы описания источника могут быть опционно добавлены, если этого требует характер приложения и позволяет пропускная способность используемого канала.

Bye или APP. Другие типы RTCP-пакетов, включая те, которые еще предстоит определить, могут следовать далее в произвольном порядке. Пакет bye, если он присутствует, должен быть последним и содержать SSRC/CSRC. Пакеты одного и того же типа могут повторяться.

Приложение может игнорировать RTCP пакеты неизвестного ему типа. Дополнительныетипы RTCP-пакетов могут быть зарегистрированы IANA (internet assigned numbers authority).

Рис.5 Пример составного пакета RTCP (#: SSRC/CSRC)

Протокол RTP построен так, чтобы позволять приложению изменять число участников от единиц до тысяч. Например, при аудио конференциях информационный поток всегда ограничен (сколько бы не было участников, все они одновременно говорить не могут, так как не смогут ничего понять). Однако, трафик управления таким свойством не обладает. Если доклады о приеме от каждого участника поступают с постоянной частотой, трафик управления будет расти пропорционально числу участников. Следовательно, нужно принимать меры по ограничению трафика.

Для каждой сессии предполагается, что предельно допустимый информационный трафик сессии делится между участниками. Эта полоса пропускания может быть зарезервирована. Полоса не зависит от метода кодирования, но на выбор метода кодирования может оказать влияние имеющаяся в распоряжении полоса пропускания используемого канала. Определенные ограничения на полосу сессии может накладывать конкретное приложение. Вычисления полосы пропускания, необходимой для управления, требует учета издержек транспортных протоколов (например, UDP и IP).

Трафик управления должен быть ограничен малой долей полной полосы пропускания сессии: настолько малой, чтобы не нанести ущерба основной функции транспортного протокола - переносу информации. Предлагается, чтобы доля трафика сессии, выделенная на RTCP была фиксирована на уровне не более 5%. Параметры, определяющие трафик, должны быть

идентичными для всех участников, так чтобы они могли корректно вычислить период рассылки отчетов.

Протокол H.323

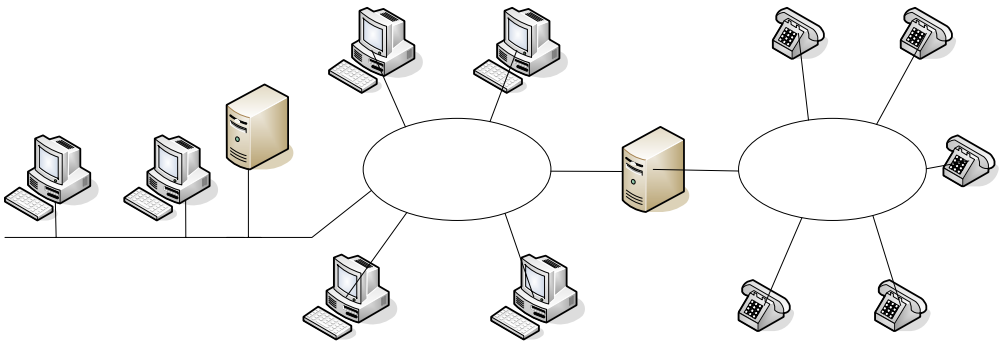

Рис. 6 H323 архитектурная модель для Интернет телефонии

В 1990 году был одобрен первый международный стандарт в области видеоконференцсвязи – спецификация H.320 для поддержки видеоконференций по ISDN. Затем ITU одобрил еще целую серию рекомендаций, относящихся к видеоконференцсвязи. Однако, в отличие от ISDN, IP сети плохо приспособлены для передачи аудио и видеопотоков. Стремление использовать сложившуюся структуру IP сетей привело к появлению в 1996 году стандарта H.323 (Visual Telephone Systems and Terminal Equipment for Local Area Networks which Provide a Non-Guaranteed Quality of Service, Видеотелефоны и терминальное оборудование для локальных сетей с негарантированным качеством обслуживания). В 1998 году была одобрена вторая версия этого стандарта H.323 v.2 (Packet-based multimedia communication systems, Мультимедийные системы связи для сетей с коммутаций пакетов), в сентябре 1999 года была одобрена третья версия рекомендаций, 17 ноября 2001 года была одобрена четвертая версия стандарта H.323. Сейчас H.323 - один из важнейших стандартов из этой серии. H.323 - это рекомендации ITU-T для мультимедийных приложений в вычислительных сетях, не обеспечивающих гарантированное качество обслуживания(QoS).

Рекомендации H.323 предусматривают:

- Управление полосой пропускания
- Возможность взаимодействия сетей
- Платформенную независимость
- Поддержку многоточечных конференций
- Поддержку многоадресной передачи
- Стандарты для кодеков
- Поддержку групповой адресации

В число "объектов" H.323, как они названы в стандарте, включаются терминалы, мультимедиа шлюзы, устройства управления многоточечными конференциями и контроллеры зоны (Привратник) (Gatekeeper).

Терминал - оконечное мультимедийное (голос, видео, данные) устройство, предназначенное для участия в конференции, Вследствие того, что основной

функцией терминала является передача звука, он играет ключевую роль в предоставлении сервиса IP- телефонии. H.323 терминал должен поддерживать следующие протоколы:

H.245 - для согласования параметров соединения;

Q.931 - для установления и контроля соединения;

RAS — для взаимодействия с привратником;

RTP/RTCP — для оптимизации доставки потокового аудио (видео);

семейство протоколов H.450 - для поддержки обязательных в H.323 дополнительных видов обслуживания.

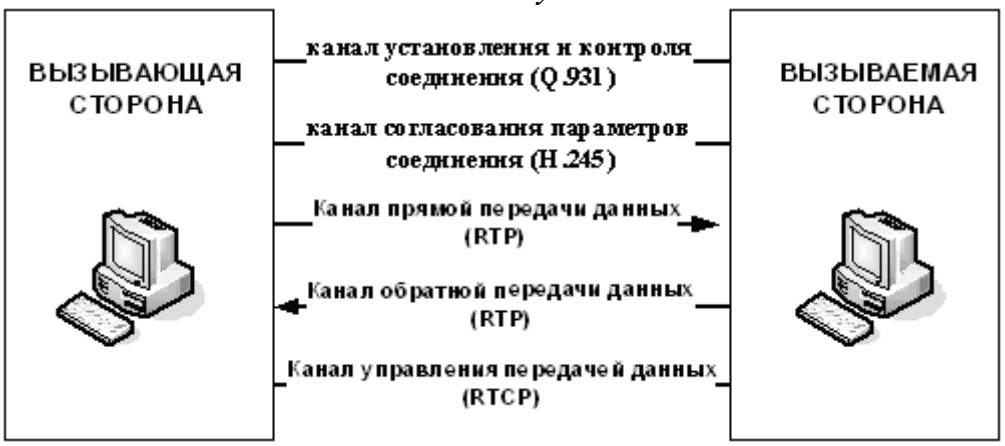

Рис.7 Логические каналы между вызывающей и вызываемой сторонами при установлении связи по протоколу H.323

Дополнительными компонентами могут быть другие аудио- и видеокодеки (H.261, H.263, MPEG).

Мультимедиа шлюз (Gateway) - устройство, предназначенное для преобразования мультимедийной и управляющей информации при сопряжении разнородных сетей. Он необходим только в случае, когда требуется установить соединение с терминалом другого стандарта. Эта связь обеспечивается трансляцией протоколов установки и разрыва соединений, а также форматов передачи данных. Шлюзы H.323 сетей широко применяются в IP телефонии для сопряжения IP сетей и цифровых или аналоговых коммутируемых телефонных сетей.

Устройство управления многоточечными конференциями (Multipoint Control Unit - MCU) - предназначено для организации конференций с участием трех и более участников. Все терминалы, участвующие в конференции, устанавливают соединение с MCU. Сервер управляет ресурсами конференции, согласовывает возможности терминалов по обработке звука и видео, определяет аудио и видеопотоки, которые необходимо направлять по многим адресам. В результате появления стандарта H.323, описывающего механизмы взаимодействия устройств обеспечивающих передачу голоса и видео по IP сетям, появилась возможность объединять в сети устройства различных производителей, что эффективно для сетей специальной связи.

Контроллер зоны (Gatekeeper, Привратник, Конференц-менеджер) - рекомендуемое, но не обязательное устройство, обеспечивающее сетевое управление и исполняющее роль виртуальной телефонной станции.

Выступает в качестве центра обработки вызовов внутри своей зоны и выполняет важнейшие функции управления вызовами. Зона определяется как совокупность всех терминалов, шлюзов и MCU под управлением данного привратника. Привратник необязательный компонент сети H.323, однако, если он присутствует в сети, то терминалы и шлюзы должны использовать его услуги. Основные и дополнительные функции контроллера зоны определены в таблице.

Функции	*Описание*
Основные	
Трансляция адресов	*Преобразование внутренних адресов ЛВС и телефонных номеров формата E.164 в адреса протоколов IP/IPX*
Управление доступом	*Авторизация доступа в H.323 сеть*
Управление полосой пропускания	*Разрешение или запрещение запрашиваемой терминалом полосы пропускания*
Дополнительные	
Управление процессом установления соединения	*При двусторонней конференции привратник способен обрабатывать служебные сообщения протокола сигнализации Q.931, а также может служить ретранслятором таких сообщений от конечных точек.*
Авторизация соединения	*Допускается отклонение привратником запроса на установление соединения. Основания — ограничение прав или времени доступа, и иные, лежащие вне рамок H.323*
Управление вызовами	*Привратник может отслеживать состояние всех активных соединений, что позволяет управлять вызовами, обеспечивая выделение необходимой полосы пропускания и баланс загрузки сетевых ресурсов за счёт переадресации вызовов на другие терминалы и шлюзы.*

Протокол SIP

Протокол SIP, разработан группой MMUSIC (Multiparty Multimedia Session Control) комитета IETF (Internet Engineering Task Force), а спецификации протокола представлены в документе RFC 2543

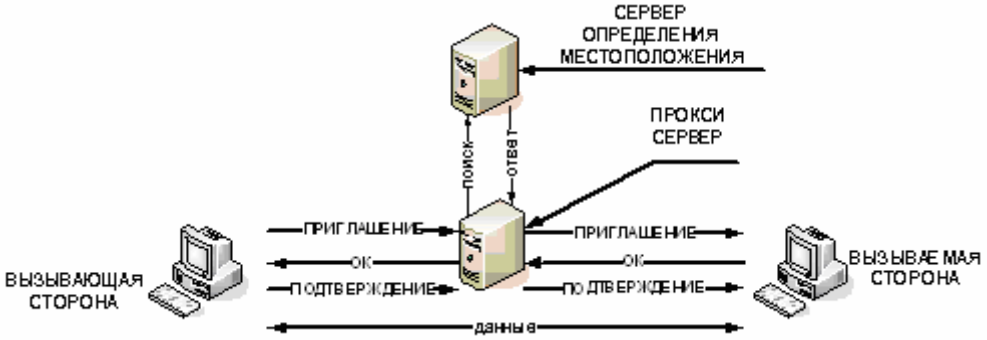

Рис 8 Процедура установления связи по протоколу SIP

Протокол инициирования сеансов - Session Initiation Protocol (SIP)- является протоколом прикладного уровня и предназначается для

организации, модификации и завершения сеансов связи: мультимедийных конференций, телефонных соединений и распределения мультимедийной информации, в основу которого заложены следующие принципы:

Персональная мобильность пользователей.

Пользователи могут перемещаться без ограничений в пределах сети, поэтому услуги связи должны предоставляться им в любом месте этой сети. Пользователю присваивается уникальный идентификатор, а сеть предоставляет ему услуги связи вне зависимости от того, где он находится. Для этого пользователь с помощью специального сообщения - REGISTER - информирует о своих перемещениях сервер определения местоположения.

Масштабируемость сети.

Характеризуется, в первую очередь, возможностью увеличения количества элементов сети при ее расширении. Серверная структура сети, построенной на базе протокола SIP, в полной мере отвечает этому требованию.

Расширяемость протокола.

Характеризуется возможностью дополнения протокола новыми функциями при введении новых услуг и его адаптации к работе с различными приложениями.

Интеграция в стек

существующих протоколов Интернет. Протокол SIP является частью глобальной архитектуры мультимедиа, разработанной комитетом Internet Engineering Task Force (IETF).

Взаимодействие с другими протоколами сигнализации.

Протокол SIP может быть использован совместно с протоколом H.323.

Одной из важнейших особенностей протокола SIP является его независимость от транспортных технологий. Структура сообщений SIP не зависит от выбранной транспортной технологии. Но в то же время предпочтение отдается технологии маршрутизации пакетов IP и протоколу UDP.

Здесь же следует отметить, что сигнальные сообщения могут переноситься не только протоколом транспортного уровня UDP, но и протоколом TCP. По сети с маршрутизацией пакетов IP может передаваться пользовательская информация практически любого вида: речь, видео и данные, а также любая их комбинация, называемая мультимедийной информацией. При организации связи между терминалами пользователей необходимо известить встречную сторону, какого рода информация может приниматься (передаваться), алгоритм ее кодирования и адрес, на который ее следует передавать. Таким образом, одним из обязательных условий организации связи при помощи протокола SIP является обмен между предполагаемыми участниками этой связи данными об их функциональных возможностях. Для этой цели чаще всего используется протокол описания

сеансов связи SDP (Session Description Protocol). В течение сеанса связи может производиться его модификация, поэтому предусмотрена передача средствами SDP сообщений SIP с новыми описаниями сеанса.

Для передачи речевой информации комитет IETF предлагает использовать протокол RTP, но сам протокол SIP не исключает возможность применения для этих целей других протоколов.

Элементы SIP-сети

Сеть SIP содержит следующие основные элементы.

Агент пользователя (User Agent или SIP client) является приложением терминального оборудования и включает в себя две составляющие: клиент агента пользователя (User Agent Client и сервер агента пользователя User Agent Server - UAS. Клиент UAC инициирует SIP-запросы, т.е. выступает в качестве вызывающей стороны. Сервер UAS принимает запросы и отвечает на них, т.е. выступает в качестве вызываемой стороны.

Запросы могут передаваться не прямо адресату, а на некоторый промежуточный узел. Такие узлы бывают двух основных типов: прокси-сервер и сервер переадресации

Прокси-сервер (proxy server) принимает запросы, обрабатывает их и отправляет дальше на следующий сервер, который может быть как другим прокси-сервером, так и последним UAS. Таким образом, прокси-сервер принимает и отправляет запросы и клиента, и сервера. Приняв запрос от UAC, прокси-сервер действует от имени этого UAC.

Существует два вида прокси-серверов: с сохранением состояний (stateful) и без сохранения состояний (stateless). Сервер первого типа хранит в памяти входящий запрос, который явился причиной генерации одного или нескольких исходящих запросов. Эти исходящие запросы сервер также запоминает. Все запросы хранятся в памяти сервера только до окончания транзакции, т.е. до получения ответов на за просы. Сервер без сохранения состояний просто ретранслирует запросы и ответы, которые получает. Он работает быстрее, чем сервер 1-го типа, так как ресурс процессора не тратится на запоминание состояний, вследствие чего сервер этого типа может обслужить большее количество пользователей

Прокси-сервер может модифицировать запросы, которые он переправляет дальше.

Сервер переадресации (redirect server) передает клиенту в ответе на запрос адрес следующего сервера или клиента, с которым первый клиент связывается затем непосредственно. Он не может инициировать собственные запросы. Адрес сообщается первому клиенту в поле Contact сообщений SIP. Таким образом, этот сервер просто выполняет функции поиска текущего адреса пользователя.

Пользователь может перемещаться от одной оконечной системы к другой, так что нужен какой-то метод определения его местоположения. Для этого в SIP используется сервер местоположения (location server) - это база адресов, доступ к которой имеют SIP-серверы, пользующиеся ее услугами для получения информации о возможном местоположении

вызываемого пользователя. Упрощенно базу данных можно представить как совокупность адресных записей, в которых напротив "публикуемого" адреса пользователя его стоит текущий адрес. Приняв запрос, сервер SIP обращается к серверу местоположения, чтобы узнать адрес, по которому можно найти пользователя. В ответ тот сообщает либо список возможных адресов, либо информирует о невозможности найти их. С другой стороны, пользователь информирует SIP-сервер о своем местоположении сообщением REGISTER. Сервер местоположения может располагаться как совместно с SIP-сервером , где могут присутствовать некоторые элементы базы адресов, так и отдельно от него.

Заключение

В данном реферате был дан лишь частичный обзор мультимедийных возможностей современных приложений в сети. В работе мы указали базовые сведения о протоколах RTSP, RTP, RTCP, был дан краткий обзор протоколу H.323.

Основной ценностью потоковых технологий является возможность доставки мультимедиа контента по сетям с коммутацией пакетов. По мере объединения телефонных и пакетных сетей они будут играть все большую роль в повседневной жизни, а распространение технологий широкополосного доступа превратят мечту о просмотре по запросу кинофильмов из различных фильмотек, видеофайлов и других мультимедийных данных в реальность. Поэтому в данном направлении ведутся непрерывные разработки. Постоянно появляются новые приложения и протоколы (причем как фирменные так и стандартизированные такими организациями как ITU-T или IETF)

Список литературы

1. *Куроуз Дж., Росс К. Компьютерные сети. 2-е изд. – СПб.: Питер, 2004. – 765 с.: ил.*
2. *Столингс В. Передача данных. 4-е изд. – СПб.: Питер, 2004. – 750с.: ил.*
3. *Ватолин Д. Ратушняк А., Смирнов М., Юкин В. Методы сжатия данных. Устройство архиваторов, сжатие изображений и видео. М.: Диалог-МИФИ, 2003.-384с.*
4. *Wikipedia (ru.wikipedia.org/h323)*
5. *http://openh323.org*
6. *Рекомендации H.323 (http://www.stel.ru/tech_vc/h323.htm)*
7. *Семенов Ю.А.Протокол IGMP и передача мультимедиа по Интернет (http://book.itep.ru/)*
8. *ПОСТРОЕНИЕ СЕТЕЙ IP-ТЕЛЕФОНИИ НА БАЗЕ ПРОТОКОЛА SIP http://www.dvo.sut.ru/libr/skiri/w133gold/*