Материалы по курсу "Системы TDM- и IP-коммутации в сетях следующего поколения"

№ п/п	Наименование раздела (отдельной темы) дисциплин	Лекции
1.	Переход к ССП	0,5
2.	VoIP	0,5
3.	H.323	1
4.	SIP	1
5.	H.248	1

1. Переход к ССП

Предисловие

Современный этап развития мировой цивилизации характеризуется переходом от индустриального общества к информационному, в котором предполагается наличие новых форм социальной и экономической деятельности, которые базируются на массовом использовании информационных и телекоммуникационных технологий.

Принимая во внимание особенности инфокоммуникационных услуг, перспективные сети связи должны обладать свойствами:

- мультисервисности (независимости технологий предоставления услуг от транспортных технологий);
- широкополосности (возможности гибкого и динамического изменения скорости передачи информации в широком диапазоне);
- мультимедийности (способности передачи многокомпонентной информации (речь, данные, видео, аудио));
- интеллектуальности (возможности управления услугой, вызовом и соединением со стороны пользователя или поставщика услуг);
- инвариантность доступа (возможности организации доступа к услугам независимо от используемой технологии);

- многооператорности (возможности участия нескольких операторов в процессе предоставления услуги и разделения их ответственности в соответствии с их областью деятельности).

Кроме того, при формировании требований к перспективным мультисервисным сетям необходимо учитывать особенности деятельности поставщиков услуг. В частности, современные подходы к регламентации услуг присоединения предусматривают доступ поставщиков услуг, в том числе и не обладающих собственной инфраструктурой, к ресурсам сети общего пользования без дискриминации.

Мультисервисные сети представляют собой самостоятельный класс сетей, строящихся на основе концепции NGN, на базе которых может быть осуществлено предоставление широкого набора как традиционных, так и новых услуг.

Определение мультисервисных сетей как самостоятельного класса означает, что их регламентация должна осуществляться на основе нормативно-технической базы, учитывающей особенности интеграции различных услуг и системно-технических решений в рамках одной сети.

Основные определения, относящиеся к проблематике мультисервисных сетей связи

В Концептуальных положениях по построению мультисервисных сетей на ЕСЭ России используются следующие термины и определения:

Сеть связи следующего поколения (*Next Generation Net, NGN*) – концепция построения сетей связи, обеспечивающих предоставление неограниченного набора услуг с гибкими возможностями по их управлению, персонализации и созданию новых услуг за счет унификации сетевых решений. Предполагает реализацию универсальной транспортной сети с распределенной коммутацией, вынесение функций предоставления услуг в оконечные сетевые узлы и интеграцию с традиционными сетями связи.

Мультисервисная сеть (МС) – это сеть связи, построенная в соответствии с концепцией NGN и обеспечивающая предоставление неограниченного набора услуг.

Мультипротокольная сеть – транспортная сеть связи, входящая в состав мультисервисной сети, обеспечивающая перенос разных видов информации с использованием различных протоколов передачи.

Инфокоммуникационная сеть (ранее применялись также термины “информационная сеть”, “компьютерная сеть” и др.) – это технологическая система, которая включает в себя кроме средств доставки также *средства хранения, обработки и поиска информации* и предназначена для обеспечения пользователей электрической связью и доступом к необходимой им информации.

Процессы *интеграции* и *конвергенции* телекоммуникационной отрасли и средств *информатизации* будут способствовать в период до 2015 г. превращению телекоммуникационных сетей в *инфокоммуникационные сети*.

Сеть доступа (*Access Network, AN*) – сеть связи, обеспечивающая подключение терминальных устройств пользователя к оконечному узлу мультипротокольной сети.

Традиционная сеть связи – существующая сеть связи, такая как ТФОП, СДОП, сеть кабельного телевидения и тому подобные, изначально предназначенная для предоставления услуг связи одного вида.

Инфокоммуникационная услуга (услуга информационного общества) – услуга связи, предполагающая автоматизированную обработку, хранение или предоставление по запросу информации с использованием средств вычислительной техники, как на входящем, так и на исходящем конце соединения.

.

Особенности инфокоммуникационных услуг

К основным технологическим особенностям, отличающим инфокоммуникационные услуги от услуг традиционных сетей связи, можно отнести следующие:

- *инфокоммуникационные услуги* оказываются на верхних уровнях модели ВОС (в то время как услуги связи предоставляются на третьем, сетевом, уровне);
- большинство инфокоммуникационных услуг предполагает наличие клиентской и серверной частей (клиентская часть реализуется в оборудовании пользователя, а серверная – на специальном выделенном узле сети, называемом узлом служб);
- инфокоммуникационные услуги, как правило, предполагают передачу информации мультимедиа, которая характеризуется высокими скоростями передачи и несимметричностью входящего и исходящего информационных потоков;
- для предоставления инфокоммуникационных услуг зачастую необходимы сложные *многоточечные конфигурации соединений*;
- для инфокоммуникационных услуг характерно разнообразие прикладных протоколов и возможностей по управлению услугами со стороны пользователя;
- для идентификации абонентов может использоваться дополнительная адресация в рамках данной инфокоммуникационной услуги.

Большинство инфокоммуникационных услуг являются "приложениями", то есть их функциональность распределена между оборудованием поставщика услуги и оконечным оборудованием пользователя. Как следствие, функции оконечного оборудования также должны быть отнесены к составу инфокомунникационных услуг, что необходимо учитывать при их регламентации.

Бизнес-модель, определяющая участников процесса предоставления инфокоммуникационных услуг и их взаимоотношения, также отличается от модели традиционных услуг электросвязи, в которой было представлено всего лишь три основных участника: оператор, абонент и пользователь. Новая деловая модель предполагает наличие поставщика услуг, который предоставляет инфокоммуникационные услуги абонентам и пользователям. При этом сам поставщик является потребителем услуг переноса, предоставляемых оператором сети связи. На рынке могут также присутствовать дополнительные виды поставщиков услуг: *поставщики информации*, *брокеры*, *ретейлеры* и др.

Поставщик информации предоставляет информацию поставщику услуг для распространения.

Брокер предоставляет информацию о поставщиках услуг и их потенциальных абонентах, содействует пользователям при поиске поставщиков услуг, оказывающих требуемые им услуги.

Ретейлер выступает как посредник между поставщиком услуг и пользователем с целью адаптации услуги к его индивидуальным требованиям.

Конвергенция сетей и услуг

Конвергенция сетей, обусловленная необходимостью одновременной передачи разными категориями пользователей голосовой и видеоинформации в реальном времени, данных, породила две глобальные технические проблемы:

- необходимость поддержки большого разнообразия систем сигнализации, используемых в каждой из объединяемых сетей, базирующихся на технологиях TDM, ATM, IP, MPLS и др.;
- "конвергенция услуг связи" (наряду с "конвергенцией сетей") - ввод новых инфокоммуникационных услуг с универсальным доступом из ССОП, ISDN, интеллектуальной сети (IN), сети IP.

Решение этих задач возлагается на аппаратно-программные средства нового типа: так называемые “программные коммутаторы (Softswitch)” и медиашлюзы (MGW).

Программные коммутаторы (Softswitch) специально создавались для обоих типов сетей (ТфОП и IP), в каждой из них это оборудование воспринимается по-разному:

Для работы в ТфОП Softswitch должен выполнять функции пункта сигнализации ОКС № 7 и иметь интерфейсы для поддержки других систем сигнализации ТфОП/ISDN: EDSS1, 2ВСК, R2 и др.

В сети с коммутацией пакетов Softswitch выступает в качестве единого устройства управления медиашлюзами (Media Gateway Controller, MGC) и/или контроллера

сигнализации (Signaling Controller), диспетчера H.323 (системы видеоконференцсвязи) и сервера SIP (Session Initial Protocol).

Под термином *интеграция* понимают объединение:

- служб (услуг);
- методов коммутации;
- аппаратных или программных средств в единую систему;
- элементной базы средств коммутации и доставки информации.

Конвергенция – это процесс постепенного сближения различных по своему назначению технологий и служб связи с целью унификации оборудования и расширения функциональных возможностей.

Мультисервисность – это поддержка множества служб (service) программно-аппаратными средствами одной сети.

Мультипротокольность – это возможность доставки информации независимо от того, с помощью каких протоколов созданы протокольные блоки данных.

Концепция сетей следующего поколения (NGN)

Общие подходы к построению мультисервисных сетей связи нашли отражение в концепции перспективных сетей связи следующего поколения – NGN.

Базовым принципом концепции NGN является *отделение друг от друга:*

- *функций переноса и коммутации,*
- *функций управления вызовом и управления услугами*.

Функциональная модель NGN, в общем случае, может быть представлена тремя уровнями:

- *транспортным*;
- *управления коммутацией и передачей информации*;
- *управления услугами*.

Задачей транспортного уровня является коммутация и прозрачная передача информации пользователя.

Задачей уровня управления коммутацией и передачей информации является обработка информации сигнализации, маршрутизация вызовов и управление потоками.

Уровень управления услугами содержит функции управления логикой услуг и приложений и представляет собой распределенную вычислительную среду, обеспечивающую:

- предоставление инфокоммуникационных услуг;
- управление услугами;
- создание и внедрение новых услуг;

- взаимодействие различных услуг.

Уровень управления услугами позволяет реализовать специфику услуг и применять одну и ту же программу логики услуги вне зависимости от типа транспортной сети (IP, ATM, FR) и способа доступа. Наличие этого уровня позволяет также вводить на сети любые новые услуги без вмешательства в функционирование других уровней.

Уровень управления услугами может включать множество независимых подсистем ("сетей услуг"), базирующихся на различных технологиях, имеющих своих абонентов и использующих свои, внутренние системы адресации.

2. VoIP

Технология передачи речевой информации по сетям с маршрутизацией пакетов IP - Voice over IP (VoIP) или IP-телефония предусматривает оцифровку, кодирование и компрессию голосового сигнала с последующей передачей по цифровым каналам передачи данных с использованием протокола IP. Частным случаем IP-телефонии является Интернет-телефония, при которой в качестве транспортной сети используется общедоступная сеть Интернет.

Три основных сценария IP-телефонии

Прежде чем обсудить более подробно различные подходы к архитектуре, протоколам и вариантам построения систем и оборудования рассмотрим три наиболее часто используемых на практике сценария IP-телефнии:

*“компьютер-компьютер”;

*“компьютер-телефон”;

*“телефон-телефон”.

Сценарий “компьютер-компьютер” реализуется на базе стандартных персональных компьютеров, оснащенных средствами мультимедиа и подключенных к сети Интернет или другой IP-сети.

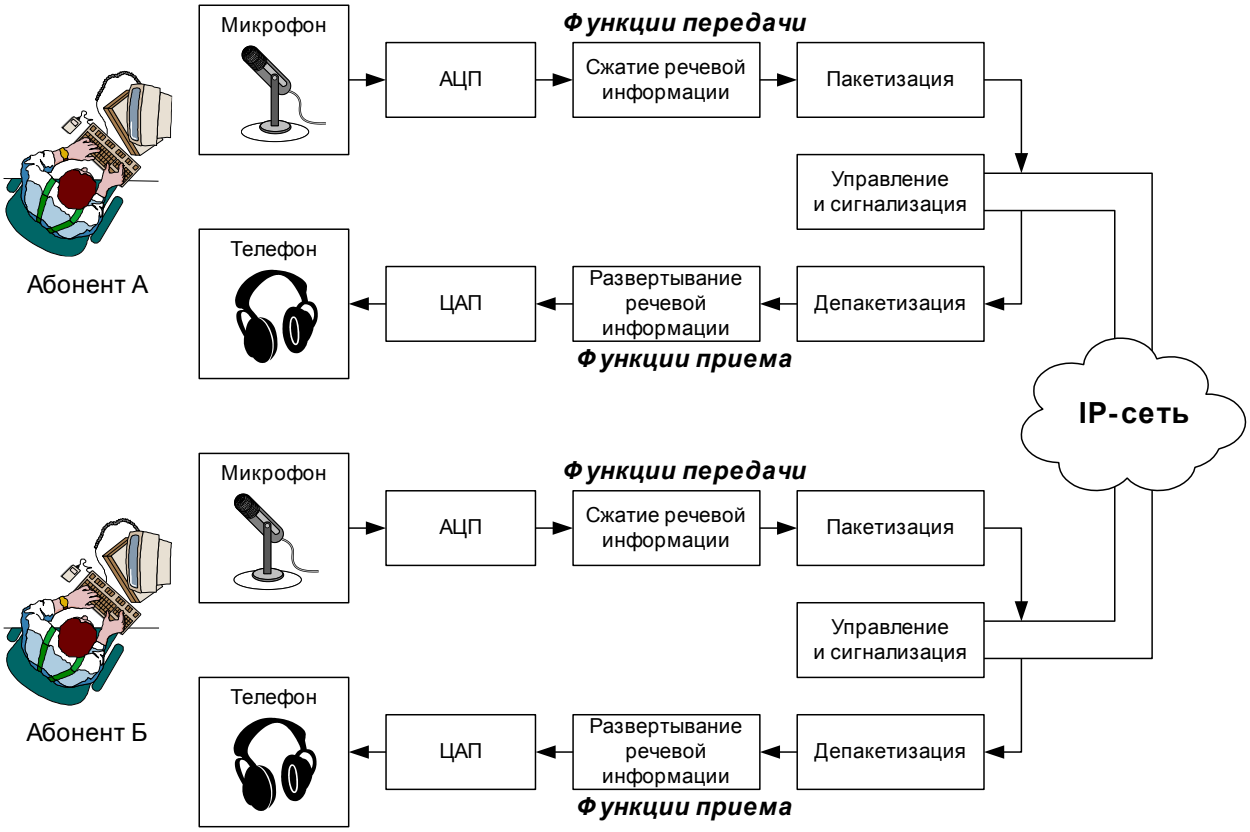

Рис. Сценарий IP-телефонии «компьютер-компьютер»

Компоненты модели IP-телефонии по сценарию «компьютер-компьютер» показаны на рисунке. В этом соединении аналоговые сигналы разговорной речи от микрофона абонента А преобразуются в цифровую форму с помощью аналого-цифрового преобразователя (АЦП). Эти отсчеты речевых данных в цифровой форме затем сжимаются кодирующим устройством для сокращения использования полосы пропускания в 4, 8 или даже 10 раз и. Выходные данные после сжатия снабжаются заголовками протокола IP и других служебных протоколов и полученные таким образом пакеты передаются через IP-сеть в систему IP-телефонии, обслуживающей абонента Б. Когда пакеты принимаются системой абонента Б, заголовки протоколов удаляются и сжатые речевые данные полезной нагрузки посылаются в декодирующее устройство, после чего речевые данные снова преобразуются в аналоговую форму с помощью цифроаналогового преобразователя (ЦАП) и попадают в телефон (гарнитуру, наушники, колонки) абонента Б. Для обычного вызова с двумя абонентами, системы IP-телефонии на каждом конце одновременно реализуют как функции передачи, так и функции приема.

Название сценария «компьютер – компьютер» отнюдь не означает, что у пользователя в распоряжении обязательно должен находиться стандартный ПК с

микрофоном и колонками. Главным требованием для такой схемы является то, что оба пользователя должны иметь подключенные к IP-сети интеллектуальные терминалы. К ним можно отнести мультимедийные компьютеры со специализированным программным обеспечением, IP-телефоны, сотовые телефоны 3G.

В противовес «компьютеру» будем использовать термин «телефон» - оконечное оборудование пользователя, включаемое в сеть коммутации каналов любого типа: ТфОП, ISDN или GSM.

Следующий сценарий “телефон-компьютер” находит применение в различного рода справочно-информационных службах Интернет, в службах сбыта товаров или в сервисных службах технической поддержки. Существует две модификации этого сценария IP-телефонии:

- от компьютера (пользователя IP-сети) к телефону (абоненту ТфОП), в частности, в связи с предоставлением пользователям IP-сетей доступа к телефонным речевым услугам, в том числе к справочно-информационным услугам и услугам Интеллектуальной сети;
- от абонента ТфОП к пользователю IP-сети с идентификацией вызываемой стороны на основе нумерации по E.164 или IP-адресации.

В первом из упомянутых сценариев «компьютер – телефон» соединение устанавливается между пользователем IP-сети и пользователем сети коммутации каналов. Предполагается, что установление соединения инициируется пользователем IP-сети.

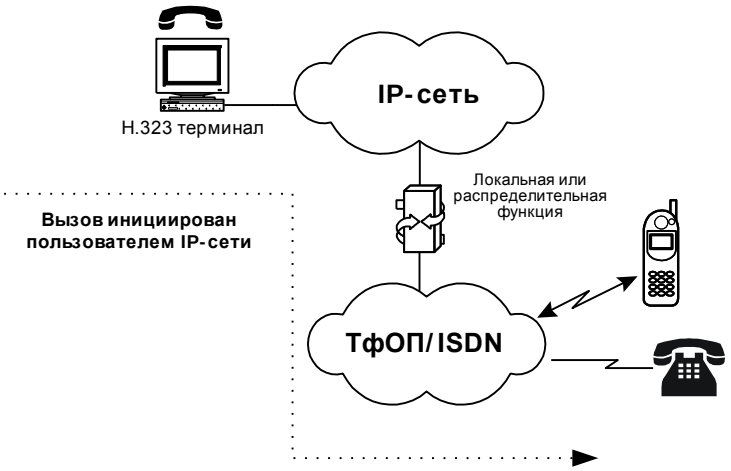

Рис. Вызов абонента ТфОП пользователем IP-сети по сценарию «компьютер – телефон»

Шлюз (GW) для взаимодействия сетей ТфОП и IP может быть реализован в отдельном устройстве или интегрирован в существующее оборудование ТфОП или IP-сети.

В соответствие со второй модификацией сценария «компьютер – телефон» соединение устанавливается между пользователем IP-сети и абонентом ТфОП, но инициирует установление абонент ТфОП.

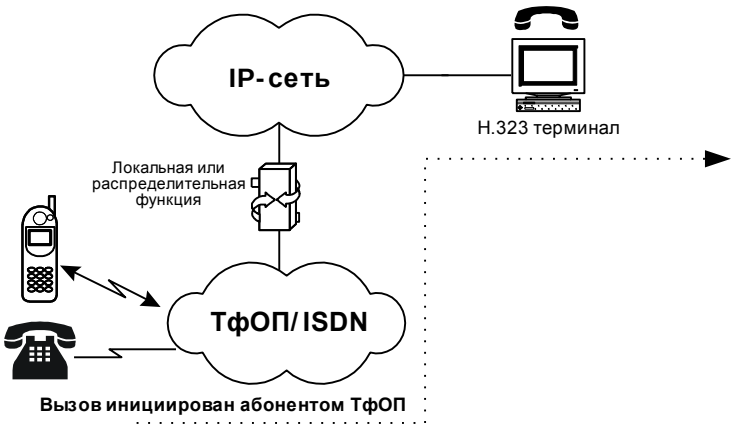

Рис. Пользователя IP-сети вызывает абонент ТФОП по сценарию «компьютер – телефон»

Сценарий “телефон-телефон” в значительной степени отличается от остальных сценариев IP-телефонии по его социальной значимости, поскольку целью его применения является предоставление обычным абонентам ТфОП альтернативной междугородной и международной телефонной связи. Типичная услуга IP-телефонии по сценарию “телефон-телефон» использует стандартный телефон в качестве интерфейса пользователя. Благодаря маршрутизации телефонного трафика по IP-сети стало возможным обходить сети общего пользования операторов и, соответственно, не платить за вызовы по этим сетям.

Как показано на рисунке, провайдеры услуг IP-телефонии предоставляют услуги “телефон-телефон” путём установки шлюзов IP-телефонии на входе и выходе IP-сетей. Их абоненты подключаются к шлюзу провайдера через сеть с коммутацией каналов (ТфОП, ISDN, GSM.

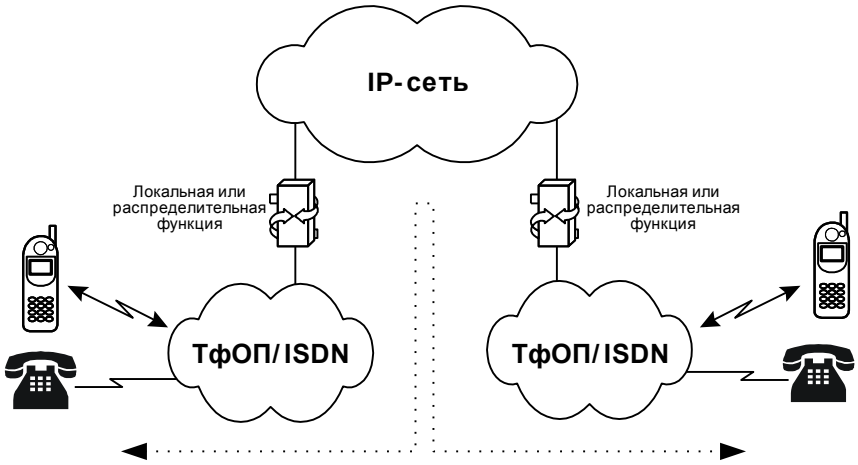

Рис.Соединение абонентов ТфОП через транзитную IP-сеть по сценарию «телефон-телефон»

Особенности передачи речи по IP-сети

Если проблемы ограничения задержки и подавления эха в традиционной телефонии существовали всегда, а при переходе к IP-сетям лишь усугубились, то потери информации (пакетов) и стохастический характер задержки породили совершенно новые проблемы, решение которых сопряжено с большими трудностями. Этим объясняется тот факт, что понадобился длительный период развития сетевых технологий, прежде чем появились коммерческие приложения IP-телефонии.

Задержки в IP-сетях

При передаче речи по IP-сети возникают намного большие, чем в ТфОП, задержки, которые к тому же, изменяются случайным образом. Задержка определяется как промежуток времени, затрачиваемый на то, чтобы речевой сигнал прошел расстояние от говорящего до слушающего. Покажем, что и как оказывает влияние на количественные характеристики этого промежутка времени.

Влияние сети.

Во-первых, неустойчиво и плохо предсказуемо время прохождения пакета через сеть. Если нагрузка сети относительно мала, маршрутизаторы и коммутаторы, безусловно, могут обрабатывать пакеты практически мгновенно, а линии связи бывают доступны почти всегда. Если загрузка сети относительно велика, пакеты могут довольно долго ожидать обслуживания в очередях. Чем больше маршрутизаторов, коммутаторов и линий в маршруте, по которому проходит пакет, тем больше время его запаздывания, и тем больше вариация этого времени, т.е. *джиттер*.

Влияние операционной системы.

Большинство приложений IP-телефонии (особенно клиентских), представляет собой обычные программы, выполняемые в среде какой-либо операционной системы, такой как Windows или Linux. Большинство операционных систем не может контролировать распределение времени центрального процессора между разными процессами с точностью, превышающей несколько десятков миллисекунд, и не может обрабатывать за такое же время более одного прерывания от внешних устройств. Это приводит к тому, что задержка в продвижении данных между сетевым интерфейсом и внешним устройством речевого вывода составляет, независимо от используемого алгоритма кодирования речи, величину такого же порядка, или даже больше.

Из сказанного следует, что выбор операционной системы является важным фактором, влияющим на общую величину задержки. Чтобы минимизировать влияние операционной системы, некоторые производители шлюзов и IP-телефонов используют так называемые ОС реального времени (VxWorks, pSOS, QNX Neutrino и т.д.) или перекладывают все функции, которые необходимо выполнять в жестких временных рамках, на отдельный быстродействующий специализированный процессор.

Влияние джиттер-буфера.

Проблема джиттера весьма существенна в пакетно-ориентированных сетях. Отправитель речевых пакетов передает их через фиксированные промежутки времени (например, через каждые 20 мс), но при прохождении через сеть задержки пакетов оказываются неодинаковыми, так что они прибывают в пункт назначения через разные промежутки времени. Это иллюстрирует рис. 3.1.

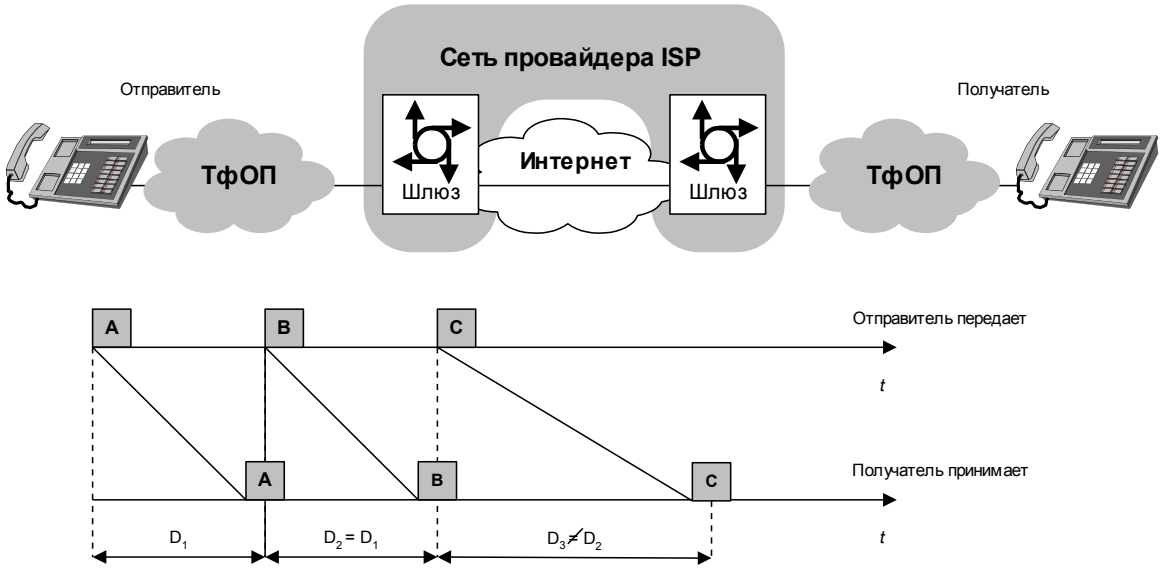

Рис. Различие интервалов между моментами прибытия пакетов (джиттер)

Для того, чтобы компенсировать влияние джиттера, в терминалах используется т.н. *джиттер-буфер*. Этот буфер хранит в памяти прибывшие пакеты в течение времени, определяемого его емкостью (длиной). Пакеты, прибывающие слишком поздно, когда буфер заполнен, отбрасываются. Время воспроизведения определяется на основе значений временных меток, выставляемых специальным протоколом RTP. В функции джиттер-буфера обычно входит и восстановление исходной очередности следования пакетов, если при транспортировке по сети они оказались «перепутаны».

Слишком короткий буфер будет приводить к слишком частым потерям «опоздавших» пакетов, а слишком длинный – к неприемлемо большой дополнительной задержке. Обычно предусматривается динамическая подстройка длины буфера в течение всего времени существования соединения. Для выбора наилучшей длины используются эвристические алгоритмы.

Влияние кодека и количества передаваемых в пакете кадров.

Большинство современных эффективных алгоритмов кодирования/декодирования речи ориентировано на передачу информации кадрами, а не последовательностью кодов отдельных отсчетов. Поэтому в течение времени, определяемого длиной кадра кодека, должна накапливаться определенной длины последовательность кодов отсчетов. Кроме того, некоторым кодекам необходим предварительный анализ большего количества кодов речевой информации, чем должно содержаться в кадре. Это неизбежное время накопления и предварительного анализа входит в общий бюджет длительности задержки пакета.

На первый взгляд, можно было бы заключить, что чем меньше длина кадра, тем меньше должна быть задержка. Однако, как будет показано ниже, из-за значительного объема служебной информации, передаваемой в RTP/UDP/IP-пакетах (заголовки IP – 20 байтов, UDP – 8 байтов, RTP – 12 байтов), передача маленьких порций данных очень неэффективна, так что при применении кодеков с малой длиной кадра приходится упаковывать несколько кадров в один пакет. Кроме того, кодеки с большей длиной кадра более эффективны, поскольку могут «наблюдать» сигнал в течение большего времени и, следовательно, могут более эффективно сжимать этот сигнал.

ITU-T в рекомендации G.114 определил требования к качеству передачи речи. Оно считается хорошим, если сквозная задержка при передаче сигнала в одну сторону не превышает 150 мс. Современное оборудование IP-телефонии при прямом соединении друг с другом вносит задержку порядка 60-70 мс. Таким образом, остается еще около 90 мс на сетевую задержку при передаче IP-пакета от отправителя к пункту назначения, что

говорит о возможности обеспечить при современном уровне технологии передачу речи с достаточно хорошим качеством.

Эхо

Феномен эха вызывает затруднения при разговоре и у говорящего, и у слушающего. Говорящий слышит, с определенной задержкой, свой собственный голос. Если сигнал отражается дважды, то слушающий дважды слышит речь говорящего (второй раз - с ослаблением и задержкой).

Эхо может иметь электрическую и акустическую природу и характерно как для сетей ТфОП, так и для сетей IP-телефонии.

Существуют два типа устройств, предназначенных для ограничения вредных эффектов эха: эхозаградители и эхокомпенсаторы.

Эхозаградители появились в начале 70-х годов. Принцип их работы прост и состоит в отключении канала передачи, когда в канале приема присутствует речевой сигнал, т.е. связь, по сути, становится полудуплексной.

Эхокомпенсатор – это более сложное устройство, которое моделирует эхосигнал для последующего его вычитания из принимаемого сигнала. Эхокомпенсаторы являются неотъемлемой частью шлюзов IP-телефонии.

Принципы кодирования речи в IP-телефонии

Для того, чтобы передать речь через телефонную проводную сеть, речевую информацию нужно преобразовать в аналоговый электрический сигнал. При переходе к цифровым сетям связи возникла необходимость преобразовать аналоговый электрический сигнал в цифровой формат на передающей стороне, и перевести обратно в аналоговую форму на приемной стороне. При передачи речи по сетям IP телефонии используют ряд механизмов, позволяющих эффективно передавать речь по сети, используя минимум полосы пропускания.

Использование полосы пропускания канала.

Скорость передачи, которую предусматривают имеющиеся сегодня узкополосные кодеки, лежит в пределах 1.2 – 64 Кбит/с. Естественно, что от этого параметра прямо зависит качество воспроизводимой речи. Существует множество подходов к проблеме определения качества. Наиболее широко используемый подход оперирует оценкой MOS (Mean Opinion Score), которая определяется для конкретного кодека как средняя оценка качества большой группой слушателей по пятибалльной шкале. Для прослушивания

экспертам предъявляются разные звуковые фрагменты – речь, музыка, речь на фоне различного шума и т.д. Оценки интерпретируют следующим образом:

- ***4-5*** - высокое качество; аналогично качеству передачи речи в ISDN, или еще выше.
- **3.5-4** - качество ТфОП (toll quality); аналогично качеству речи, передаваемой с помощью кодека ADPCM при скорости 32 Кбит/с. Такое качество обычно обеспечивается при большинстве телефонных разговоров. Мобильные сети обеспечивают качество чуть ниже toll quality.
- ***3-3.5*** - качество речи, по-прежнему, удовлетворительно, однако его ухудшение хорошо заметно на слух.
- ***2.5-3*** – речь разборчива, однако требует концентрации внимания для понимания. Такое качество обычно обеспечивается в системах связи специального применения (например, в вооруженных силах).

В рамках существующих технологий качество ТфОП (toll quality) невозможно обеспечить при скоростях менее 5 Кбит/с.

Подавление периодов молчания (VAD, CNG, DTX).

При диалоге один его участник говорит, в среднем, только 35 процентов времени. Таким образом, если применить алгоритмы, которые позволяют уменьшить объем информации, передаваемой в периоды молчания, то можно значительно сузить необходимую полосу пропускания. В двустороннем разговоре такие меры позволяют достичь сокращения объема передаваемой информации до 50%, а в децентрализованных многоадресных конференциях (за счет большего количества говорящих) - и более. Технология подавления таких периодов имеет три важные составляющие.

Нужно отметить, что определение границ пауз в речи очень существенно для эффективной синхронизации передающей и приемной сторон: приемник может, незначительно изменяя длительности пауз, производить подстройку скорости воспроизведения для каждого отдельного сеанса связи, что исключает необходимость синхронизации тактовых генераторов всех элементов сети, как это имеет место в ТфОП.

Детектор речевой активности (Voice Activity Detector – VAD) необходим для определения периодов времени, когда пользователь говорит. Детектор VAD должен обладать малым временем реакции, чтобы не допускать потерь начальных слов и не упускать бесполезные фрагменты молчания в конце предложений; в то же время детектор VAD не должен срабатывать от воздействия фонового шума.

Детектор VAD оценивает энергию входного сигнала и, если она превышает некоторый порог, активизирует передачу. Если бы детектор отбрасывал всю информацию

до момента, пока энергия сигнала не стала выше порога, то происходило бы клиппирование начальной части периода активности. Поэтому реализации VAD требуют сохранения в памяти нескольких миллисекунд информации, чтобы иметь возможность запустить передачу до начала периода активности. Это увеличивает, в некоторой степени, задержку прохождения сигнала.

Прерывистая передача (Discontinuous Transmission - DTX) позволяет кодеку прекратить передачу пакетов в тот момент, когда VAD обнаружил период молчания. Некоторые наиболее совершенные кодеры не прекращают передачу полностью, а переходят в режим передачи гораздо меньшего объема информации (интенсивность, спектральные характеристики), нужной для того, чтобы декодер на удаленном конце мог восстановить фоновый шум.

Генератор комфортного шума (Comfort Noise Generator - CNG) служит для генерации фонового шума. В момент, когда в речи активного участника беседы начинается период молчания, терминалы слушающих могут просто отключить воспроизведение звука. Однако это было бы неразумно. Если в трубке возникает «гробовая тишина», т.е. фоновый шум (шум улицы и т.д.), который был слышен во время разговора, внезапно исчезает, то слушающему кажется, что соединение по каким-то причинам нарушилось, и он обычно начинает спрашивать, слышит ли его собеседник.

Генератор CNG позволяет избежать таких неприятных эффектов. Простейшие кодеки просто прекращают передачу в период молчания, и декодер генерирует какой-либо шум с уровнем, равным минимальному уровню, отмеченному в период речевой активности. Более совершенные кодеки (G.723.1 Annex A, G.729 Annex B) имеют возможность предоставлять удаленному декодеру информацию для восстановления шума с параметрами, близкими к фактически наблюдавшимся.

Чувствительность к потерям кадров. Потери пакетов являются неотъемлемым атрибутом IP-сетей. Так как пакеты содержат кадры, сформированные кодеком, то это вызывает потери кадров. Однако потери пакетов и потери кадров не обязательно напрямую связаны между собой, так как существуют подходы (такие как применение кодов с исправлением ошибок), позволяющие уменьшить число потерянных кадров при данном числе потерянных пакетов. Требующаяся для этого дополнительная служебная информация распределяется между несколькими пакетами, так что при потере некоторого числа пакетов кадры могут быть восстановлены.

Кодеки, стандартизованные ITU-T

Кодек G.711

Кодек G.711 - «дедушка» всех цифровых кодеков речевых сигналов, был одобрен ITU-T в 1965 году. Типичная оценка MOS составляет 4.2. В первую очередь отметим, что, как и для ТфОП, минимально необходимым для оборудования VoIP является ИКМ-кодирование G.711.

Кодек G.723.1

Рекомендация G.723.1 утверждена ITU-T в ноябре 1995 года. Форум IMTC выбрал кодек G.723.1 как базовый для приложений IP-телефонии.

Предусмотрено два режима работы: 6.4 Кбит/с (кадр имеет размер 189 битов, дополненных до 24 байтов) и 5.3 Кбит/с (кадр имеет размер 158 битов, дополненных до 20 байтов). Режим работы может меняться динамически от кадра к кадру. Оба режима обязательны для реализации.

Оценка MOS составляет 3.7 в режиме 6.4 Кбит/с и 3.9 в режиме 5.3 Кбит/с.

Кодек G.723.1 имеет детектор речевой активности и обеспечивает генерацию комфортного шума на удаленном конце в период молчания.

Кодек G.726

Кодек G.726 обеспечивает кодирование цифрового потока со скоростью 40, 32, 24 или 16 Кбит/с, гарантируя оценки MOS на уровне 4.3 (32 Кбит/с), что часто принимается за эталон уровня качества телефонной связи (toll quality). В приложениях IP-телефонии этот кодек практически не используется, так как он не обеспечивает достаточной устойчивости к потерям информации.

Кодек G.728

Кодек G.728 использует оригинальную технологию с малой задержкой и гарантирует оценки MOS, аналогичные G.726 при скорости передачи 16 Кбит/с.

Недостатком алгоритма является высокая сложность (требовательность к вычислительной мощности) и относительно высокая чувствительность к потерям кадров.

Кодек G.729

Кодек G.729 очень популярен в приложениях передачи речи по сетям Frame Relay. Кодек использует кадр длительностью 10 мс и обеспечивает скорость передачи 8 Кбит/с. Для кодера необходим предварительный анализ сигнала продолжительностью 5 мс.

Существуют два варианта кодека:

- G.729 одобрен ITU-T в декабре 1996
- Упрощенный вариант G.729A одобрен ITU-T в ноябре 1995

В спецификациях G.729 определены алгоритмы VAD, CNG и DTX. В периоды молчания кодер передает кадры с информацией о фоновом шуме, если только шумовая обстановка изменяется.

3. H.323

Архитектура сети H.323

Первой рекомендацией для построения сетей IP-телефонии стала рекомендация H.323 Международного союза электросвязи (ITU-T). H.323 является первой зонтичной спецификацией систем мультимедийной связи для работы в сетях с коммутацией пакетов, не обеспечивающих гарантированное качество обслуживания.

Так как ITU-T исторически занимался проблемами телефонных сетей, то и предложенная рекомендация была в большей степени ориентирована на передачу телефонного трафика по сети с коммутацией пакетов. Сети, построенные на базе протоколов H.323, ориентированы на интеграцию с телефонными сетями и могут рассматриваться как сети ISDN, наложенные на сети передачи данных. В частности, процедура установления соединения в таких сетях IP-телефонии базируется на рекомендации ITU-T Q.931 и практически идентична той же процедуре в сетях ISDN.

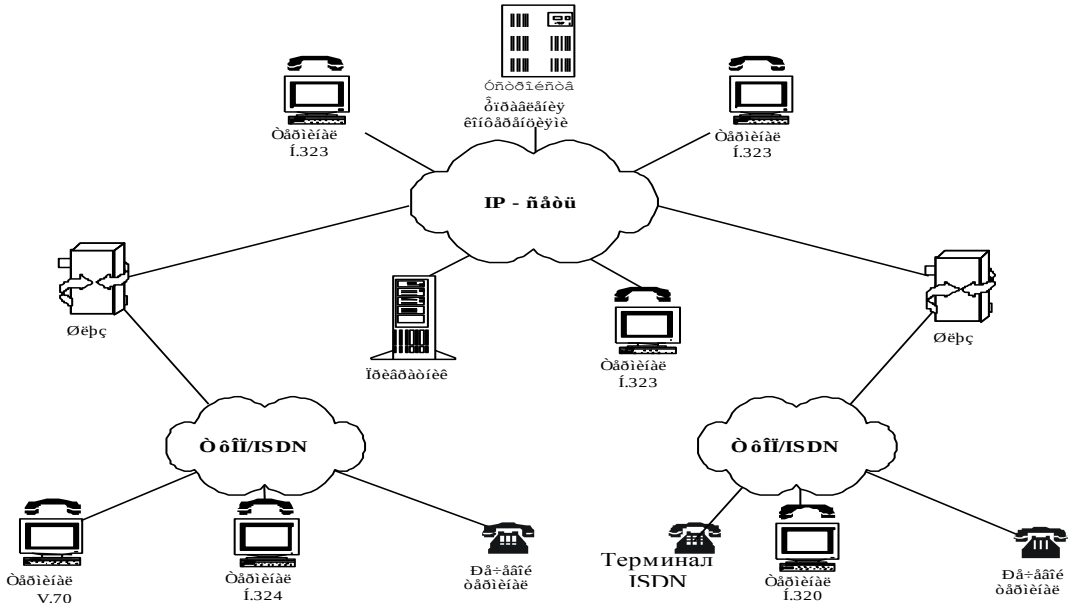

Рис. Архитектура сети H.323

Основными устройствами сети являются: терминал, шлюз, привратник и устройство управления конференциями. Необходимо отметить, что в отличие от

устройств ТфОП, устройства Н.323 не имеют жестко закрепленного места в сети. Устройства подключаются в любую точку IP-сети. Однако при этом сеть Н.323 разбивается на зоны, а каждой зоной управляет привратник.

Терминал Н.323

Терминал Н.323 - это оконечное устройство сети IP-телефонии, обеспечивающее двухстороннюю речевую или мультимедийную связь с другим терминалом, шлюзом или устройством управления конференциями (

.

Шлюз Н.323

Шлюз является соединяющим мостом между ТфОП и IP. Основной функцией шлюза является преобразование речевой (мультимедийной) информации, поступающей со стороны ТФОП с постоянной скоростью, в вид, пригодный для передачи по IP-сетям, т.е. кодирование информации, подавление пауз в разговоре, упаковку информации в пакеты RTP/UDP/IP, а также обратное преобразование. Кроме того, шлюз должен уметь поддерживать обмен сигнальными сообщениями как с коммутационным или терминальным оборудованием ТфОП, так и с привратником или оконечным устройством сети Н.323. Таким образом, шлюз должен преобразовывать аналоговую абонентскую сигнализацию, сигнализацию по 2ВСК и сообщения систем сигнализации DSS1 и ОКС7 в сигнальные сообщения Н.323.

При отсутствии в сети привратника должна быть реализована еще одна функция шлюза – преобразование номера ТфОП в транспортный адрес IP-сети.

Со стороны сетей с маршрутизацией пакетов IP, так же, как и со стороны ТфОП, шлюз может участвовать в соединениях в качестве терминала или устройства управления конференциями. Шлюз может сначала участвовать в соединении в качестве терминала, а затем, при помощи сигнализации Н.245, продолжить работу в качестве устройства управления конференциями. Очевидно, что в случае, когда терминал Н.323 связывается с другим терминалом Н.323, расположенным в той же самой IP-сети, шлюз в этой связи не участвует.

Привратник

В привратнике сосредоточен интеллект сетей IP-телефонии, базирующихся на рекомендации ITU H.323. Привратник выполняет функции управления зоной сети IP-телефонии, в которую входят терминалы, шлюзы и блоки конференций, зарегистрированные у этого привратника.

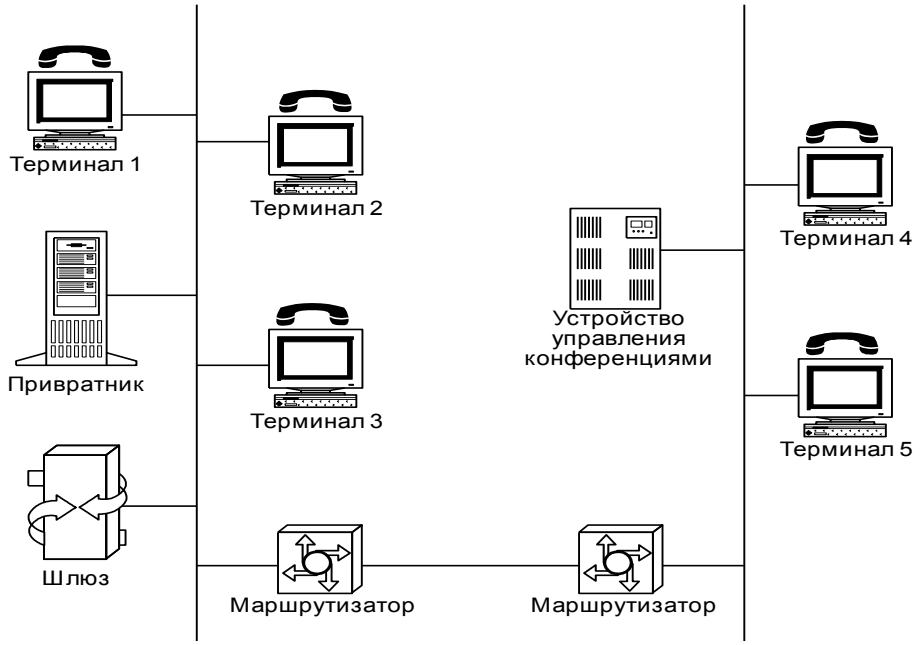

Рис.Зона сети H.323

В число наиболее важных функций, выполняемых привратником, входят:

- преобразование так называемого *alias*-адреса (имени абонента, телефонного номера, адреса электронной почты и др.) в транспортный адрес сетей с маршрутизацией пакетов IP (IP-адрес и номер порта TCP);
- контроль доступа пользователей системы к услугам IP-телефонии при помощи сигнализации RAS (используются сообщения ARQ/ACF/ARJ);
- контроль, управление и резервирование пропускной способности сети;
- маршрутизация сигнальных сообщений между терминалами, расположенными в одной зоне; привратник может организовывать сигнальный канал непосредственно между терминалами или ретранслировать сигнальные сообщения от одного терминала к другому.

Привратник также обеспечивает мобильность абонентов, т.е. способность пользователя получить доступ к услугам с любого терминала в любом месте сети и способность сети идентифицировать пользователей при их перемещении из одного места в другое.

Устройство управления конференциями

Одна из дополнительных услуг IP-телефонии, возможность организации конференций. Рекомендация H.323 предусматривает три вида конференции (рис.1.5).

Первый вид – централизованная конференция, в которой оконечные устройства соединяются в режиме «точка-точка» с устройством управления конференциями (MCU), контролирующим процесс создания и завершения конференции, а также обрабатывающим потоки пользовательской информации.

Второй вид – децентрализованная конференция, в которой каждый ее участник соединяется с остальными участниками в режиме «точка-группа точек», и оконечные устройства сами обрабатывают (переключают или смешивают) потоки информации, поступающие от других участников конференции.

Третий вид – смешанная конференция, т.е. комбинация двух предыдущих видов.

Преимущество централизованной конференции - сравнительно простые требования к терминальному оборудованию, недостаток – большая стоимость устройства управления конференциями.

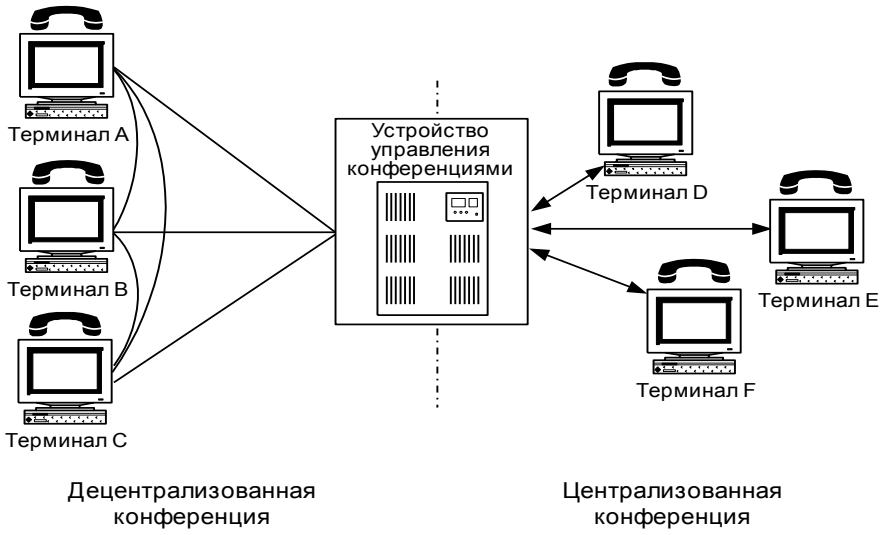

Рис. Разные виды конференции в сети H.323

Для децентрализованной конференции требуется более сложное терминальное оборудование; кроме того, желательно, чтобы в сети поддерживалась передача пакетов IP в режиме многоадресной рассылки (IP multicasting). H.323 в современных сетях

Протоколы H.323

В H.323 входит три основных протокола: протокол взаимодействия оконечного оборудования с привратником – RAS (Registration, Admission and Status), протокол управления соединениями - H.225 и протокол управления логическими каналами - H.245.

Протокол RAS

ITU-T в Рекомендации H.225.0 определил протокол взаимодействия компонентов сети H.323 – оконечного оборудования (терминалов, шлюзов, устройств управления конференциями) с привратником. Этот протокол получил название RAS (Registration, Admission and Status). Основными процедурами, выполняемыми оконечным оборудованием и привратником с помощью протокола RAS, являются:

- обнаружение привратника;
- регистрация оконечного оборудования у привратника;
- контроль доступа оконечного оборудования к сетевым ресурсам;
- определение местоположения оконечного оборудования в сети;
- изменение полосы пропускания в процессе обслуживания вызова;
- опрос и индикация текущего состояния оконечного оборудования;
- оповещение привратника об освобождении полосы пропускания, ранее занимавшейся оборудованием.

Выполнение первых трех процедур, предусмотренных протоколом RAS, является начальной фазой установления соединения с использованием сигнализации H.323. Далее следуют фаза сигнализации H.225.0 (Q.931) и обмен управляющими сообщениями H.245. Разъединение происходит в обратной последовательности: в первую очередь закрываются управляющий канал H.245 и сигнальный канал H.225.0, после чего по каналу RAS привратник оповещается об освобождении ранее занятой оконечным оборудованием полосы пропускания.

Выполнение всех перечисленных выше процедур осуществляется с помощью пар сообщений, специализированных для каждой из процедур. Для переноса сообщений протокола RAS используется протокол негарантированной доставки информации UDP.

Сигнальный протокол H.225.0

Процедуры управления соединениями в сетях H.323 специфицированы ITU-T в рекомендации H.225.0. Эти процедуры предусматривают использование в базовом процессе обслуживания вызова сигнальных сообщений Q.931.

Сообщение *Setup* передается вызывающим оборудованием с целью установить соединение. Это сообщение передается на TCP порт 1720 вызываемого оборудования.

Сообщение *Call Proceeding* передается к вызывающему оборудованию, чтобы известить его о том, что вызов принят к обслуживанию.

Сообщение *Alerting* передается к вызывающему оборудованию и информирует его о том, что вызываемое оборудование не занято и что вызываемому пользователю подается сигнал о входящем вызове.

Сообщение *Connect* передается к вызывающему оборудованию и информирует его о том, что вызываемый пользователь принял входящий вызов. Сообщение *Connect* может содержать транспортный адрес управляющего канала H.245.

Сообщение *Release Complete* передается вызывающим или вызываемым оборудованием с целью разрушить соединение. Это сообщение передается только в том случае, если открыт сигнальный канал.

Сообщение Q.932 *Facility* используется для обращения к дополнительным услугам в соответствии с рекомендациями ITU-T H.450.x.

Транспортировку сигнальных сообщений обеспечивает протокол с установлением соединения и с гарантированной доставкой информации TCP.

Сценарий установления соединения схож с аналогичным сценарием в сетях ISDN, рассмотрим успешное установление соединения.

Управляющий протокол H.245

В рекомендации ITU-T H.245 определен ряд независимых процедур, которые должны выполняться для управления информационными каналами:

- определения ведущего и ведомого устройств (Master/slave determination);
- обмена данными о функциональных возможностях (Capability Exchange);
- открытия и закрытия однонаправленных логических каналов (Open/Close Logical Channel Signalling);
- открытия и закрытия двунаправленных логических каналов (Open/Close Bidirectional Logical Channel Signalling);
- определения задержки, возникающей при передаче информации от источника к приемнику и в обратном направлении (Round Trip Delay Determination);

- выбора режима обработки информации (Mode Request);
- сигнализации по петле, создаваемой для целей технического обслуживания оборудования (Maintenance Loop Signalling).

Для выполнения вышеуказанных процедур между оконечными устройствами (или между оконечным оборудованием и устройством управления конференциями или привратником) организуется управляющий канал H.245. При этом оконечное оборудование должно открывать один (и только один) управляющий канал для каждого соединения, в котором оно участвует. Примечательно, что терминалы, устройства управления конференциями, шлюзы и привратники могут участвовать одновременно в нескольких соединениях и, следовательно, открывать несколько управляющих каналов.

4. SIP

Построение сетей IP-телефонии на базе протокола SIP

Функциональные возможности протокола

Вторым вариантом построения сетей стал протокол SIP, разработанный группой MMUSIC (Multiparty Multimedia Session Control) комитета IETF (Internet Engineering Task Force), а спецификации протокола представлены в документе RFC 2543

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.

SIP (Session Initiation Protocol) предназначен для организации, модификации и прекращения сеансов связи: мультимедийных конференций, телефонных соединений и распределения мультимедийной информации.

В основу протокола 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 её 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, разработанных IETF. 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. Возможно также взаимодействие протокола SIP с системами сигнализации ТфОП - DSS1 и ОКС7.

Одной из важнейших особенностей протокола SIP является его независимость от транспортных технологий.

Адресация SIP

Для того чтобы вызвать кого-то, необходимо знать его адрес или хотя бы имя. В сети Интернет для нахождения хоста используется URL (для SIP он обозначается как SIP URL). В качестве адреса в SIP выбран самый распространенный тип – адрес электронной почты. Он уже сейчас является основным адресом, не зависящим от местоположения пользователя.

Есть четыре основные формы адреса: «*имя@домен*», «*имя@хост*», «*имя@IP-адрес*», «*№телефона@шлюз*».

Адрес состоит из двух частей. Первая – это та часть, в которой указывается адрес домена, хоста или шлюза. Она может быть представлена и alias-адресом; тогда, чтобы найти IP-адрес, необходимо обратиться к сервису системы DNS. Если же здесь помещен IP-адрес, то никакого преобразования не надо, так как в этом случае достаточно напрямую связаться с адресатом.

Вторая часть адреса – это имя пользователя в домене или на хосте. Если в первой части указан адрес шлюза, то вторая часть представлена телефонным номером абонента в глобальной или частной системе нумерации.

В начале адреса SIP ставятся слово ’sip:’, указывающее, что это именно SIP-адрес, так как бывают другие (например, ‘mailto’).

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 – UAC) и сервер агента пользователя (User Agent Server – UAS), иначе называемые просто *клиент* и *сервер*. 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, поэтому он содержит обе составляющие – и ‘клиент' и ‘сервер’. 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 запросы. Сервер без сохранения состояний просто ретранслирует запросы и ответы, которые получает. Он работает быстрее, чем сервер первого 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. Проще говоря, пользователь отсылает требование установить соединение на прокси-сервер, а тот сам «заботится» о том, чтобы оно было установлено.

Прокси-сервер может размножать запрос и передавать его по разным направлениям, чтобы запрос достиг нескольких мест, в надежде на то, что нужный пользователь окажется в одном из них.

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 её услугами для получения информации о возможном местоположении вызываемого пользователя. Принципы работы сервера местоположения

не регламентированы документом RFC 2543, но там имеются примеры протоколов, которые могут использоваться для этого: LDAP (RFC 1777), rwnois (RFC 2167) и др. Упрощенно базу данных можно представить себе 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.

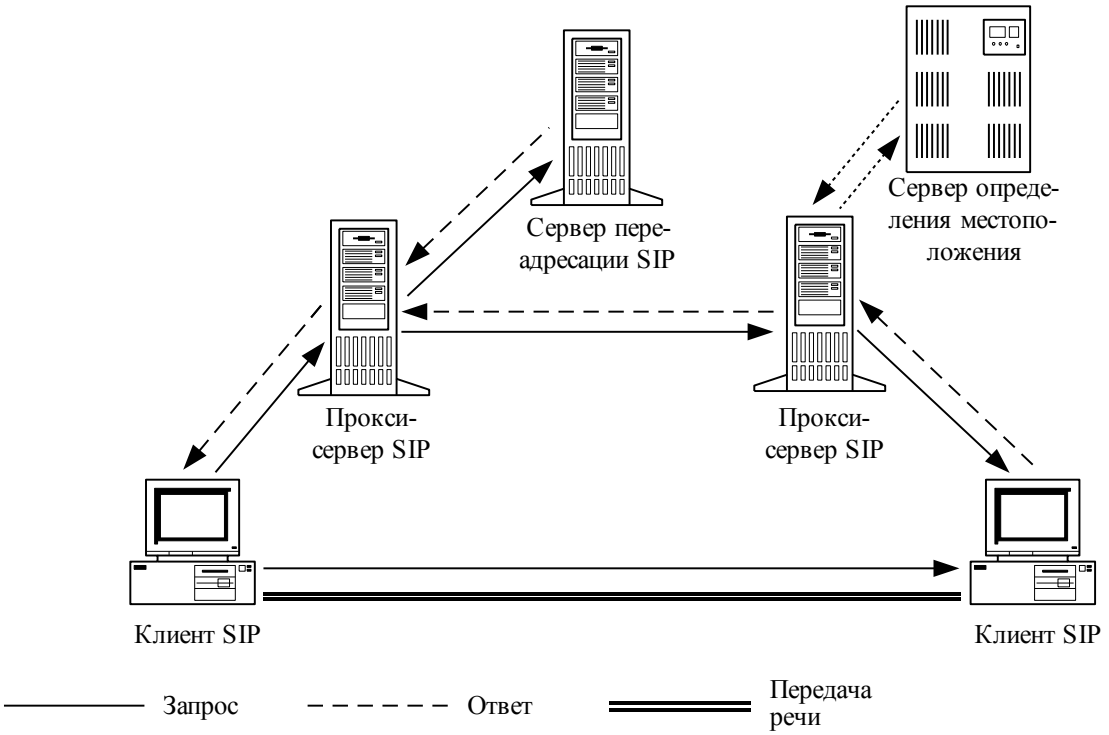

Рис. Архитектура SIP-сети

Сообщения SIP

Структура сообщений

Согласно архитектуре «клиент-сервер» все сообщения делятся на запросы, передаваемые от клиента к серверу, и на ответы сервера клиенту.

Например, чтобы инициировать установление соединения, вызывающий пользователь должен сообщить серверу ряд параметров, в частности, адрес вызываемого пользователя, параметры информационных каналов и др. Эти параметры передаются в специальном SIP-запросе. От вызываемого пользователя к вызывающему передается ответ на запрос, также содержащий ряд параметров.

Вся информация, необходимая для установления соединения, помещается в заголовке. Это может быть, например, адрес вызываемого и вызывающего пользователей, пройденный сообщением путь, размер тела сообщения. О типе заголовка и содержащейся в нем информации можно узнать по его имени. Оно всегда начинается с прописной буквы, за которой следуют строчные. Некоторые заголовки используются во всех сообщениях, а некоторые – только в определенных случаях.

Примеры и смысл наиболее часто встречаемых заголовков.

Call-ID – уникальный идентификатор отдельного сеанса связи или регистрации отдельного клиента; он подобен метке соединения (call reference) в DSS-1. Назначается стороной, которая инициирует вызов. Содержит буквенно-числовое значение и имя хоста, разделенные символом @:

2345call@rts.loniis.ru

To – определяет получателя запроса; кроме SIP-адреса, здесь может присутствовать параметр 'tag' для идентификации пользователя или услуги, находящихся на одном SIP URL. Если необходим визуальный вывод имени пользователя, например, на дисплей, его также можно поместить в поле **To**:

the director <userA@loniis.ru> tag=12345.

From – определяет отправителя запроса; по организации аналогичен полю To.

CSeq – уникальный идентификатор запроса внутри одного **Call-ID**, он необходим для того, чтобы отличить, на какой запрос прошел ответ, так как в некоторых случаях он может оказаться ответом на другой запрос; состоит из двух частей: натурального числа в диапазоне от 1 до 2^32 и названия типа запроса.

Via – запрос может проходить через несколько прокси-серверов, каждый из которых принимает, обрабатывает и направляет его на следующий прокси-сервер, пока сообщение не достигнет конечного UAS. Поле **Via** показывает путь, пройденный запросом; каждый прокси-сервер добавляет это поле со своим адресом. Это необходимо для обнаружения колец, т.е. когда сообщение ходит в сети по кругу и не передается дальше, а также в случаях, когда необходимо, чтобы запросы и ответы обязательно проходили по одному и тому же пути (например, в случае использования firewall).

Content-Type – определяет формат описания сеанса связи. Само описание сеанса, например, в формате протокола SDP включается в тело сообщения.

Content-Length – показывает размер тела сообщения.

Запросы

С помощью запросов клиент сообщает о текущем местоположении, приглашает пользователей принять участие в сеансах связи, модифицирует уже установленные

сеансы, завершает их и т.д. Сервер определяет тип принятого запроса по названию, указанному в стартовой строке. В той же строке в поле **Request-URI** указан SIP-адрес вызываемого пользователя. Описание основных запросов приведено ниже.

INVITE – приглашает пользователя принять участие в сеансе связи. Он обычно содержит описание сеанса связи, где указывается вид принимаемой информации и параметры (список возможных вариантов параметров), необходимые для приема информации, и может указываться вид информации, который вызываемый пользователь желает передавать. В ответе на запрос INVITE указывается вид информации, которая будет приниматься вызываемым пользователем, и может указываться вид информации, которую вызываемый пользователь собирается передавать

ACK – подтверждает прием от вызываемой стороны ответа на команду INVITE и завершает транзакцию.

OPTIONS –позволяет получить информацию о функциональных возможностях пользовательских агентов и сетевых серверов. Однако этот запрос не используется для организации сеансов связи.

BYE – используется вызывавшей и вызванной сторонами для разрушения соединения. Перед тем как разрушить соединение, пользовательские агенты отправляют этот запрос к серверу, сообщая о намерении прекратить сеанс связи.

CANCEL – позволяет пользовательским агентам и сетевым серверам отменить любой ранее переданный запрос, если финальный ответ на него (т.е. ответ с номерами 2xx, 3xx, 4xx, 5xx, 6xx) еще не был получен.

REGISTER –применяется клиентами для регистрации данных о местоположении с использованием серверов SIP.

Ответы

После приема и интерпретации запроса, адресат (прокси-сервер) передает ответ на этот запрос. Содержание ответов бывает разным: подтверждение установления соединения, передача запрошенной информации, сведения о неисправностях и т.д. Структуру ответов и их типы протокол SIP унаследовал от протокола HTTP.

Определено шесть типов ответов, несущих разную функциональную нагрузку. Тип ответа кодируется 3-х значным числом. Самой важной является первая цифра, которая определяет класс ответа, остальные две цифры лишь дополняют первую. В некоторых случаях оборудование даже может не знать все коды ответов, но оно обязательно должно знать, как интерпретировать первую цифру.

Все ответы делятся на две группы: информационные и финальные. Информационные ответы показывают, что запрос находится в стадии обработки. Финальные ответы

кодируются 3-хзначными числами, начинающимися с цифр 2, 3, 4, 5 и 6: они означают завершение обработки запроса и содержат, когда это нужно, результат обработки запроса. Смысл первых цифр такой:

1xx – (информационный) – запрос принят, продолжается его обработка;

2xx – (успех) - запрос принят, понят и успешно обработан;

3xx – (переадресация) – для завершения обработки запроса нужны дальнейшие действия;

4xx – (ошибка клиента) – запрос содержит ошибку и не может быть выполнен;

5xx – (ошибка сервера) – сервер не может выполнить явно правильный запрос;

6xx – (глобальный сбой) – запрос не может быть обработан никаким сервером.

5. H.248

Принцип декомпозиции шлюза.

Архитектура распределённого шлюза

Ещё одним вариантом построения сетей IP-телефонии является распределённый шлюз. Сейчас он реализован в последних версиях H.323, может применяться совместно с протоколом SIP, а также существует в виде отдельных стандартных технологий.

Принцип декомпозиции шлюзов – это сетевая архитектура, предусматривающая разбиение шлюза IP-телефонии на структурные элементы.

Упомянутый принцип декомпозиции шлюза делит его на следующие функциональные блоки:

- транспортный шлюз - Media Gateway, который выполняет функции преобразования речевой информации, поступающей со стороны ТФОП с постоянной скоростью, в вид, пригодный для передачи по сетям с маршрутизацией пакетов IP: кодирование и упаковку речевой информации в пакеты RTP/UDP/IP, а также обратное преобразование;
- устройство управления шлюзом – Media Gateway Controller, руководящее работой шлюза и контролирующего его; в практических реализациях протокола MGCP функции MGC выполняет оборудование Softswitch;
- шлюз сигнализации - Signaling Gateway, который обеспечивает доставку сигнальной информации, поступающей со стороны ТфОП, к устройству управления шлюзом и перенос сигнальной информации в обратном направлении.

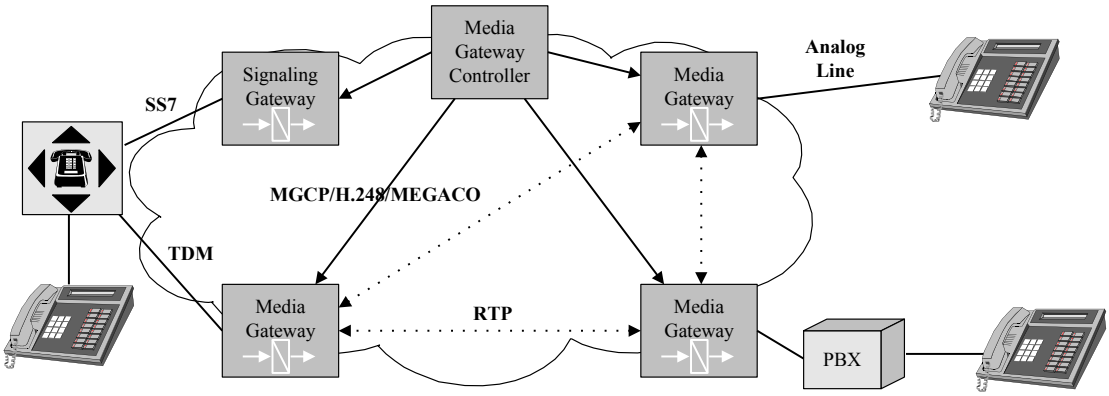

Рис. Архитектура сети, базирующейся на протоколе управления шлюзами

Таким образом, весь интеллект функционально распределенного шлюза размещается в устройстве управления. Шлюз сигнализации выполняет функции STP – транзитного пункта системы сигнализации по общему каналу - ОКС7 или функции конвертера других систем сигнализации, кроме CAS-сигнализации. Если распределенный шлюз подключается к ТфОП при помощи сигнализации по выделенным сигнальным каналам (CAS), то сигнальная информация вместе с пользовательской информацией сначала поступает в транспортный шлюз, а затем передается оттуда в устройство управления без посредничества шлюза сигнализации. Транспортные шлюзы выполняют только функции преобразования речевой информации. Одно устройство управления обслуживает одновременно несколько шлюзов. В сети может присутствовать несколько устройств управления. Предполагается, что эти устройства синхронизованы между собой и согласованно управляют шлюзами, участвующими в соединении.

Модель процесса обслуживания вызова MEGACO/H.248

При описании алгоритма установления соединения с использованием протокола MEGACO комитет IETF опирается на специальную модель процесса обслуживания вызова. Протокол MEGACO оперирует с двумя логическими сущностями внутри транспортного шлюза: окончание (termination) и контекст (context), которыми может управлять контроллер шлюза. Пример модели процесса обслуживания вызова приведен на Рис.

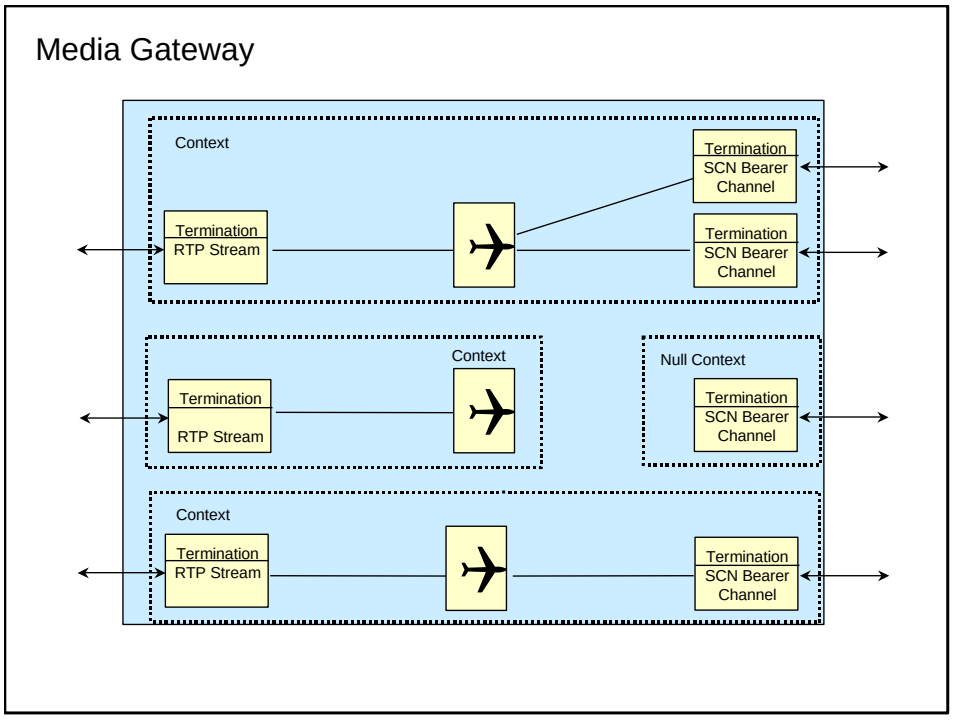

Рис. Примеры модели процесса обслуживания вызова

Окончания (Terminations)

Окончания (также в русскоязычной литературе часто встречается термин *порты*) являются источниками и приемниками медиа-информации. Они являются логическими объектами медиа-шлюза. Можно выделить два вида окончаний в зависимости от того, какой они представляют интерфейс физический или виртуальный. Физические окончания, существуют полупостоянно с момента конфигурации шлюза, это аналоговые телефонные интерфейсы оборудования, поддерживающие одно телефонное соединение, или цифровые каналы. Виртуальные окончания, существующие только в течение разговорной сессии, являются интерфейсами со стороны IP сети (например, RTP-окончания), через которые ведутся передача и прием пакетов.

Виртуальные окончания создаются шлюзом при получении от контроллера команды Add и ликвидируются при получении команды Subtract, тогда как физические окончания при получении команды Add или Subtract, соответственно, выводятся из нулевого контекста или возвращаются обратно в нулевой контекст.

Окончание имеет уникальный идентификатор (TerminationID), который назначается шлюзом при конфигурации порта. Идентификаторы физических окончаний формируются в MG, например, идентификатором порта может служить номер тракта E1 и номер временного канала внутри тракта. Иногда команды могут относиться ко всему шлюзу, тогда используется общий идентификатор окончаний (TerminationID) - “Root”.

Окончания обладают рядом свойств (properties), каждое из которых имеет уникальный идентификатор (propertyID). Например, окончания могут обладать способностью генерировать речевые подсказки, акустические и вызывные сигналы и подсказки, а также выявлять сигналы DTMF.

При создании окончаний некоторые свойства присваиваются им по умолчанию. При помощи протокола MEGACO контроллер может изменять свойства окончаний шлюза. Свойства окончаний группируются в дескрипторы, которые включаются в команды управления окончаниями.

Окончания, как уже говорилось, могут генерировать и выдавать сигналы, при этом говорят, что сигнал применён на окончании. Окончания могут быть запрограммированы на обнаружение событий, при возникновении которых MG должен будет отослать извещение контроллеру или выполнить определённые действия. На окончании может накапливаться статистика и потом выдаваться по запросу контроллера и при удалении окончания из контекста.

5.1.1. Контекст (Context)

Контекст – это отображение связи между несколькими окончаниями, то есть абстрактное представление соединения двух или более портов (физических и/или виртуальных) одного шлюза. В любой момент времени окончание может относиться только к одному контексту, который имеет свой уникальный идентификатор. Существует особый вид контекста – нулевой. Все окончания, входящие в нулевой контекст, не связаны ни между собой, ни с другими портами. Например, абстрактным представлением свободного (не занятого) канала в модели соединений является окончание в нулевом контексте.

В общем случае для присоединения окончания к контексту служит команда Add. При этом, если контроллер не специфицирует существующий контекст, к которому должен быть доставлен порт, то шлюз создает новый контекст. Удаление окончания из контекста производится командой Subtract. Перемещение окончания из одного контекста в другой производится командой Move.

Максимальное количество окончаний, включённых в контекст, ограничивается возможностями шлюза. Если он поддерживает только соединения точка-точка, то их будет всего два.

Атрибутами контекста являются

- Идентификатор контекста ContextID

- Топология контекста (кто кому передаёт и от кого принимает информацию). Топология контекста описывает потоки информации внутри контекста, т.е. внутри шлюза, в то время как подобный параметр окончания - режим работы окончания, описывает внешние потоки шлюза, входящие и исходящие.
- Приоритет используется для того, чтобы указать шлюзу на первоочерёдную важность обслуживания контекста. Система приоритетов включает 16 уровней, изменяющихся от низшего нулевого до наивысшего 15-го.
- Индикатор «аварийного вызова» позволяет получить высший приоритет в обслуживании.

Протокол имеет средства, чтобы управлять параметрами контекста. Удаление контекста происходит автоматически после исключения из него последнего окончания.

Сообщения протокола H.248/MEGACO

Дескрипторы

Рассмотрение структуры информационных элементов протокола мы начнём от наименьших к наибольшим, чтобы было понятно, что из чего состоит.

Параметры команд H.248 сгруппированы в объекты, которые называются дескрипторами. Дескриптор состоит из названия и списка элементов. Некоторые элементы могут иметь численные значения. Многие команды содержат общие дескрипторы, то есть конкретный дескриптор может встречаться в нескольких разных командах. Общий вид дескрипторов можно представить следующим образом:

Название дескриптора = <Идентификатор ID> {*параметр = значение, параметр = значение…*}.

Не все команды должны обязательно содержать те или иные дескрипторы, в ряде команд дескрипторы лишь опциональны.

Определённые в протоколе дескрипторы перечислены в таблице.

Название дескриптора	**Описание**
Modem	Идентифицирует тип и параметры модема
Mux	Описывает тип мультиплексирования информации, используемый мультимедийными терминалами, например, H.221, H.223, H.225.0
Media	Специфицирует параметры информационного потока

TerminationState	Специфицирует свойства порта шлюза. Дескриптор содержит два параметра. Параметр ServiceStates описывает статус порта (работает в тестовом режиме - test, находится в нерабочем состоянии - out of service, по умолчанию указывается, что порт работает в нормальном режиме - in service). Параметр BufferedEventProcessingMode описывает реакцию шлюза на событие, о котором не надо немедленно оповещать контроллер. Определены две реакции на событие: игнорировать или обработать.
Stream	Включает в себя ряд дескрипторов (Remote, Local, LocalControl, Signals, Events), специфицирующих параметры отдельного двунаправленного информационного потока
Local	Содержит параметры, описывающие информационный поток, передаваемый или принимаемый локальным шлюзом. Информация, содержащаяся в этом дескрипторе, переносится от одного шлюза к другому.
Remote	Содержит параметры, описывающие информационный поток, передаваемый или принимаемый удаленным шлюзом. Информация, содержащаяся в этом дескрипторе, переносится от одного шлюза к другому.
LocalControl	Содержит параметр Mode – режим работы и ряд свойств порта. Параметр Mode может принимать значения send-only, receive-only, send/receive, inactive, loop-back и delete. Дескриптор передается на участке между шлюзом и контролером.
Events	Определяет события, которые шлюз должен отслеживать, и реакцию на эти события. Определены следующие реакции: NotifyAction (известить контроллер), Accumulate (сохранить информацию о событии в буфере), AccumulateByDigitMap (накопить цифры номера в соответствии с планом нумерации), KeepActive (известить контроллер, и продолжить передачу сигнала).
Signals	Описывает сигналы конечному пользователю, передачу которых порт шлюза должен начать или прекратить.
Audit	Содержит информацию (в виде ряда дескрипторов), которую

	контроллер запрашивает у шлюза. Посылается в командах AuditValue и AuditCapabilities.
Packages	Описывает совокупность свойств порта, передается в команде AuditValue
DigitMap	При помощи этого дескриптора контроллер информирует шлюз об используемом плане нумерации
ServiceChange	Содержит информацию, относящуюся к изменению состояния порта шлюза, такую как причина, метод изменения и др.
ObservedEvents	Содержит информацию о произошедших событиях. Передается в командах Notify и AuditValue.
Statistics	Содержит статистическую информацию, собранную портом за время соединения.
Extension	Позволяет передавать информацию, не специфицированную в протоколе

По умолчанию значения всех дескрипторов, за исключением дескриптора состояния окончания и дескриптора местного управления, устанавливаются пустыми (т.е. без значений).

Дескрипторы, как следует из названия – это некие «описатели», которые содержат значения параметров, присваиваемых окончаниям, контекстам или всему шлюзу.

Команды

Команды протокола обеспечивают управление логическими единицами модели обслуживания вызова – контекстами и окончаниями. Команды позволяют управлять свойствами контекстов и окончаний. Большинство команд могут передаваться только контроллером, за исключением команд Notify и ServiceChange. Приведём полный список используемых команд.

Команда	Направление передачи	Назначение
Add (Добавить)	MGC - > MG	Контроллер дает указание шлюзу добавить окончание к контексту.
Modify (Изменить)	MGC - > MG	Контроллер дает указание шлюзу изменить свойства окончания.
Subtract (Отключить)	MGC - > MG	Контроллер изымает окончание из контекста.
Move (Переместить)	MGC - > MG	Контроллер переводит окончание из одного контекста в другой в одно действие.
AuditValue	MGC - > MG	Контроллер запрашивает свойства

(Проверить окончание)		окончания, произошедшие события или сигналы, передаваемые в канал, а также статистику, собранную на текущий момент времени.
AuditCapabilities (Проверить возможности окончания)	MGC - > MG	Контроллер запрашивает возможные значения свойств окончания, список событий, которые могут быть выявленные портом, список сигналов, которые окончание может посылать в канал, статические данные.
Notify (Уведомить)	MG - > MGG	Шлюз информирует контроллер о произошедших событиях.
ServiceChange (Рестарт)	MGC - > MG, MG - > MGG	Шлюз информирует контроллер о том, что одно или несколько окончаний выходят из рабочего состояния или возвращаются в рабочее состояние. Контроллер может предписать окончанию или группе окончаний выйти из обслуживания или вернуться в обслуживание.

Транзакции

Команды, передаваемые между MGC и MG группируются в транзакции, каждая из которых снабжается идентификатором TransactionID, необходимом для соотнесения запросов и ответов транзакций. Транзакция состоит из одного или более Действий. Действие состоит из серии команд, указаний модифицировать или проверить (выдать) свойства контекста, причём область всех этих операций должен ограничиваться одним контекстом. На приводимом рисунке изображена иерархия транзакций, действий и команд.

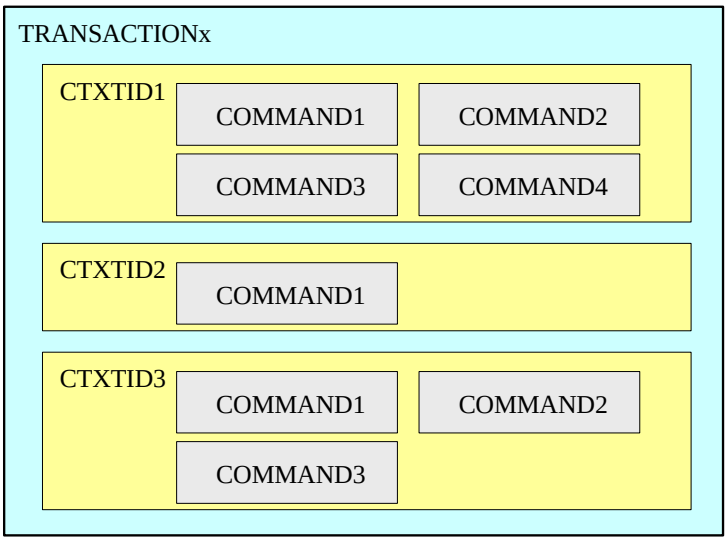

Рис. Иерархия в пределах транзакции

Сообщения

Несколько транзакций протокола могут помещаться в его сообщение. Сообщение снабжается заголовком, определяющим отправителя. Идентификатор сообщения (Message Identifier – MID) устанавливается равным назначенному имени (например доменному адресу/ доменному имени/ имени устройства) объекта, передающего сообщение. По умолчанию предлагается использовать доменное имя. Сообщение H.248 – это, по сути, только транспортный механизм, в отличие от сообщений многих других сетевых протоколов, имеющих собственные функции. Общая структура сообщения представлена на следующем рисунке.

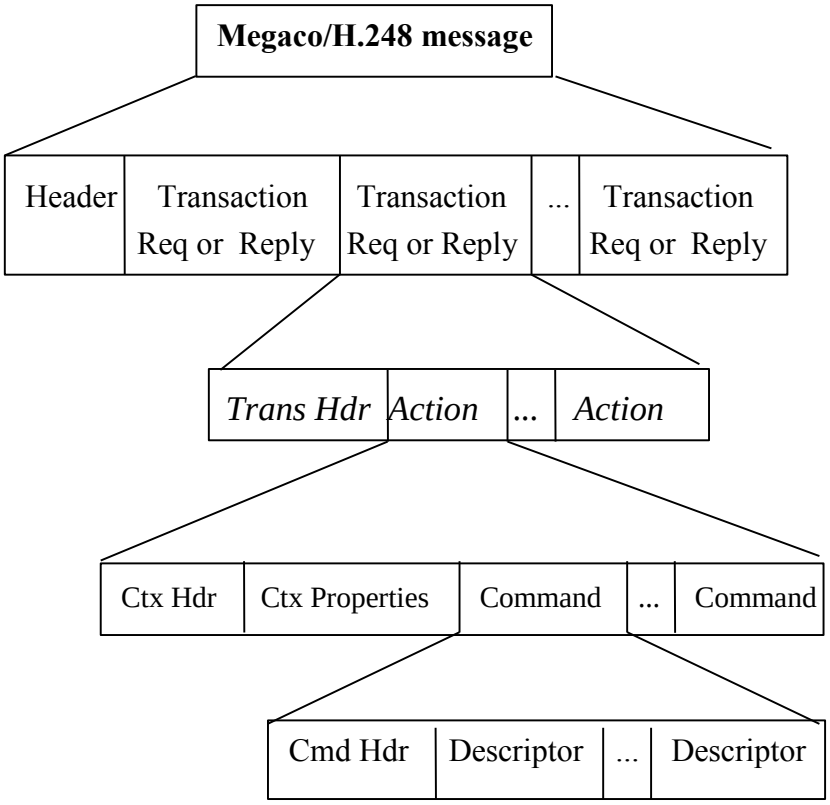

Рис. Структура сообщений H.248/MEGACO