СОДЕРЖАНИЕ

ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ

ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ «САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ им. проф. М.А. БОНЧ-БРУЕВИЧА»

А.А. Атцик
А.Б. Гольдштейн
В.В. Саморезов

IP-КОММУНИКАЦИИ В NGN

Рекомендовано УМО по образованию в области телекоммуникаций в качестве учебного пособия по специальности 210406 «Сети связи и системы коммутации»

САНКТ-ПЕТЕРБУРГ
2007

УДК 621.391:681.324
ББК 388я73
А92

Рецензенты:

В.И. Исаев – кандидат технических наук, профессор (СПбГУТ)
Н.А. Соколов – кандидат технических наук, профессор (СПбГУТ)

Атцик А.А., Гольдштейн А.Б., Саморезов В.В.
А92 IP-коммуникации в NGN: учебное пособие (спец. 210406) / ГОУВПО СПбГУТ. – СПб, 2007.

Излагаются теоретические основы, приводятся конкретные задания для практических занятий и лабораторных работ по сетевым аспектам, протоколам H.323, H.248 и SIP, сценариям взаимодействия, вариантам реализации IP-коммуникаций в NGN.

УДК 621.391:681.324
ББК 388я73

ЛИТЕРАТУРА

1. *Гольдштейн, Б.С.* IP-телефония / Б.С. Гольдштейн, А.В. Пинчук, А.Л. Суховицкий. – М.: Радио и связь, 2005.

2. ITU-T Recommendation H.225.0. Call signaling protocols and media stream packetization for packet-based multimedia communication systems. – Geneva, 1998.

3. ITU-T Recommendation H.245. Control protocol for multimedia communication. – Geneva, 1998.

4. ITU-T Recommendation H.323. Packet based multimedia communication systems. – Geneva, 1998.

5. RFC 2543. SIP: Session Initiation Protocol. – M. Handley, 1999.

6. *Гольдштейн, А.Б.* Softswitch / А.Б. Гольдштейн, Б.С. Гольдштейн.– СПб: БХВ, 2006.

ВВЕДЕНИЕ

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

К настоящему моменту IP-телефония прошла три этапа развития протокола сигнализации: *докоммерческий* (1980–1995), *компьютерный* (1995–1999), и начавшийся на рубеже веков *инфокоммуникационный,* продолжающийся и сегодня.

Докоммерческий этап характеризовался научно-исследовательской деятельностью в различных университетах и исследовательских организациях сообщества Интернет. Исторически первая попытка IP-телефонии была осуществлена уже в 1983 г. в Кембридже (Массачусетс).

Компьютерный этап был начат израильской компанией VocalTec, сумевшей к 1995 г. собрать воедино достижения в областях цифровых сигнальных процессоров (DSP), кодеков, компьютеров, протоколов. Первоначально, продукты VocalTec позволяли пользователям организовывать только соединения PC – PC. Все функции сигнализации и управления реализовывались непосредственно в этих PC, а программное обеспечение сеансов связи все еще ориентировалось на нестандартные протоколы разных компаний производителей. Но уже в июне 1996 г. 16-я Исследовательская комиссия Международного союза электросвязи (ITU-T) согласовала версию первого протокола H.323, названную стандартом для видеоконференц-связи через локальную вычислительную сеть с негарантированным качеством обслуживания (QoS). Этот первый «зонтичный» стандарт IP-телефонии появился в нужное время и открыл тем самым следующий этап инфокоммуникационных услуг.

Инфокоммуникационный этап, в котором термин *IP-телефонии* постепенно заменяется термином *IP-коммуникации,* характеризуется тем, что услуга передачи речи через IP-сети, которая первоначально воспринималась как угроза существующим телекоммуникационным операторам, оказалась с успехом востребована почти всеми сторонами в отрасли как

инновационное средство, которое может реально выполнить обещания мультимедийных коммуникаций.

Да и по мере развития первых сетей IP-телефонии стали проявляться недостатки и ограничения H.323. Для того чтобы справиться с возникающими проблемами, была разработана концепция декомпозиции шлюза, при которой управление вызовом сосредоточивается в одном блоке, называемом контроллером транспортного шлюза MGC (Media Gateway Controller) или Softswitch, а элементы трансформации транспортных потоков находятся в другом блоке, называемом транспортным шлюзом MG (Media Gateway). Тогда же, в 1998 г. был создан протокол управления шлюзами MGCP (Media Gateway Control Protocol), а после еще 2 лет напряженной работы Исследовательской комиссии 16 ITU-T и IETF в июне 2000 появился стандарт управления транспортным шлюзом, названный H.248 или MEGACO.

Нельзя не упомянуть и о таком протоколе как SIP, доминирующем в современном инфокоммуникационном этапе. Сам же мультимедийный трафик переносится при любых системах сигнализации, как правило, протоколом RTP.

Россия не была исключением среди стран, проявивших интерес к IP-телефонии. Интерес к новой технологии в России имеет особый практический смысл. Дело в том, что в нашей стране услуги международной телефонной связи традиционно дороже, чем на Западе. Кроме того, географические размеры нашей страны делают актуальным вопрос о стоимости междугородной связи. А использование IP-технологии подразумевает возможность ведения телефонных разговоров по более дешевому тарифу, что позволяет сэкономить значительные средства удаленным на большие расстояния абонентам.

В 1996 г. российско-американская компания CompTek приобрела пробный комплект оборудования для IP-связи, состоящий из двух шлюзов производства израильской фирмы VocalTec, а впоследствии заключила с VocalTec соглашение о дистрибъюции шлюзов на территории России и СНГ. Хотя этот проект ожидал большой коммерческий успех, возникли некоторые проблемы. С чем будет связываться имеющийся шлюз, если развитых IP-сетей в России еще не существует? Поэтому изначально покупателями шлюзов становились в основном территориально распределенные компании, использовавшие IP-телефонию для связи между своими офисами. Очевидный выход из сложившейся ситуации заключался в налаживании партнерских отношений с фирмами-операторами. На этом этапе ведущую роль в продви-

жении IP-технологии в России сыграла компания «Тарио». К тому времени она уже сотрудничала с VocalTec, и появление IP-шлюзов открыло новые перспективы и возможности для совместного бизнеса. Установкой шлюзов после заключения соответствующих соглашений занялись компании «Тарио» и RGC. При этом «Тарио» строила сети шлюзов в городах России, RGC налаживала связи для предоставления услуг международной связи.

Начиная с 1997 г., в России стали реально строиться сети IP-телефонии. Правда, из-за неопределенности с лицензированием эта услуга предоставлялась с пометкой *в тестовом режиме*. Тем не менее технология широко рекламировалась в прессе и демонстрировалась на выставках. Там постоянно предоставлялась бесплатная возможность сделать городские, междугородные и международные звонки через систему IP-телефонии. Представители компании VocalTec, в то время единственной фирмы, поставлявшей оборудование для IP-сетей, участвуя в различных семинарах и конференциях, неоднократно заявляли, что Россия обогнала многие страны на пути предоставления коммерческих услуг междугородной и международной IP-связи.

В то же время крупные Internet-провайдеры и крупные телефонные операторы не спешили осваивать новую технологию. Свои услуги на рынке активно предлагали только небольшие и средние компании. Такое положение объяснялось двумя аспектами: правовым и техническим.

Порядка лицензирования для IP-телефонии еще не существовало, и эта технология распространялась в стране практически нелегально, а следовательно, крупные фирмы не могли выйти на рынок с рекламной компанией услуг IP-телефонии.

Технический аспект состоял в несовершенстве оборудования. Первые шлюзы поддерживали не более одного потока E1 (до 30 одновременных звонков), а качество связи было низким, что приводило к значительному искажению голосовых сообщений. Со временем эти проблемы начали решать, и 1998 г. ознаменовался радикальным скачком в развитии технологии.

В 1998 г. по решению коллегии Миниинформсвязи (тогда называвшимся Госкомитетом по связи) в Ассоциации документальной электросвязи (АДЭ) была создана рабочая группа IP-телефонии. В группу вошли фирмы-разработчики и фирмы-поставщики оборудования, а также традиционные операторы связи (всего 41 компания). Группе было поручено разработать пакет документов для легализации интернет-телефонии в России. IP-телефония была (2000) официально признана «телематиче-

ской службой передачи речевой информации». На сегодняшний день уже многие российские компании, получив лицензии, приступили к внедрению IP-телефонии либо рассматривают такую возможность, решая, на каком оборудовании остановить свой выбор.

В Санкт-Петербурге на базе платформы Протей была начата разработка узла услуг IP-телефонии и в 2001 г. на выставке Связь-Экспоком в Москве был представлен первый российский коммерческий продукт – шлюз IP-телефонии Протей-IP. Именно учебная установка на базе Протей-IP может быть использована для выполнения лабораторных работ.

Данное издание составлено на базе учебных дисциплин лабораторных работ и практических занятий, начатых авторами (2001/2002) на кафедре систем коммутации и распределения информации существенно расширенных в настоящее время.

1. ОСНОВЫ IP-ТЕЛЕФОНИИ

1.1. 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. 1.1).

В этом соединении аналоговые сигналы разговорной речи от микрофона абонента А преобразуются в цифровую форму с помощью аналого-цифрового преобразователя (АЦП) обычно при 8000 отс/с, 8 бит/отс, в итоге 64 кбит/с (скорость первичного цифрового канала ISDN). Эти отсчеты речевых данных в цифровой форме затем сжимаются кодирующим устройством для сокращения использования полосы пропускания в 4, 8 или даже 10 раз. 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, Ко-

гда 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 соединения двух абонентов, системы IP-телефонии на каждом конце одновременно реализуют как функции передачи, так и функции приема.

Рис. 1.1. Сценарий IP-телефонии «компьютер-компьютер»

Для поддержки сценария «компьютер-компьютер» поставщику услуг (это может быть как провайдер IP-телефонии, так и владелец корпоративной сети) желательно иметь отдельный сервер адресов, преобразующий присвоенные (например, доменные) имена пользователей в динамические адреса IP, а сам сценарий ориентирован на пользователя, который использует сеть, в основном, для передачи данных и иногда применяет программное обеспечение IP-телефонии для разговоров с коллегами. Эффективное использование телефонной связи по IP по сценарию «компьютер-компьютер» обычно связано с повышением продуктивности работы крупных компаний, например, при организации виртуальной презентации в корпоративной сети с возможностью не

только видеть документы на Web-сервере, но и обсудить их содержание с помощью IP-телефона. При этом между двумя IP-сетями могут использоваться элементы ТфОП, а идентификация вызываемой стороны может осуществляться как на основе E.164, так и IP-адресации. Наиболее распространенным программным обеспечением для этих целей является пакет Microsoft Net Meeting, доступный для бесплатной загрузки с узла Microsoft.

Название сценария «компьютер-компьютер» отнюдь не означает, что у пользователя в распоряжении обязательно должен находиться стандартный ПК с микрофоном и колонками (рис. 1.1). Главным требованием для такой схемы является то, что оба пользователя должны иметь подключенные к IP-сети интеллектуальные терминалы: 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 сервисных службах технической поддержки. Пользователь, подключившийся к серверу WWW какой-либо компании, имеет возможность обратиться к оператору справочной службы. Этот сценарий, по всей вероятности, будет более активно востребован деловым сектором в ближайшие несколько лет.

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 (рис. 1.2). Предполагается, что установление соединения инициируется пользователем IP-сети.

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

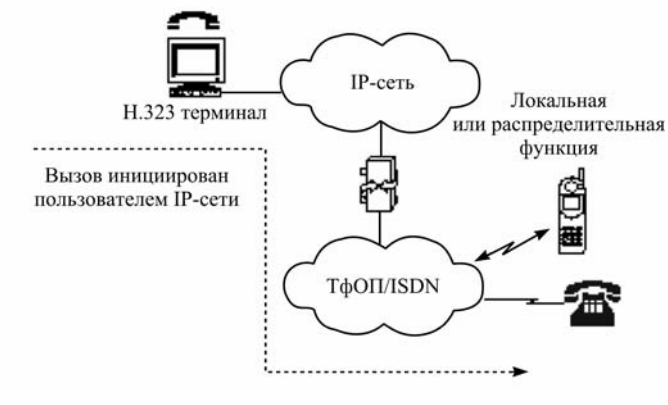


Рис. 1.2. Вызов абонента ТфОП пользователем IP-сети
по сценарию «компьютер-телефон»

В соответствии со второй модификацией сценария «компьютер-телефон» соединение устанавливается между пользователем IP-сети и абонентом ТфОП, но инициирует установление абонент ТфОП (рис. 1.3).

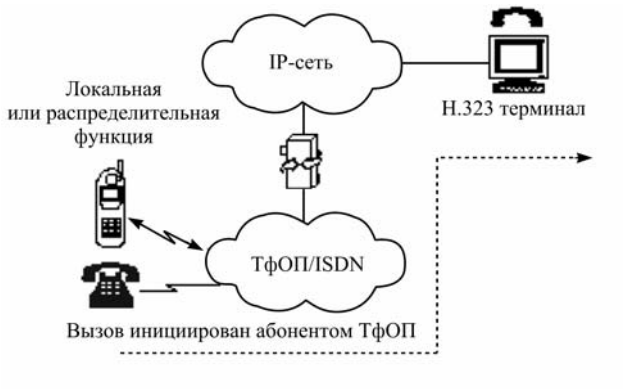


Рис. 1.3. Пользователя IP-сети вызывает абонент ТФОП
по сценарию «компьютер-телефон»

Рассмотрим несколько подробнее пример (рис. 1.3) упрощенной архитектуры системы IP-телефонии по сценарию «телефон-компьютер».

При попытке абонента А осуществить вызов к справочно-информационной службе, используя услуги пакетной телефонии и обычный телефон, на начальной фазе абонент А вызывает близлежащий шлюз IP-телефонии. От шлюза поступает запрос к абоненту А ввести номер, по которому должен быть направлен вызов (например, номер службы), и личный идентификационный номер (PIN) для аутентификации и последующего начисления оплаты, если это справочно-информационная служба, вызов к которой оплачивается самим вызывающим абонентом.

Основываясь на вызываемом номере, шлюз определяет наиболее доступный путь к данной службе. Кроме того, шлюз активирует свои функции кодирования речи и пакетизации для вызова, устанавливает контакт со службой, осуществляет мониторинг вызова и принимает информацию о прохождении вызова (например, состояние занятости, посылка вызова, разъединение и т. п.) от исходящей стороны через протокол управления и сигнализации. Разъединение на любом конце передается противоположной стороне по протоколу сигнализации и вызывает завершение установленных соединений и освобождение ресурсов шлюза для следующего вызова.

Для организации вызовов от службы к телефонным абонентам (рис. 2.2) используется аналогичная процедура. Эффективность объединения услуг передачи речи и данных является основным стимулом использования IP-телефонии по сценариям «компьютер-компьютер» и «компьютер-телефон», не представляя при этом никакой опасности интересам операторов традиционных телефонных сетей.

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.

Провайдеры услуг IP-телефонии (рис. 1.4) предоставляют услуги «телефон-телефон» путем установки шлюзов IP-телефонии на входе и выходе IP-сетей, абоненты которых подключаются к шлюзу провайдера через сеть с коммутацией каналов (ТфОП, ISDN, GSM), набирая специальный номер доступа. После установления соединения со шлюзом пользователь вводит персональный идентификационный номер (PIN) или применяется идентификации номера вызывающего абонента (Calling Line Identification), для получения доступа к услугам шлюза.

При удачной авторизации шлюз просит пользователя ввести телефонный номер вызываемого абонента. Номер вызываемого абонента анализируется входным шлюзом для определения шлюза ближайшего к телефону вызываемого абонента. Как только между шлюзами устанавливается контакт, дальнейшее установление соединения к вызываемому абоненту будет выполняться выходным шлюзом через его местную телефонную сеть.

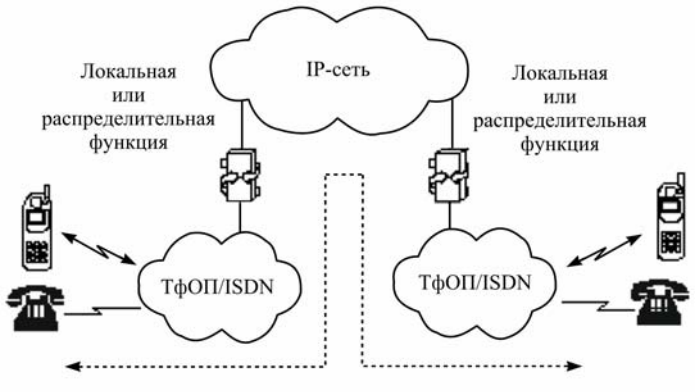


Рис. 1.4. Соединение абонентов ТфОП через транзитную IP-сеть
по сценарию «телефон-телефон»

Полная стоимость такого вызова для пользователя будет складываться из расценок ТфОП на связь с местным шлюзом, провайдера IP-телефонии и удаленной ТфОП на завершение установления соединения с вызываемым абонентом.

1.2. 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.

1.2.1. 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 (рис. 1.5).

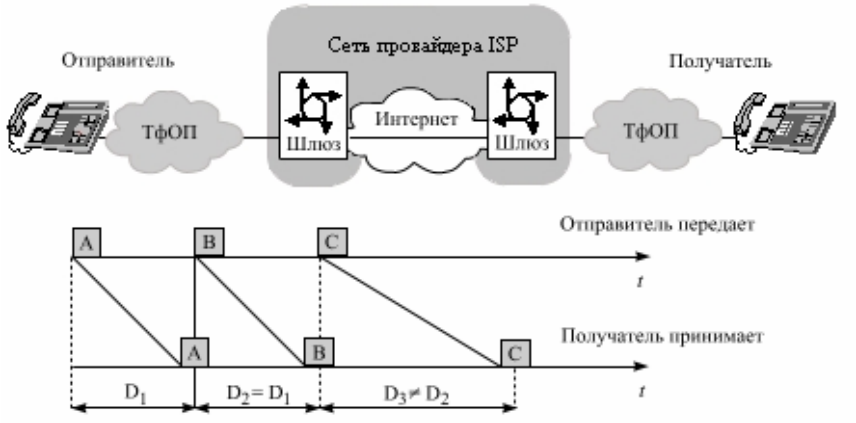


Рис. 1.5. Различие интервалов между моментами прибытия пакетов (джиттер)

Для того чтобы компенсировать влияние джиттера, в терминалах используется так называемый *джиттер-буфер*, который 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.

1.2.2. Эхо

Феномен эха вызывает затруднения при разговоре и говорящего, и слушающего. Говорящий слышит с определенной задержкой свой собственный голос. Если сигнал отражается дважды, 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 гг. 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.

1.2.3. 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 передаче 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 5-балльной 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% времени. Таким образом, если применить алгоритмы, которые позволяют уменьшить объем информации, передаваемой в периоды молчания, 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, 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. п.), 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. Пакеты содержат кадры, сформированные кодеком, что вызывает потери кадров. Однако потери пакетов и потери кадров не всегда напрямую связаны между собой, так как существуют подходы (например, 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.

1.2.4. Кодеки, стандартизованные ITU-T

Кодек G.711 – «дедушка» всех цифровых кодеков речевых сигналов, был одобрен ITU-T в 1965 г. Типичная оценка MOS составляет 4.2. 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 (1995), и 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 бит, 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 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 использует оригинальную технологию с малой задержкой и гарантирует оценки MOS, аналогичные G.726 при скорости передачи 16 кбит/с. Недостатком алгоритма являются высокая сложность (требовательность к вычислительной мощности) и относительно высокая чувствительность к потерям кадров.

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: упрощенный G.729A и полный G.729.

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.

1.2.5. Кодеки, стандартизованные ETSI

В рамках деятельности европейского института ETSI стандартизованы узкополосные кодеки для применения в системах мобильной связи (GSM).

Спецификации кодека *GSM Full Rate*, известного также как GSM 06.10, утверждены в 1987 г. Кодек обеспечивает хорошее качество и устойчивую работу в условиях фонового шума (оценка MOS порядка 3.7 в условиях без шума). Кодируются кадры длительностью 20 мс, образуя цифровой поток со скоростью 13 кбит/с. Кодек не требует высокой производительности процессора. Этот кодек очень важен для некоммерческих проектов в области IP-телефонии особенно для проектов, связанных с открытым распространением исходных текстов ПО из-за возможности бесплатного лицензирования.

Существуют также спецификации кодеков GSM Half Rate, принятые в 1994 г., и GSM Enhanced Full Rate, принятые в 1995 г. Характеристики этих кодеков превосходят характеристики исходного варианта, однако алгоритмы требуют большей производительности процессора. В приложениях IP-телефонии они, по разным причинам, распространения пока не получили.

1.3. Протокол RTP

Основным транспортным протоколом для приложений IP-телефонии стал *протокол реального времени RTP (Real-Time Protocol),* предназначенный для организации передачи пакетов с закодированными речевыми сигналами по IP-сети. Передача пакетов RTP осуществляется поверх протокола UDP, в свою очередь функционирующего поверх IP (рис. 1.6).

Для передачи речевого (мультимедийного) трафика RTP использует пакеты, структура которых показана на рис. 1.7.

Пакет RTP состоит, как минимум, из 12 байтов. В первых двух битах RTP-заголовка (после версии *V*) указывается версия протокола RTP (в настоящее время это версия 2). Ясно, что для такой структуры заголовка возможна максимум еще только одна версия RTP.

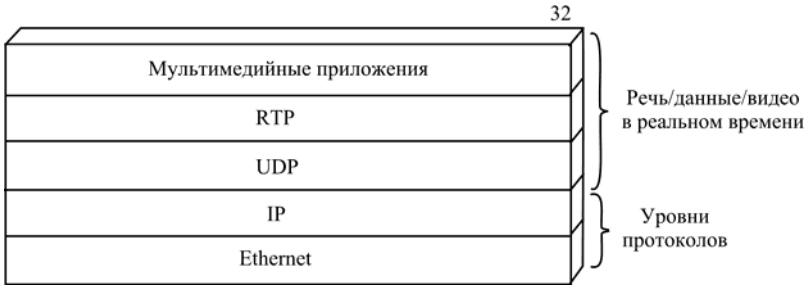


Рис. 1.6. Уровни протоколов RTP/UDP/IP

Следующее за ними поле содержит два бита: бит *P*, который указывает, были ли добавлены в конце поля с полезной нагрузкой символы-наполнители (они обычно добавляются, если транспортный протокол или алгоритм кодирования требует использования блоков фиксированного размера), и бит *X*, который указывает, используется ли расширенный заголовок. Если он используется, то первое слово расширенного заголовка содержит общую длину расширения.

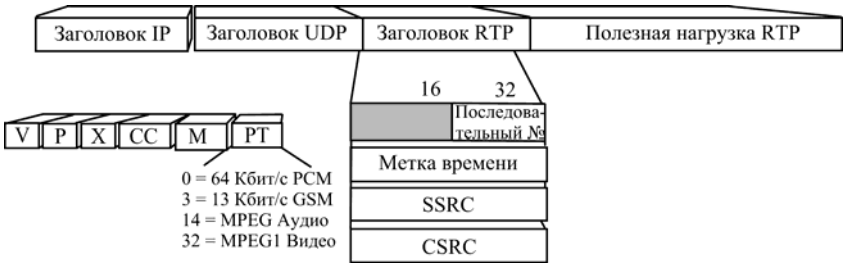


Рис. 1.7. Заголовок VoIP

Далее четыре бита *CC* определяют число CSRC-полей в конце RTP-заголовка, т. е. число источников, формирующих поток. Маркерный бит *M* позволяет отмечать то, что стандарт определяет как *существенные события*, например, начало видеокадра, начало слова в аудиоканале и т. п. За ним следует поле типа данных *PT* (7 бит), где указывается код типа

полезной нагрузки, определяющий содержимое поля полезной нагрузки – *данные приложения (Application Data),* например, несжатое 8-битное аудио MP3 и т. п. По этому коду приложение может узнать, что нужно делать, чтобы декодировать данные.

Остальная часть заголовка фиксированной длины состоит из поля *порядкового номера (SequenceNumber),* поля *метки времени (Time Stamp)* для записи момента создания первого слова пакета и поля *источника синхронизации SSRC*, которое идентифицирует этот источник. В последнем поле можно указывать единственное устройство, имеющее только один сетевой адрес, множественные источники, которые могут представить различные мультимедийные среды (аудио, видео и т. д.), или различные потоки одной и той же среды. Так как источники могут быть на различных устройствах, SSRC-идентификатор выбирается случайным образом так, чтобы шанс получать данные сразу от двух источников во время RTP-сеанса был минимальным. Однако определен также и механизм решения конфликтов, если они возникают. За фиксированной частью RTP-заголовка могут следовать еще до 15 отдельных 32-разрядных CSRC-полей, которые идентифицируют источники данных.

RTP поддерживается другим *протоколом управления реального времени RTCP (Real-Time Transport Control Protocol)*, который обеспечивает дополнительные отчеты, содержащие информацию о сеансах связи RTP. Напомним, что ни UDP-, ни RTP-протоколы не занимаются обеспечением *качества обслуживания QoS (Quality of Service)*. RTCP-протокол обеспечивает обратную связь с отправителями, а получателям потоков он предоставляет некоторые возможности повышения QoS, информацию о пакетах (потери, задержки, джиттер) и о пользователе (приложении, потоке). Для управления потоком существуют отчеты двух типов, генерируемые и отправителями, и получателями. Например, информация о доле потерянных пакетов и абсолютном количестве потерь позволяет отправителю (при получении отчета) обнаруживать, что перегрузка канала может заставить получателей не принимать потоки обслуживающих пакетов, которые они ожидали. В этом случае отправитель имеет возможность понизить скорость кодирования, чтобы уменьшить перегрузку и улучшить прием. Отчет отправителя содержит информацию о том, когда был сгенерирован последний RTP-пакет (она включает как внутреннюю метку, так и реальное время). Эта информация позволяет получателю координиро-

вать и синхронизировать множественные потоки, например, видео и аудио. Если поток направляется нескольким получателям, то организуются потоки RTCP-пакетов от каждого из них. При этом будут предприняты шаги для ограничения ширины полосы обратно пропорционально скорости, с которой генерируются RTCP-отчеты, и числу получателей.

2. ПОСТРОЕНИЕ СЕТЕЙ IP-ТЕЛЕФОНИИ НА БАЗЕ H.323

2.1. Архитектура сети H.323

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

ITU-T исторически занимался проблемами телефонных сетей, поэтому 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.

При этом рекомендация H.323 предусматривает применение разнообразных алгоритмов сжатия речевой информации, что позволяет использовать полосу пропускания ресурсов передачи гораздо более эффективно, чем в сетях с коммутацией каналов.

Этот вариант построения сетей IP-телефонии ориентирован на операторов местной телефонной связи (или на компании, владеющие транспортными сетями), которые хотят использовать сети с маршрутизацией пакетов IP для предоставления услуг междугородной и международной связи (рис. 2.1).

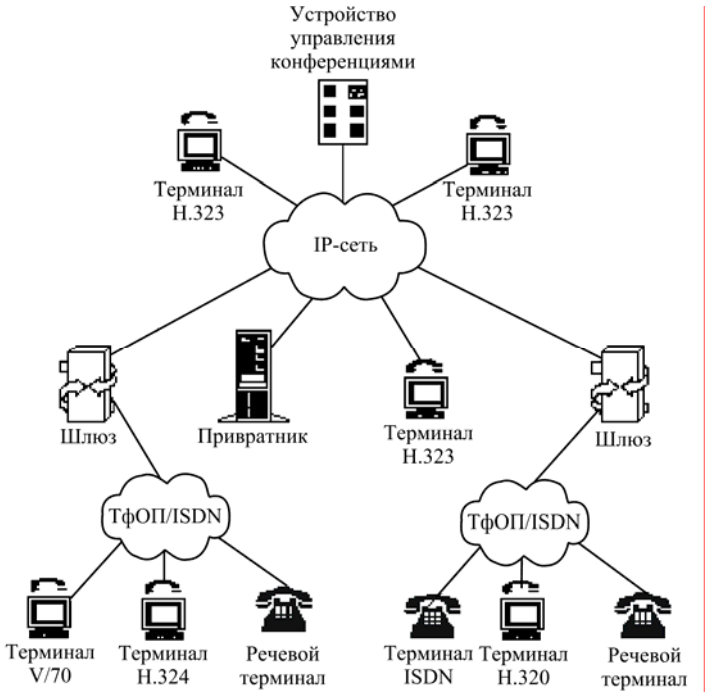


Рис. 2.1. Архитектура сети H.323

Основными устройствами сети являются: терминал, шлюз, привратник и устройство управления конференциями. Необходимо отметить, что в отличие от устройств ТфОП, устройства H.323 не имеют жестко закрепленного места в сети. Устройства подключаются к любой точке IP-сети, но при этом сеть H.323 разбивается на зоны, а каждой зоной управляет привратник.

2.1.1. Терминал H.323

Терминал H.323 – это оконечное устройство сети IP-телефонии, обеспечивающее двухстороннюю речевую или мультимедийную связь с другим терминалом, шлюзом или устройством управления конференциями (рис. 2.2). При этом терминалом для сети H.323 может оказаться обычный телефонный аппарат, с которого абонент позвонил на шлюз с помощью предоплаченных карт или персональный компьютер с установленным мультимедийным приложением (например, NetMeeting). Сейчас появилось понятие упрощенных H.323 терминалов, которые поддерживают аудио или текстовую связь согласно H.323, но не реализуют весь функционал классического H.323 терминала.

Пользовательский интерфейс управления системой дает пользователю возможность создавать и принимать вызовы, а также конфигурировать систему и контролировать ее работу.

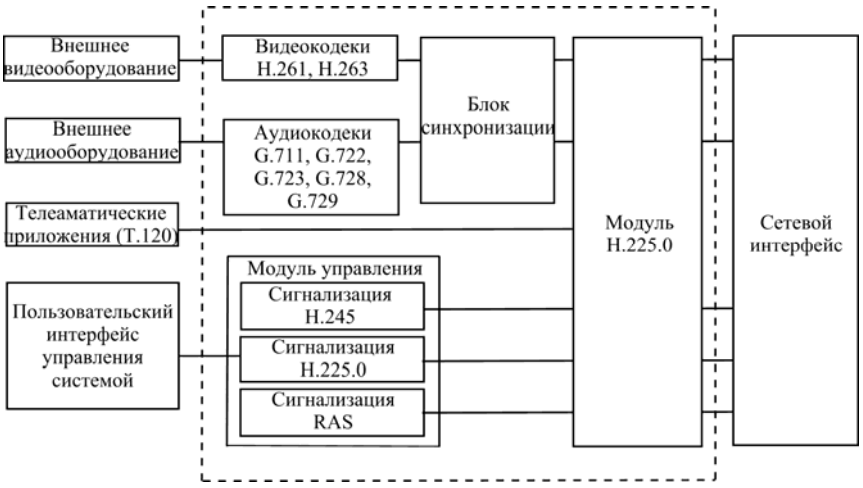


Рис. 2.2. Терминал стандарта H.323

Модуль управления поддерживает три вида сигнализации: H.225, H.245, RAS и обеспечивает регистрацию терминала у привратника, установление и завершение соединения, обмен информацией, необходимой для открытия разговорных каналов, предоставление дополнительных услуг и техобслуживание.

Телематические приложения обеспечивают передачу пользовательских данных, неподвижных изображений и файлов, доступ к базам данных и т. п. Стандартным протоколом для поддержки таких приложений является протокол T.120.

Модуль H.225.0 отвечает за преобразование видеоинформации, речи, данных и сигнальной информации в вид, пригодный для передачи по сетям с маршрутизацией пакетов IP, и наоборот. Кроме того, функциями модуля являются разбиение информации на логические кадры, нумерация последовательно передаваемых кадров, выявление и коррекция ошибок.

Сетевой интерфейс обеспечивает гарантированную передачу управляющих сообщений H.245, сигнальных сообщений H.225.0 (Q.931) и пользовательских данных при помощи протокола TCP и негарантирован-

ную передачу речевой и видеоинформации, а также сообщений RAS при помощи протокола UDP.

Блок синхронизации вносит задержку на приемной стороне с целью обеспечить синхронизацию источника информации с ее приемником, согласование речевых и видеоканалов или сглаживание вариации задержки информации.

Видеокодеки кодируют видеоинформацию, поступающую от внешнего источника видеосигналов (видеокамеры или видеомагнитофона), для ее передачи по сети с маршрутизацией пакетов IP и декодируют сигналы, поступающие от сети, для последующего отображения видеоинформации на мониторе или телевизоре.

Аудиокодеки кодируют аудиоинформацию, поступающую от микрофона (или от других источников), для ее передачи по сети с маршрутизацией пакетов IP и декодируют сигналы, поступающие от сети, для последующего воспроизведения.

Естественно здесь приведена наиболее полная конфигурация терминального устройства. Понятно, что домашний телефонный аппарат не имеет видеокодеков.

2.1.2. Шлюз H.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 H.323. Таким образом, шлюз должен преобразовывать аналоговую абонентскую сигнализацию, сигнализацию по 2ВСК и сообщения систем сигнализации DSS1 и ОКС7 в сигнальные сообщения H.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 тер-

минала или устройства управления конференциями. Шлюз может сначала участвовать в соединении в качестве терминала, а затем при помощи сигнализации H.245 продолжить работу в качестве устройства управления конференциями. Очевидно, что в случае, когда терминал H.323 связывается с другим терминалом H.323, расположенным в той же самой IP-сети, шлюз в этой связи не участвует.

2.1.3. Привратник

В привратнике сосредоточен весь интеллект сетей IP-телефонии, базирующихся на рекомендации ITU H.323. Как уже говорилось, сеть H.323 имеет зонную архитектуру (рис. 1.4). Привратник выполняет функции управления зоной сети IP-телефонии, в которую входят терминалы, шлюзы и блоки конференций, зарегистрированные у этого привратника. Разные участки зоны сети H.323 могут быть территориально разнесены и соединяться друг с другом через маршрутизаторы.

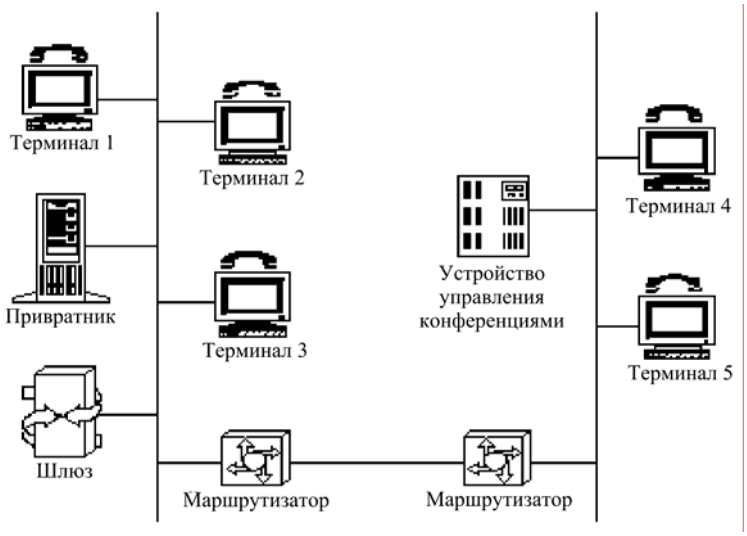


Рис. 2.3. Зона сети H.323

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.

Если вызывающий абонент знает IP-адрес терминала вызываемого абонента, соединение между двумя устройствами может быть установлено без помощи привратника. Часть функций привратника берет на себя шлюз, например, преобразование адреса вызываемого абонента, поступающего со стороны ТфОП в формате E.164, в транспортный адрес IP-сетей.

2.1.4. Устройство управления конференциями

Одна из дополнительных услуг IP-телефонии, возможность организации конференций, а рекомендация H.323 предусматривает три вида конференции (рис. 2.4).

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.

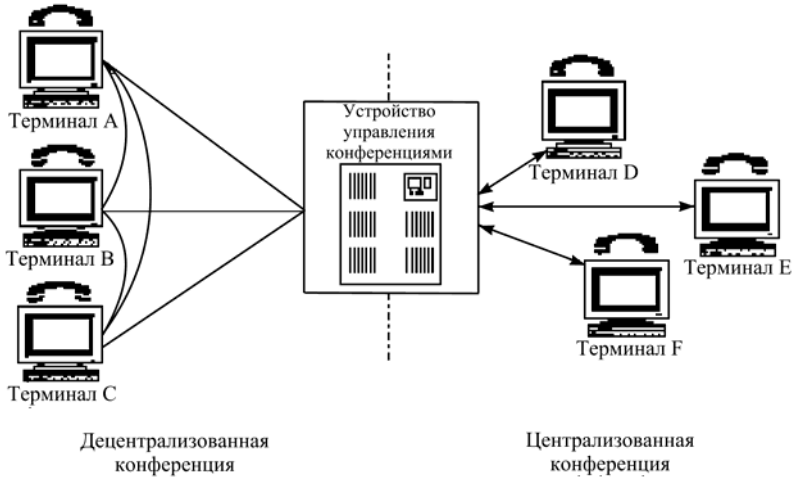


Рис. 2.4. Разные виды конференции в сети H.323

Для децентрализованной конференции требуется более сложное терминальное оборудование; кроме того, желательно, чтобы в сети поддерживалась передача пакетов IP в режиме многоадресной рассылки (IP multicasting). Если сеть не поддерживает этот режим, терминал может передавать информацию к каждому из остальных терминалов, участвующих в конференции, в режиме «точка-точка», но это становится неэффективным при числе участников более четырех.

Устройство управления конференциями MCU содержит один обязательный элемент: контроллер многоточечных соединений (Multipoint controller, MC). Кроме того, MCU может содержать один или более процессоров для обработки информации пользователей при многоточечных соединениях (Multipoint processor, MP).

2.1.5. H.323 в современных сетях

Протокол H.323 стал первым из коммерчески успешных протоколов IP-телефонии и, разумеется, его наиболее распространенная 2-я версия сейчас уже считается устаревшей. Она не приспособлена для предос-

тавления многих современных мультимедийных услуг, но будущее H.323 еще до конца не определено: сетей на базе H.323 сейчас построено больше, чем на остальных технологиях IP-телефонии, и к тому же разработаны новые версии этого протокола.

В версиях 4 и 5 разработчики постарались внедрить наиболее востребованные сетевые функции и архитектуры, в частности, начиная с версии 4, в H.323 используется принцип декомпозиции шлюза, о котором будет сказано ниже.

2.2. 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, которые совместно с интернет-протоколами TCP/IP, UDP, RTP и RTCP, а также протоколом Q.931, представлены на рис. 2.5.

Протокол TCP (рис. 2.5) используется для переноса сигнальных сообщений H.225 и управляющих сообщений H.245, сигнальные сообщения RAS переносятся с помощью протокола UDP, а перенос речевой и видеоинформации производится посредством использования RTP/RCP.

Рис. 2.5. Стек протокола H.323

2.2.1. Протокол RAS

В рекомендации H.225.0 определен протокол взаимодействия компонентов сети H.323 оконечного оборудования (терминалов, шлюзов, устройств управления конференциями) с привратником, который получил название Registration, Admission and Status (RAS).

Основные процедуры, выполняемые оконечным оборудованием и привратником с помощью протокола RAS:

* 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 H.245 и сигнальный H.225.0 каналы, 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.

Обнаружение привратника

Прежде чем устройство станет полноправной частью сети, необходимо сделать так, чтобы все остальные устройства увидели нового участника и смогли взаимодействовать с ним. Для этого необходимо зарегистрировать оборудование на привратнике зоны, в которой будет работать данное устройство. Прежде всего, нужно, чтобы устройству стал известен сетевой адрес подходящего привратника. Процесс определения этого ад-

реса называется обнаружением привратника. Определены два способа обнаружения: ручной и автоматический.

Ручной способ заключается в том, что привратник, обслуживающий определенное устройство, определяется заранее при конфигурации этого устройства. Первая фаза установления соединения начинается сразу с запроса регистрации устройства, который передается на уже известный сетевой адрес привратника и на UDP порт 1719 (2-я версия протокола) или на порт 1718 (1-я версия).

При автоматическом способе обнаружения привратника устройство передает запрос Gatekeeper Request (GRQ) в режиме многоадресной рассылки (multicasting), используя IP-адрес 224.0.1.41 (Gatekeeper UDP Discovery Multicast Address) и UDP порт 1718 (Gatekeeper UDP Discovery Port). Ответить оконечному оборудованию могут один или несколько привратников, передав на адрес, указанный в поле rasAddress запроса GRQ, сообщение Gatekeeper Confirmation (GCF) с предложением своих услуг и указанием транспортного адреса канала RAS (рис. 2.6). Если привратник не имеет возможности зарегистрировать оконечное оборудование, он отвечает на запрос сообщением Gatekeeper Reject (GRJ).

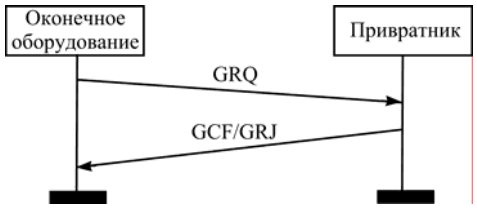


Рис. 2.6. Автоматическое обнаружение привратника

Если на GRQ отвечает несколько привратников, оконечное оборудование может выбрать по своему усмотрению любой из них, после чего инициировать процесс регистрации. Если в течение 5 с ни один привратник не ответит на GRQ, оконечное оборудование может повторить запрос.

При возникновении ошибки в процессе регистрации у своего привратника, т. е. при получении отказа в регистрации или при отсутствии ответа на запрос регистрации, оконечное оборудование должно провести процедуру обнаружения привратника снова.

Регистрация оконечного оборудования

Следующим шагом после обнаружения привратника оконечным оборудованием, будет присоединение к зоне сети, обслуживаемой данным привратником, т. е. оборудование должно пройти процедуру регистрации (рис. 2.7). Для этого привратнику сообщается адресная информация: список и alias-адресов и транспортных адресов оконечного оборудования.

Оконечное оборудование передает запрос регистрации Registration Request (RRQ) на сетевой адрес привратника либо полученный при выполнении процедуры его автоматического обнаружения, либо известный априори. Стоит отметить, что запрос направляется на общеизвестный номер UDP порта 1719 (Gatekeeper UDP Registration and Status Port). Привратник отвечает на запрос подтверждением Registration Confirmation (RCF) или отказом в регистрации Registration Reject (RRJ). Напомним, что оконечное оборудование может зарегистрироваться только у одного привратника.

Если оконечное оборудование не указывает alias-адрес в запросе RRQ, привратник может сам назначить такой адрес и передать его оборудованию в сообщении RCF.

Оконечное оборудование может регистрироваться на ограниченный промежуток времени, указывая в параметре **timeToLive** сообщения RRQ длительность этого промежутка в секундах. Привратник может подтвердить регистрацию сообщением RCF с параметром **timeToLive**, имеющим то же или меньшее значение.

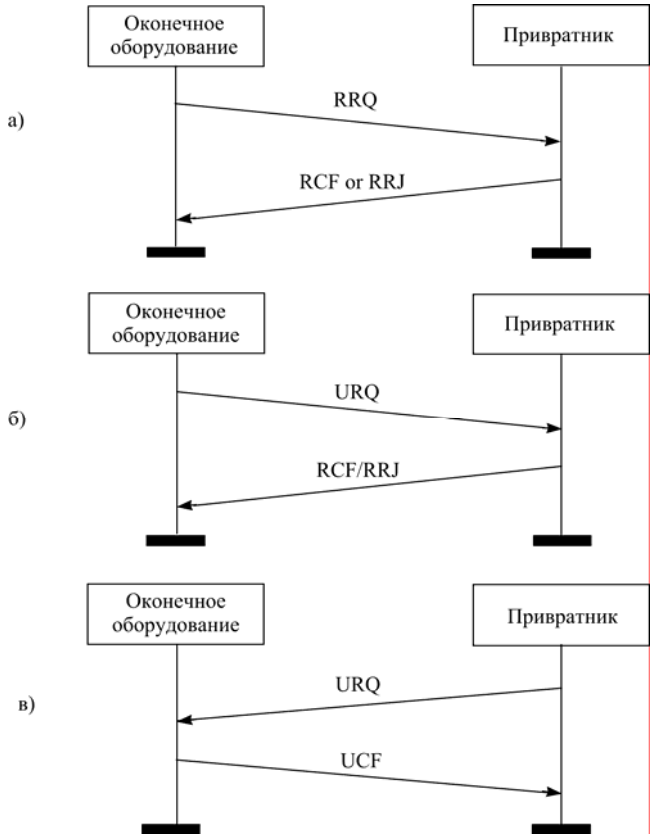


Рис. 2.7. Процессы управления регистрацией:
а – регистрация,
б – отмена регистрации оконечным оборудованием,
в – отмена регистрации привратником

В течение указанного промежутка времени оконечное оборудование может продлить регистрацию, передав сообщение RRQ с параметром **keepAlive**. Получив это сообщение, привратник должен перезапустить таймер.

По истечении назначенного промежутка времени регистрация считается недействительной. В этом случае привратник может передать сообщение об отмене регистрации, а оконечное оборудование должно пройти повторную регистрацию.

Оконечное оборудование может отменить регистрацию у привратника, передав сообщение Unregister Request (URQ); привратник должен ответить подтверждением Unregister Confirmation (UCF). Такая процедура позволяет оборудованию изменить свой alias-адрес или транспортный адрес. Если оборудование не было зарегистрировано у привратника, последний должен ответить на требование URQ отказом Unregister Reject (URJ).

Привратник может отменить регистрацию оборудования, передав сообщение Unregister Request (URQ), при получении которого оконечное оборудование должно ответить подтверждением Unregister Confirmation (UCF). Теперь, чтобы получить возможность участия в любом соединении, оконечное оборудование должно перерегистрироваться у того же привратника или зарегистрироваться у нового.

Доступ оконечного оборудования к сетевым ресурсам

Чтобы оборудование могло работать в сети, ему необходим доступ к ресурсам этой сети, поэтому в начальной фазе установления соединения, а также после получения сообщения Setup, оборудование обращается к привратнику при помощи запроса Admissions Request (ARQ) с просьбой разрешить соединение с другим оборудованием (рис. 2.8), что является началом процедуры доступа к сетевым ресурсам. Причем процедура доступа выполняется всеми участниками соединения.

В сообщении ARQ содержится идентификатор оборудования, передавшего сообщение ARQ, и контактная информация того оборудования, с которым оно желает связаться. Контактная информация оборудования включает в себя alias-адрес и/или транспортный адрес сигнального канала, но, как правило, в запрос ARQ помещается только alias-адрес вызываемого оборудования.

В сообщении ARQ указывается также верхний предел суммарной скорости передачи и приема пользовательской информации по всем речевым и видеоканалам (без учета заголовков RTP/UDP/IP и другой служебной информации).

Привратник может выделить требуемую полосу пропускания или снизить предел суммарной скорости (рис. 2.8), передав сообщение Admissions Confirm (ACF). В этом же сообщении, кроме суммарной ско-

рости, указывается транспортный адрес сигнального канала встречного оборудования, если сигнальный канал будет связывать оборудование непосредственно, или адрес привратника, если он будет маршрутизировать сигнальные сообщения.

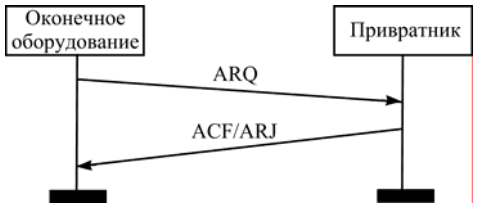


Рис. 2.8. Управление доступом к сетевым ресурсам

После получения ответа ACF на указанный в этом сообщении адрес вызывающий терминал передает сообщение Setup, и делается попытка установить сигнальное соединение H.225.0. Только после организации сигнального канала и получения по нему сообщения Setup вызываемое оборудование инициирует процедуру доступа к сетевым ресурсам. Если требуемая полоса недоступна, привратник передает сообщение Admissions Reject (ARJ).

Определение местоположения оборудования в сети

Если оконечное оборудование или привратник желает узнать контактную информацию некоего терминала (адреса сигнального канала и канала RAS) по его alias-адресу, посылается многоадресный запрос Location Request (LRQ). Привратник, у которого зарегистрировано указанное оборудование, должен ответить сообщением Location Confirmation (LCF), содержащим требуемую контактную информацию. Эта процедура называется определением местоположения оконечного оборудования в сети (рис. 2.9).

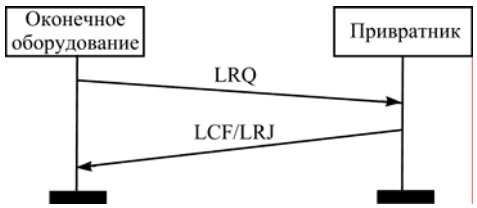


Рис. 2.9. Определение местоположения оборудования в сети

Привратник, получивший на транспортный адрес своего канала RAS запрос LRQ, должен ответить отказом Location Reject (LRJ), если искомое оборудование у него не зарегистрировано. Привратники, у которых искомое оборудование не зарегистрировано, а сообщение LRQ получено в режиме многоадресной рассылки Gatekeeper′s Discovery Multicast, вообще не должны отвечать на запрос.

Вышеописанная процедура используется тогда, когда в сети имеется несколько зон, а вызов выходит за пределы одной зоны. Привратник, у которого зарегистрировано вызывающее оборудование, передает запрос адреса сигнального канала вызываемого оборудования.

Опрос текущего состояния оборудования

Поскольку необходим постоянный контроль за оборудованием и за процессом установления соединения привратник рассылает специальные сообщения через определенные промежутки времени. Данный процесс называется опросом текущего состояния оборудования (рис. 2.10).

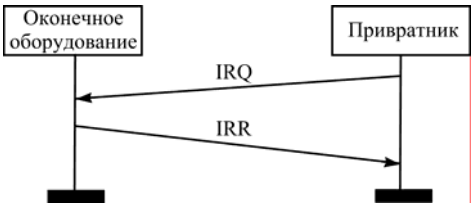


Рис. 2.10. Опрос текущего состояния оборудования

Запрос информации о текущем состоянии (статусе) оборудования производится привратником при помощи сообщения Information Request (IRQ). Выбор интервала между посылками IRQ оставлен на усмотрение производителя, но он должен быть не меньше 10 с. Получив запрос IRQ, оконечное оборудование должно передать запрашиваемую информацию в сообщении Information Request Response (IRR).

Освобождение полосы пропускания

В конечной фазе разрушения соединения оборудование извещает привратника об освобождении раннее занимавшейся полосы пропускания (рис. 2.11). Оконечное оборудование передает своему привратнику сооб-

щение Disengage Request (DRQ), на которое тот должен ответить подтверждением Disengage Confirm (DCF).

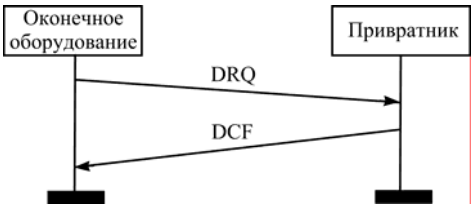


Рис. 2.11. Освобождение полосы пропускания

Привратник может сам инициировать освобождение сетевых ресурсов, т. е. разрушение существующего соединения, передав сообщение DRQ. Получив сообщение DRQ, оконечное оборудование должно закрыть логические каналы, управляющий и сигнальный каналы, а затем ответить подтверждением DCF. В случае если привратник инициирует завершение конференции, сообщение DRQ должно передаваться каждому участнику.

2.2.2. Сигнальный канал 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 для установления соединения, 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 незанято и что вызываемому пользователю подается сигнал о входящем вызове.

Сообщение *Connect* передается 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 для разрушения соединения и 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.

В сетях, не имеющих привратника, сигнальный канал H.225.0 открывается непосредственно между вызывающим и вызываемым оконечным оборудованием. В этом случае вызывающий пользователь должен знать транспортный адрес сигнального канала (Call Signalling Transport Address) терминала вызываемого пользователя.

В сетях с привратником вызывающее оборудование передает по транспортному адресу канала RAS привратника сообщение ARQ с указанием alias-адреса вызываемого пользователя. Если сигнальные сообщения будут маршрутизировать привратник (Gatekeeper Routed Call Signalling), то в ответном сообщении он передает транспортный адрес своего сигнального канала. Если же сигнальный канал будет организован непосредственно между вызывающим и вызываемым оборудованием (Direct Endpoint Call Signalling), в ответном сообщении передается транспортный адрес сигнального канала вызываемого оборудования. Выбор варианта передачи сигнальных сообщений оставлен за привратником, хотя оконечное оборудование может указывать, какой вариант для него предпочтителен. И в первом, и во втором случаях сигнальный канал H.225 выполняет одни и те же функции и переносит одни и те же сообщения.

При маршрутизации сигнальных сообщений привратником сигнальный канал может закрываться сразу после установления соединения или оставаться открытым в течение всего соединения для предоставления дополнительных услуг. Закрыть сигнальный канал может только привратник, но если в соединении участвует шлюз, то сигнальный канал должен оставаться открытым до окончания соединения. При закрытии сигнального канала оконечным оборудованием должно сохраняться текущее состояние соединения. Привратник может в любой момент соединения снова открыть сигнальный канал.

Сценарий установления соединения схож с аналогичным сценарием в сетях ISDN. Рассмотрим успешное установление соединения. После обмена с привратником сообщениями ARQ и ACF по каналу RAS вызывающее оборудование передает запрос соединения *Setup* по указанному транспортному адресу сигнального канала. В ответ на сообщение

Setup вызываемое оборудование посылает сообщение *Call Proceeding*, означающее, что вся информация, необходимая для установления соединения, получена, и вызов принят к обслуживанию. Далее от вызываемого оборудования исходит сообщение *Alerting*, означающее, что вызываемому пользователю подается вызывной сигнал. После того как пользователь принимает вызов, вызываемому оборудованию передается сообщение *Connect* с транспортным адресом управляющего канала H.245 вызываемого оборудования, если управляющий канал устанавливается напрямую между вызывающим и вызываемым оборудованием, или транспортный адрес канала H.245 привратника, если управляющие сообщения маршрутизирует привратник. В некоторых случаях, например, для проключения разговорных каналов в предответном состоянии транспортный адрес управляющего канала H.245 вводится в сообщения *Call Proceeding* или *Alerting*.

2.2.3. Управляющий канал 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 (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.

Перенос управляющей информации H.245 осуществляется протоколом TCP по нулевому логическому каналу, который должен быть постоянно открытым с момента организации канала H.245 и вплоть до его ликвидации.

По управляющему каналу H.245 передаются сообщения четырех категорий: запросы, ответы, команды и индикации. Получив сообщение-запрос, оборудование должно выполнить определенное действие и немедленно передать обратно сообщение-ответ. Получив сообщение-команду, оборудование также должно выполнить определенное действие, но отвечать на команду не должно. Сообщение-индикация служит для того, чтобы информировать о чем-либо получателя, но не требует от него ни ответа, ни каких бы то ни было действий.

Определение ведущего и ведомого оборудования

Процедура определения ведущего и ведомого оборудования используется для разрешения конфликтов, возникающих между двумя устройствами при организации конференции, когда ведущим в ней может быть любое из этих устройств, или между двумя устройствами, которые одновременно пытаются открыть двунаправленный логический канал. Устройства обмениваются сообщениями **masterSlaveDetermination** (рис. 2.12), в поле **terminalType** которых помещается значение, соответствующее типу данного оборудования, а в поле **statusDeterminationNumber** – случайное число из интервала $[0, \ldots, (2^{24}-1)]$. Ведущим становится оборудование, поместившее большее число в поле **terminalType**, а при совпадении типов оборудования – большее число в поле **statusDeterminationNumber**.

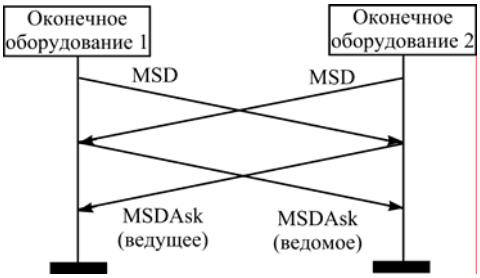


Рис. 2.12. Определение ведущего и ведомого оборудования

В ответ на полученные сообщения **masterSlaveDetermination** оба устройства передают сообщения **masterSlaveDeterminationAck**, в которых указывается, какое оборудование является для данного соединения ведущим, а какое – ведомым. При этом любое оборудование стандарта H.323 должно быть способно работать и в качестве ведущего, и в качестве ведомого.

Обмен данными о функциональных возможностях оборудования

Оборудование стандарта H.323 в общем случае способно принимать и передавать речь, видеоинформацию и данные. Это означает, что оборудование обычно содержит приемник и передатчик информации. Как правило, устройства поддерживают несколько алгоритмов кодирования и декодирования информации каждого вида. Для согласования режимов работы передающей и принимающей сторон используется процедура, называемая обменом данными о функциональных возможностях оборудования (рис. 2.13).

Терминалы обмениваются сообщениями TerminalCapabilitySet, в которых каждый из них указывает алгоритмы, используемые для декодирования принимаемой и кодирования передаваемой информации, т. е. режимы, в которых терминал способен функционировать.

В сообщение TerminalCapabilitySet включается поле **capabilityTable** – таблица функциональных возможностей, где каждому алгоритму кодирования/декодирования присвоен порядковый номер. Указанные порядковые номера объединяются в список альтернативных режимов **alternativeCapabilitySet**. Оборудование может использовать любой (но только один) из режимов, указанных в списке. В свою очередь,

альтернативные режимы объединяются в наборы одновременно возможных режимов функционирования **simultaneousCapabilities**.

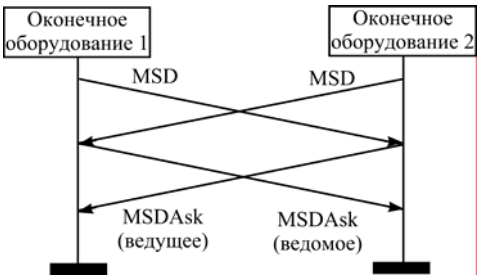


Рис. 2.13. Обмен данными
о функциональных возможностях оборудования

Функциональные возможности терминала описываются набором дескрипторов (**capabilityDescriptor**), каждый из которых состоит из одного набора одновременно возможных режимов функционирования оборудования и номера дескриптора (**capabilityDescriptorNumber)**. Если при обмене данными о функциональных возможностях оборудование указывает более одного дескриптора, то это означает, что оно поддерживает несколько режимов функционирования. Оборудование может в любое время передать сообщение TerminalCapabilitySet с дескриптором, добавляющим новые функциональные возможности, или с дескриптором, исключающим некоторые из ранее указанных возможностей.

Оборудование, которое получило от другого оборудования сообщение TerminalCapabilitySet, может подтвердить его получение передачей сообщения TerminalCapabilitySetAck. Приняв сообщение с некорректным набором возможностей, оборудование отвечает сообщением TerminalCapabilitySetReject.

При срабатывании таймера, запущенного после отправки сообщения TerminalCapabilitySet, оборудование, его пославшее, передает сообщение TerminalCapabilitySetRelease.

Открытие и закрытие логических каналов

Информация, передаваемая источником к одному или более приемникам, в сетях на базе H.323 переносится по логическим каналам, которые идентифицируются уникальным для каждого направления передачи номером канала. Рекомендацией H.245 предусмотрена возможность создания логиче-

ских каналов двух видов: однонаправленных (uni-directional), т. е. открывающихся в направлении от источника к приемнику информации, и двунаправленных (bi-directional), открывающихся сразу в двух направлениях – от источника к приемнику информации и в обратном направлении.

Однонаправленные логические каналы открываются при помощи процедуры Uni-directional Logical Signalling (рис. 2.14).

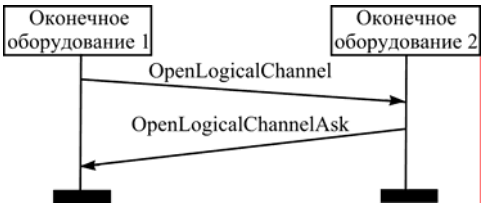


Рис. 2.14. Процедура открытия
однонаправленных логических каналов

В требовании открыть логический канал **openLogicalChannel** оборудование указывает вид информации, которая будет передаваться по этому каналу, и алгоритм кодирования информации. Если оборудование открывает однонаправленный логический канал то, чтобы организовать дуплексную связь, встречное оборудование также должно открыть однонаправленный канал в обратном направлении, используя для этого вышеописанную процедуру Uni-directional Logical Signalling.

В некоторых случаях оборудование, инициирующее такой обмен, должно открывать сразу и прямой, и обратный каналы. Делается это с помощью процедуры Bi-directional Logical Signalling, которая практически идентична вышеописанной процедуре Uni-directional Logical Signalling и также предусматривает обмен сообщениями **openLogicalChannel** и **openLogicalChannelAck**. Добавляется еще одно сообщение – **openLogicalChannelConfirm**, – которое передается в ответ на сообщение **openLogicalChannelAck** и подтверждает, что двунаправленный логический канал открыт (рис. 2.15).

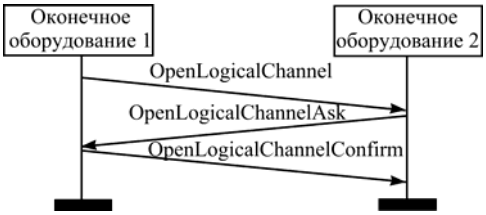


Рис. 2.15. Процедура открытия
двунаправленного логического канала

Закрытие логических каналов может производиться с помощью процедуры CloseLogicalChannel, но она используется, в основном, для поддержки предоставления дополнительных услуг, в первую очередь, услуги перевода соединения в режим удержания. Для нормального разрушения соединения стороны обмениваются сообщениями endSessionCommand. После обмена этими сообщениями закрываются не только логические каналы, но и управляющий канал H.245.

2.3. Контрольные вопросы

1. Перечислите основные функции привратника?
2. Каким требованиям должен удовлетворять терминал IP-телефонии?
3. Зачем нужен шлюз?
4. Какие виды конференций H.323 вы знаете?
5. Перечислить основные функции протокола RAS?
6. Для чего нужно сообщение ARQ в протоколе RAS?
7. В каком случае пользователь получит сообщение ARJ протокола RAS?
8. Перечислите основные сообщения H.225?
9. Когда посылается сообщение H.225 Setup?
10. Что означает H.225 Alerting с точки зрения абонента?
11. Как определяется ведущее и ведомое оборудование в H.245?
12. В чем разница между однонаправленными и двунаправленными логическими каналами H.245?
13. Что содержит сообщение H.245 TerminalCapabilitySet?

2.4. Контрольные задания

Задание 1. Нарисовать структуру сети на базе рекомендации H.323 (табл. 2.1).

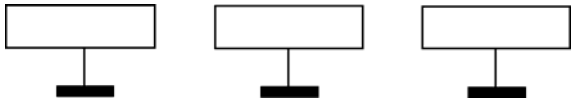
Таблица 2.1

Вариант	Аналоговые телефонные аппараты	Компьютерные терминалы	Зона	Операторы
1				
2				
3				

Пояснить принципы работы сети, взаимодействие устройств, функции, выполняемые каждым устройством.

Задание 2. Нарисовать полный сценарий взаимодействия двух устройств IP-телефонии с использованием команд и сообщений RAS: шлюз-шлюз, шлюз-привратник, терминал-привратник.

Задание 3. Нарисовать полный сценарий установления соединения с использованием команд и сообщений H.225.0: с привратником, без привратника.



Задание 4. Нарисовать полный сценарий взаимодействия 2 устройств IP-телефонии с использованием команд и сообщений H.245.

3. ПОСТРОЕНИЕ СЕТЕЙ IP-ТЕЛЕФОНИИ НА БАЗЕ ПРОТОКОЛА SIP

3.1. 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 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, 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. В качестве транспорта могут использоваться протоколы X.25, Frame Relay, AAL5, IPX и др. 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 (рис. 3.1).

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). Поскольку в течение сеанса связи может производиться его модификация, предусмотрена передача средствами SDP сообщений SIP с новыми описаниями сеанса.

Протокол инициирования сеансов связи (SIP)	Прикладной уровень
Протоколы TCP и UDP	Транспортный уровень
Протоколы IPv4 и IPv6	Сетевой уровень
PPP, AAL5 ATM, Ethernet, V.34	Уровень звена данных

Рис. 3.1. Место протокола SIP в стеке протоколов TCP/IP

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

3.2. Адресация

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, уже сейчас является основным адресом, не зависящим от местоположения пользователя.

Существует 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»).

SIP-адрес может соответствовать разным физическим адресам (в зависимости от времени суток, алгоритма работы и т. д.). Он может указывать одного определенного пользователя, направлять вызов к первому свободному из группы пользователей или ко всей группе. Благодаря этому можно организовать такие услуги, как «ночной вызов», «переадресация», «конференция» и др.

Возможно использование адреса электронной почты в качестве публикуемого SIP-адреса – применение URL позволяет размещать свой адрес на Web-страницах:

sip: user1@rts.niits.ru,
sip: user1@ 195.201.37.104,
sip: 273-44-55@gateway.ru.

3.3. 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.

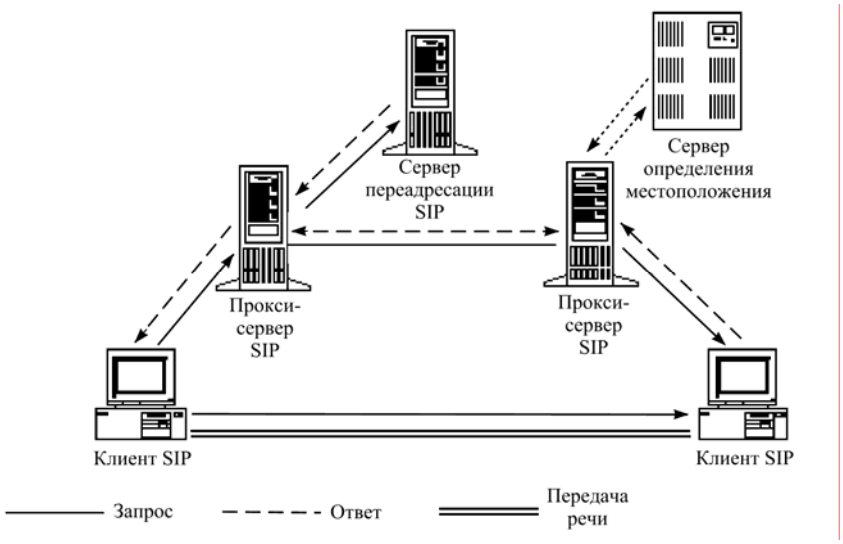


Рис. 3.2. Архитектура SIP-сети

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.

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 (рис. 3.2), где могут присутствовать некоторые элементы базы адресов, так и отдельно от него.

3.4. 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.

Все сообщения протокола SIP (запросы и ответы), представляют собой последовательности текстовых строк, закодированных в соответствии с документом RFC 2279. Структура и синтаксис сообщений SIP (рис. 3.3) идентичны используемым в протоколе HTTP.

Рис. 3.3. Структура сообщений протокола SIP

Стартовая строка представляет собой начальную строку любого SIP-сообщения. Если сообщение является запросом, в этой строке указываются тип запроса, адресат и номер версии протокола. Если сообщение является ответом на запрос, в стартовой строке указываются номер версии протоко-

ла, тип ответа и его короткая расшифровка, предназначенная только для обслуживающего персонала и необрабатываемая клиентом.

Заголовки сообщений содержат сведения об отправителе, адресате, пути следования и др., в общем, переносят информацию, необходимую для обслуживания данного сообщения. О типе заголовка можно узнать по его имени. Оно не зависит от регистра (т. е. буквы могут быть прописные и строчные), но обычно имя пишут с прописной буквы, за которой идут строчные.

Сообщения протокола SIP могут содержать так называемое тело сообщения. В сообщениях ACK, INVITE и OPTIONS тело сообщения содержит описание сеансов связи, например, в формате протокола SDP. Сообщение BYE тела сообщения не содержит, а ситуация с сообщением REGISTER подлежит дальнейшему изучению. С ответами дело обстоит иначе: любой ответ может содержать тело сообщения, но содержимое тела в ответах разных типов бывает разным.

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.

Имеются заголовки четырех видов:

- общие (есть и в запросах и ответах);
- содержания (они начинаются со слова **Content** и несут информацию о размере тела сообщения или об источнике, передавшем сообщение);
- запросов (несущие дополнительную информацию о запросе);
- ответов (несущие дополнительную информацию об ответе).

Заголовок содержит имя, за которым после двоеточия (:) следует поле, содержащее данные, заголовка:

имя: содержимое.

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.niits.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@niits.ru> tag=12345.

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

CSeq – уникальный идентификатор запроса внутри одного **Call-ID**, необходимый 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).

Запрос обрабатывается двумя прокси-серверами: сначала сервером niits.ru, потом – sip.telecom.com, тогда в нем появятся следующие поля:

Via: SIP/2.0/UDP sip.telecom.com:5060,
Via: SIP/2.0/UDP niits.ru:5060.

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

В настоящей версии протокола SIP определено 6 типов запросов. Каждый из них предназначен для выполнения довольно широкого круга задач, что является явным достоинством протокола SIP, так как благодаря этому число сообщений, которыми обмениваются терминалы и серверы, сведено к минимуму. 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 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 (рис. 3.4).

```
INVITE sip: watson@boston.bell-tel.com SIP/2.0
        Via: SIP/2.0/UDP kton.bell-tel.com
        From: A. Bell <sip: a.g.bell@bell-tel.com>
        To: T. Watson <sip: watson@bell-tel.com>
        Call-ID: 3298420296@kton.bell-tel.com
        Cseq: 1 INVITE
        Content-Type: application/sdp
        Content-Length: ...

        v=0
        o=bell 53655765 2353687637 IN IP4 128.3.4.5
        SIP=IN IP4 kton.bell-tel.com
        m=audio 3456 RTP/AVP 0 3 4 5
```

Рис. 3.4 Пример SIP-запросов

Этот запрос приглашает watson@bell-tel.com для участия в сеансе связи с a.g.bell@bell-tel.com. В теле сообщения отправитель указывает, что он может принимать на порт 3456 аудиоинформацию, кодированную 0 (PCMU), 3 (GSM), 4 (G.723) и 5 (DV14). Запрос направляется на прокси-

сервер boston.bell-tel.com. В полях To и From перед скобками с адресом (< >) помещена надпись, которую пользователь желает вывести на дисплей вызываемого пользователя.

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, но 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 6 типов ответов, несущих разную функциональную нагрузку. Тип ответа кодируется 3-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-значными 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 (рис. 3.5):

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.

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP kton.bell-tel.com
From: A. Bell <sip:a.g.bell@bell-tel.com>
To: <sip:watson@bell-tel.com>;
Call-ID: 3298420296@kton.bell-tel.com
Cseq: 1 INVITE
Content-Type: application/sdp
Content-Length: ...
v=0
o=watson 4858949 4858949 IN IP4 192.1.2.3
t=3149329600 0
SIP=IN IP4 boston.bell-tel.com
m=audio 5004 RTP/AVP 0 3
a=rtpmap:0 PCMU/8000
a=rtpmap:3 GSM/8000
```

Рис. 3.5. Пример SIP-ответов

В ответе пользователя Watson на запрос Bell сообщается, что он может принимать аудиоинформацию на порт 5004, понимает кодеки PCMU, GSM. Поля **From, To, Via, Call-ID** взяты из запроса. Поле **Cseq** показывает, что это – ответ на INVITE с Cseq: 1.

3.5. Процесс установления соединения

Сеть SIP содержит пользователей (правильно сказать UAS), прокси-серверы и серверы переадресации. Перед началом сеанса связи вызывающий пользователь должен знать либо адрес вызываемого пользователя, либо адрес SIP-сервера. Адрес может быть в виде user@domain, тогда необходимо преобразовать его в IP-адрес с помощью услуг DNS. Адреса

серверов пользователю сообщает поставщик услуги. Для доступа к серверу может потребоваться аутентификация, благодаря которой можно обеспечить обслуживание только определенной группы пользователей, например, тех, кто заплатил за услуги. Если прямого адреса пользователя нет, пользователь обращается к прокси-серверу или к серверу переадресации. Дальше алгоритм работы сети зависит от того, к какому серверу он обратился.

Сценарий установления соединения через сервер переадресации

Вызывающему пользователю требуется вызвать другого пользователя. Он передает запрос INVITE **1** на известный ему адрес сервера переадресации и на порт 5060, используемый по умолчанию (рис. 3.6).

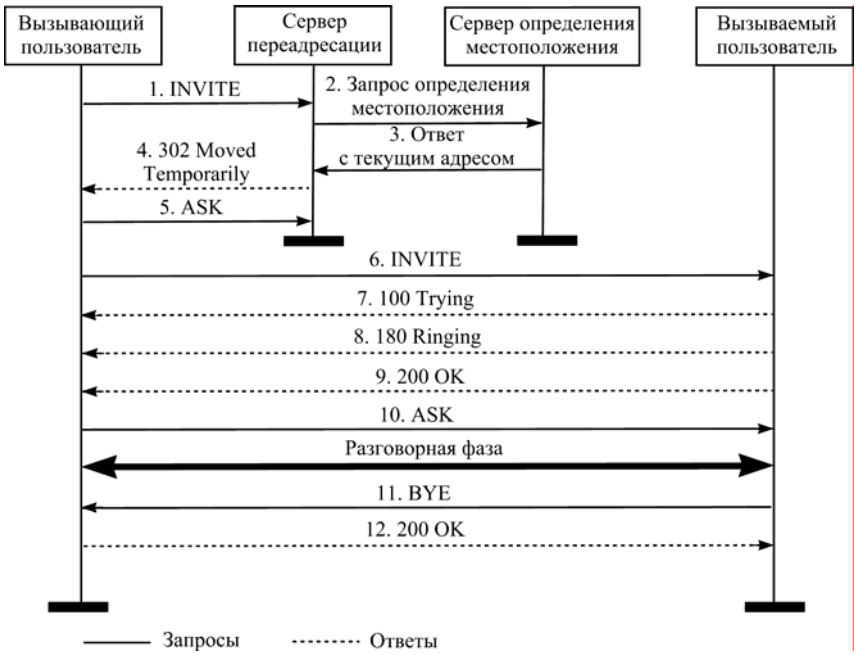


Рис. 3.6. Сценарий установления соединения через сервер переадресации

В запросе вызывающий пользователь указывает адрес вызываемого пользователя. Сервер переадресации запрашивает текущий адрес нужного пользователя у сервера определения местоположения **2**, который сообщает ему этот адрес **3**. Сервер переадресации в своем ответе 302 Moved temporarily передает вызывающей стороне текущий адрес вызываемого

пользователя **4**, или сообщает список зарегистрированных адресов вызываемого пользователя, предлагая вызывающему самому выбрать один из них. Вызывающая сторона подтверждает прием ответа 302 передачей сообщения ACK **5**.

Теперь вызывающая сторона может связаться с вызываемой стороной. Для этого она передает новый запрос INVITE **6**. В теле сообщения INVITE указываются данные о функциональных возможностях вызывающей стороны в формате протокола SDP. Вызываемая сторона принимает запрос INVITE и начинает его обработку, о чем сообщает ответом 100 Trying **7** встречному оборудованию для перезапуска его таймеров.

После завершения обработки поступившего запроса оборудование вызываемой стороны сообщает своему пользователю о входящем вызове, а встречной стороне передает ответ 180 Ringing **8**. После приема вызываемым пользователем входящего вызова встречной стороне передается сообщение 200 OK **9**, в котором содержатся данные о функциональных возможностях вызываемого терминала в формате протокола SDP. Терминал вызывающего пользователя подтверждает прием ответа запросом ACK **10**. На этом фаза установления соединения заканчивается, и начинается разговорная фаза.

По завершении разговорной фазы любая из сторон передает запрос BYE **11**, который подтверждается ответом 200 OK **12**.

Сценарий установления соединения через прокси-сервер

В этом случае действия **1, 2, 3** такие же, как и при использовании сервера переадресации. После выяснения адреса (на сервере определения местоположения) прокси-сервер передает по этому адресу запрос INVITE **4** (рис. 3.7). Вызываемый пользователь B оповещается акустическим или визуальным сигналом о том, что его вызывают **5**; он поднимает трубку, и ответ 200 OK отправляется к прокси-серверу **6**. Прокси-сервер переправляет этот ответ вызвавшему пользователю A **7**, последний подтверждает правильность приема, передавая запрос ACK **8**, который переправляется к вызванному пользователю B **9**. Соединение установлено, идет разговор. Вызванный пользователь B кладет трубку, передается запрос BYE **10**, прием которого подтверждается ответом 200 OK **11**.

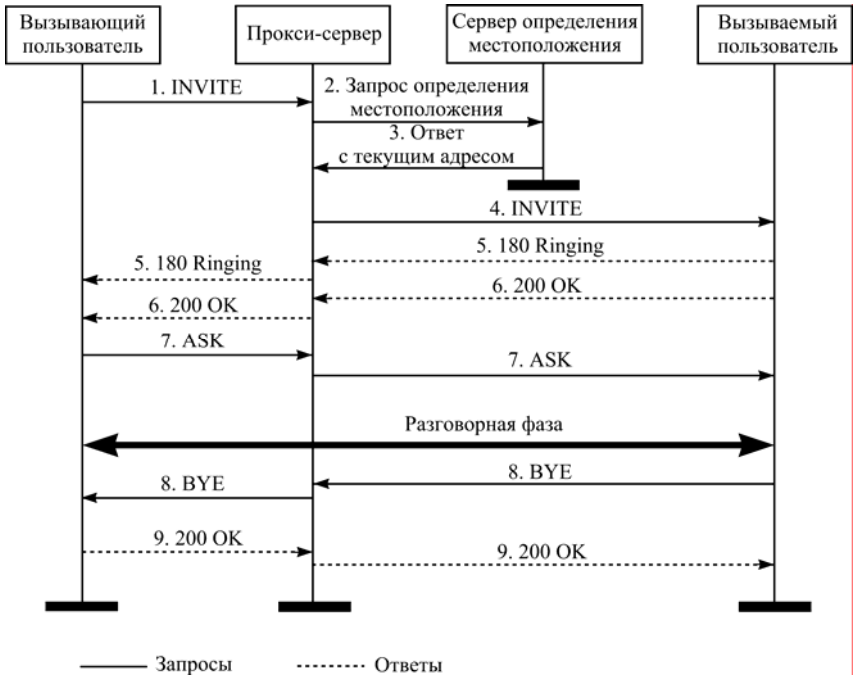


Рис. 3.7. Сценарий установления соединения через прокси-сервер

Контрольные вопросы

1. Зачем нужен протокол SIP?

2. Основные принципы, положенные в основу протокола SIP, кто его стандартизировал?

3. Какое место занимает протокол SIP в стеке протоколов TCP/IP.

4. С помощью какого протокола терминалы обмениваются информацией о своих функциональных возможностях?

5. Перечислить основные элементы SIP-сети.

6. Элементы SIP-сети. Их функции.

7. Агент пользователя. Из каких элементов он состоит.

8. Прокси-сервер. Типы прокси-серверов, их функции

9. Сервер переадресации. Функции.

10. Сервер определения местоположения. Функции.

11. Показать пример SIP-сети. Описать на нем в общем виде процесс установления соединения между терминалами.

12. Какой тип адресации используется в протоколе SIP.

13. Перечислить типы SIP-адресов, что значат их элементы?

14. Описать принцип «клиент-сервер».

15. Сообщения протокола SIP. Какой формат сообщений и их структура?

16. Какие существуют виды сообщений?

17. Назначение запросов протокола SIP.

18. Назначение ответов протокола SIP.

19. Пояснить назначение основных заголовков сообщений.

20. Описать процесс установления соединения с участием сервера переадресации

21. Описать процесс установления соединения с участием прокси-сервера

22. В чем разница двух сценариев?

23. В какие моменты времени терминалы пользователей посылают информацию о своих функциональных возможностях? В каких сообщениях эта информация располагается?

24. Какое минимальное число сообщений необходимо для установления соединения?

25. Как выглядел бы сценарий (рис. 8.2), если бы сервер определения местоположения не нашел пользователя?

Контрольные задания

Задание 1. Показать пример SIP-сети. Описать на нем в общем виде процесс установления соединения терминалов.

Задание 2. Для каждого варианта составить запрос и ответ применительно к сеансу связи вызывающего и вызываемого пользователей (табл. 3.1). Заголовки, которые нельзя составить на основе табл. 3.1, а также тело сообщения, оставить такими же, как на рис. 3.6 и 3.7.

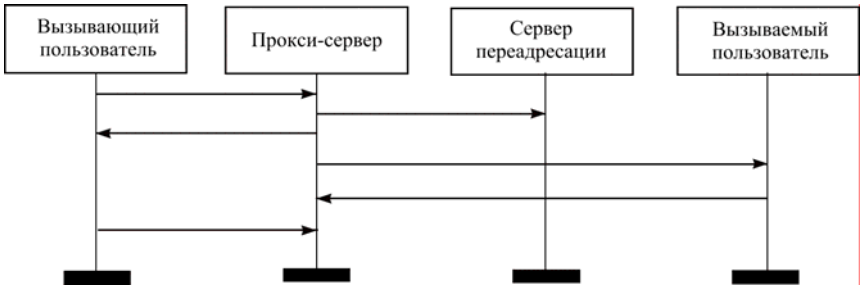
Таблица 3.1

Вариант	I	II	III	IV
Вызывающий пользователь	Имя: Director SIP-адрес: director@niits.ru	Имя: Andrew SIP-адрес: Andrew@sipserver.com	Имя: Bill Gaits SIP-адрес: bill@microsoft.com	Имя: User A SIP-адрес: userA@sip.edu
Вызываемый пользователь	Имя: engineer SIP-адрес: engineer@sip.niits.ru	Имя: Sasha SIP-адрес: sasha@sip.bell.org	Имя: V. Ivanov SIP-адрес: ivan@sip.telecom.ru	Имя: User B SIP-адрес: userB@sut.ru
Пройденные серверы	niits.ru sip.niits.ru	sipserver.com central.com bell.org	microsoft.com interconnect.com telecom.ru	bonch.edu cen-tralserver.ru
Тип запроса и ответа	INVITE, 200 OK	BYE, 302 Moved Temporarily	OPTION 404 Not Found	REGISTER 200 OK

Задание 3. Составить сценарий установления успешного соединения между терминалами пользователей A и B по данным табл. 3.2.

Таблица 3.2

Вариант	I	II	III	IV
Вид соединения	т. A → PS→ RS → PS →т. B	T. A → RS → PS → RS → т. B	т. A → PS→ PS →RS →т. B	т. A → RS → PS → PS → т. B
Сокращения: т. A/B – терминал A/B, PS – прокси-сервер, RS – сервер переадресации.				



4. ПРИНЦИП ДЕКОМПОЗИЦИИ ШЛЮЗА

4.1. Архитектура распределенного шлюза

Еще одним вариантом построения сетей IP-телефонии является распределенный 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. Первым протоколом, базирующемся на этом принципе и получившим широкое распространение, стал протокол управления шлюзами – Media Gateway Control Protocol (MGCP), разработанный комитетом IETF. Ранее подобный протокол под названием SGCP – Simple Gateway Control Protocol (простой протокол управления шлюзами) – был разработан компанией Telcordia (бывшая компания Bellcore). Фирма Level 3 предложила сходный протокол управления оборудованием, реализующим технологию маршрутизации пакетов IP, – IDCP (IP Device Control Protocol). Оба они впоследствии были объединены в протокол MGCP. Дальнейшие усилия комитета IETF, а также примкнувшего к нему союза ITU-T (Исследовательская группа 16) привели к созданию протокола H.248/MEGACO, который больше отвечает требованиям современных сетей и лишен недостатков уже устаревающего протокола MGCP (рис. 4.1).

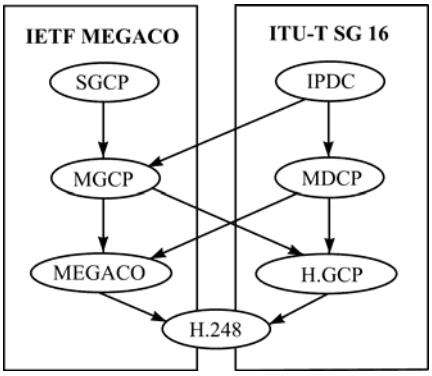


Рис. 4.1. Дерево эволюции протоколов управления шлюзами

Упомянутый принцип декомпозиции шлюза делит его на следующие функциональные блоки (рис. 4.2):

- транспортный шлюз (Media Gateway), выполняющий 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), обеспечивающий доставку сигнальной информации, поступающей со стороны ТфОП, к устройству управления шлюзом и перенос сигнальной информации в обратном направлении.

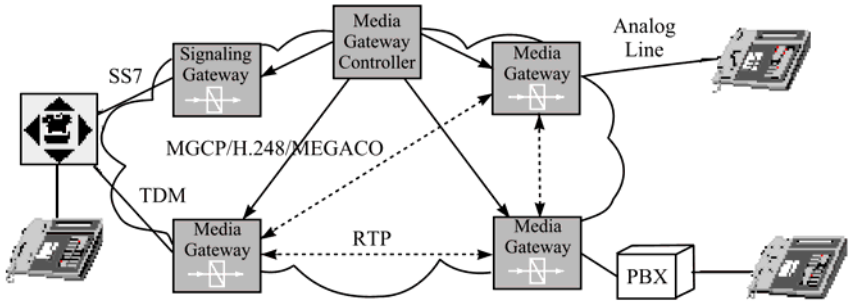


Рис. 4.2. Архитектура сети,
базирующейся на протоколе управления шлюзами

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. Рабочая группа MEGACO не определяет протокол синхронизации работы устройств управления, однако в ряде работ, посвященных исследованию возможностей протокола MGCP, для этой цели предлагается использовать протоколы H.323, SIP или ISUP/IP.

4.2. Протокол MGCP

Протокол MGCP широко популярен в сетях построенных согласно архитектуре распределенного шлюза. Он долгое время удовлетворял все потребности операторов по соединению сетей IP и ТфОП. Тот факт, что он был разработан комитетом IETF, позволил ему быстро стать стандартной технологией. Протокол включает в себя модель установления соединения, команды с различными параметрами, объединенные в дескрипторы, и позволяющие контроллеру управлять медиашлюзом для установления межсетевого соединения. Однако с развитием мультимедийных услуг выявился ряд функциональных недостатков этого протокола и несовершенство модели установления соединения, поэтому будущее развитие технологии управления распределенным шлюзом связывается с более совершенным протоколом MEGACO/H.248.

4.3. 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 (рис. 4.3), отличную от модели MGCP. Протокол MEGACO оперирует с двумя логическими сущностями внутри транспортного шлюза: окончание (termination) и контекст (context), которыми может управлять контроллер шлюза.

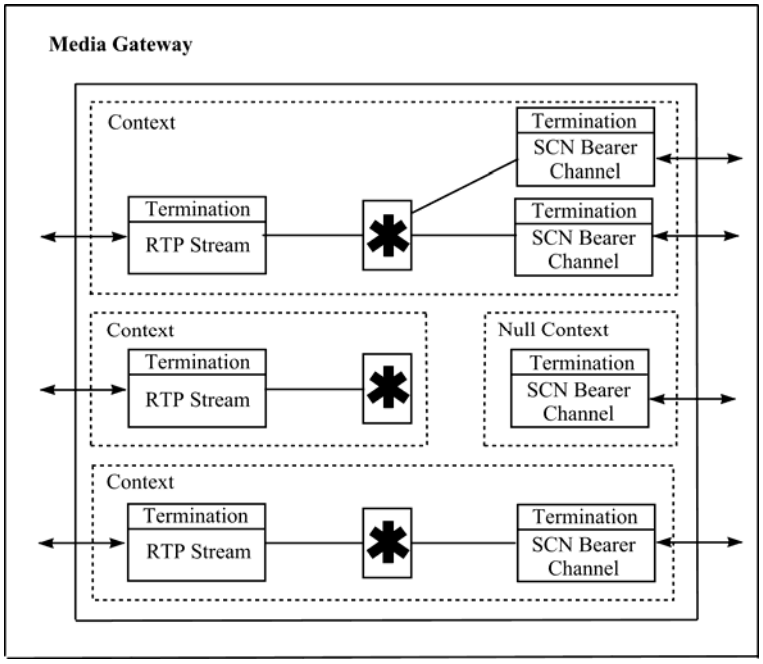


Рис. 4.3. Примеры модели процесса обслуживания вызова

4.3.1. Окончания (Terminations)

Окончания (в русскоязычной литературе часто встречается термин *порты*) являются источниками и приемниками медиаинформации. Они являются логическими объектами медиашлюза. Можно выделить два вида окончаний в зависимости от того, какой интерфейс они представляют – 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». Также используется механизм групповых символов wildcard: ALL и CHOOSE. Первый позволяет адресоваться сразу к нескольким окончаниям одновременно, а последний позволяет предоставить право выбора любого подходящего окончания шлюзу.

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.

Существует ряд общих свойств окончаний и ряд свойств, относящихся к медиапотокам. Общие свойства называются свойствами состояния окончания. Свойства, которые не могут быть описаны базовым протоколом, определяются в «пакетах» о которых будет сказано ниже.

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

4.3.2. Контекст (Context)

Контекст – это отображение связи между несколькими окончаниями, т. е. 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 (незанятого) 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, включенных 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 передает 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 первоочередную 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.

4.4. Сообщения протокола H.248/MEGACO

4.4.1. Дескрипторы

Рассмотрение структуры информационных элементов протокола начинается 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, т. е. 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 (табл. 4.1).

Определенные в протоколе дескрипторы перечислены в табл. 4.1.

Таблица 4.1

Дескриптор	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

Окончание табл. 4.1

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 контроле-ром
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.

4.4.2. Команды

Команды протокола обеспечивают управление логическими единицами модели обслуживания вызова – контекстами и окончаниями.

Таблица 4.2

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 (Проверить окончание)	MGC → MG	Контроллер запрашивает свойства 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

Команды позволяют управлять свойствами контекстов и окончаний. Большинство команд могут передаваться только контроллером, за исключением команд Notify и ServiseChange. Приведем полный список используемых команд (табл. 4.2).

4.4.3. Транзакции

Команды, передаваемые между MGC и MG группируются в транзакции, каждая из которых снабжается идентификатором TransactionID, необходимым 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, причем область всех этих операций должен ограничиваться одним контекстом (рис. 4.4).

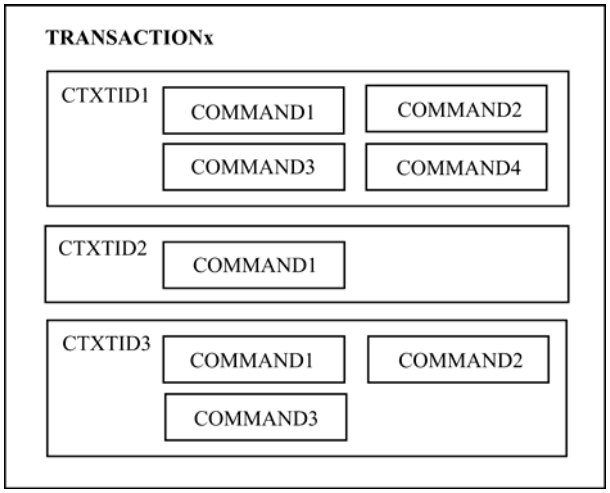


Рис. 4.4. Иерархия в пределах транзакции

4.4.4. 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. Со-

общение H.248 – это, по сути, только транспортный механизм, в отличие от сообщений многих других сетевых протоколов, имеющих собственные функции (рис. 4.5).

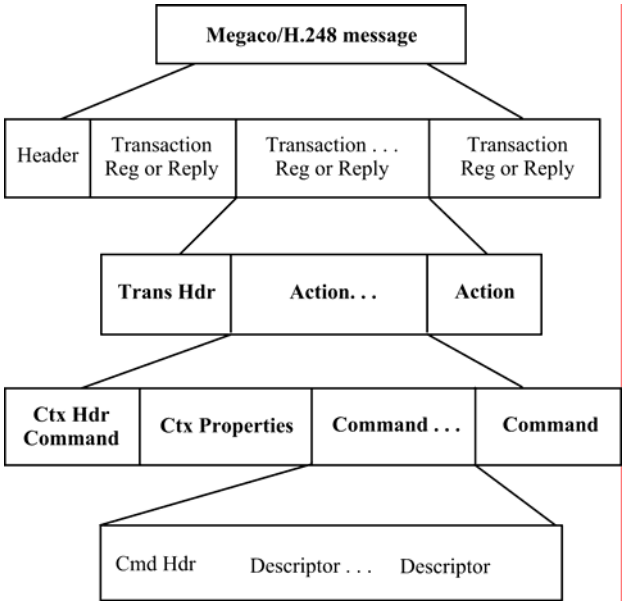


Рис. 4.5. Структура сообщений H.248/MEGACO

4.4.5. Пакеты (Packages)

Разные типы шлюзов могут иметь различные окончания, сильно разнящиеся по характеристикам. Для сглаживания таких различий протокол позволяет окончаниям иметь опциональные свойства, события, сигналы и статистику, реализуемые шлюзом. Для обеспечения возможности взаимодействия MG и MGC такие опции группируются в «пакеты» или Packages, и обычно окончание выполняет или реализует ряд таких «пакетов». Контроллер может запросить у шлюза статистику, чтобы знать, какие пакеты он может выполнять.

Пакет – это отдельная рекомендация, в которой описываются свойства, события, сигналы и статистика и все процедуры, с ними связанные. Например, если описывается событие, такое как обнаружение неис-

правности соединения, в пакете перечисляются действия, которые шлюз должен выполнить при его обнаружении.

Для того, чтобы поддерживать конкретный пакет, MG должен поддерживать все свойства, сигналы, события и статистику, определенную в нем.

4.5. Процедура установления и разрушения соединения

Установление и разрушение соединения в MEGACO/H.248, как и в большинстве сетевых протоколов, варьируется в зависимости от ситуации на сети и участвующих сторон.

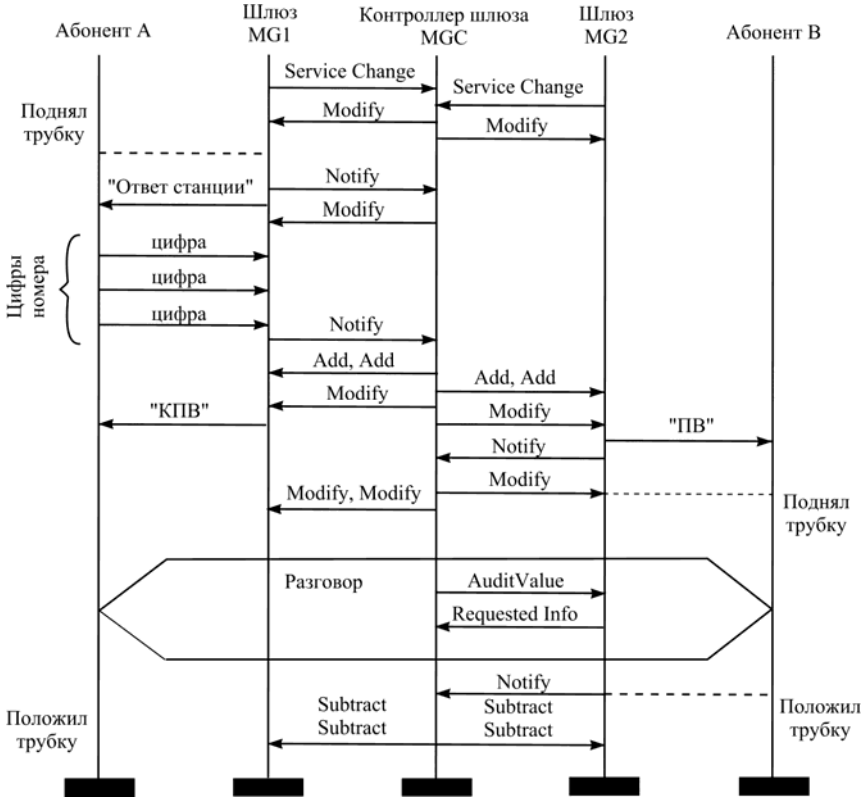


Рис 4.6. Алгоритм установления и разрушения соединения
с помощью протокола MEGACO

Одним из базовых вызовов является сценарий установления соединения между двумя резидентными шлюзами.

Резидентные шлюзы – это такие шлюзы, в которые включаются 1–2 абонентские линии, т. е. они отвечают за сопряжение 1–2 абонентских терминалов с сетью IP-телефонии. Наибольшее распространение такой сценарий нашел в корпоративном секторе.

Другим типом шлюза является транспортный шлюз – шлюз, который соединяет сети ТфОП и IP, т. е. в него включаются не абоненты, а СЛ к телефонным станциям.

В нашем случае через сеть IP-телефонии взаимодействуют два аналоговых терминала, включенных в резидентные шлюзы.

1. Шлюз MG1 регистрируется у контроллера MGC при помощи команды ServiceChange.

2. Контроллер подтверждает регистрацию шлюза, высылая ответ на команду ServiceChange.

3. Шлюз имеет свободные аналоговые порты, которые должны быть запрограммированы для отслеживания изменения сопротивления абонентского шлейфа, означающего поднятие абонентом трубки, после чего шлюз должен передать абоненту акустический сигнал «Ответ станции». Программирование производится при помощи команды Modify с соответствующими параметрами (указанными в дескрипторах), причем программируется порт, находящийся в нулевом контексте. В команде указывается режим функционирования порта –дуплексный (SendReceive).

4. Шлюз MG1 подтверждает выполнение команды Modify.

5. Подобным же образом (шаги 1–4) программируется аналоговый порт шлюза MG2.

6. Далее шлюз MG1 обнаруживает, что абонент А поднял трубку, и извещает об этом событии Media Gateway Controller при помощи команды Notify.

7. Контроллер подтверждает получение команды Notify.

8. На следующем шаге MGC, командой Modify дает шлюзу инструкцию накапливать цифры номера вызываемого абонента. Кроме того, после получения первой цифры номера необходимо остановить передачу акустического сигнала «Ответ станции».

9. Шлюз подтверждает получение команды Modify.

10. Цифры номера вызываемого абонента собираются шлюзом MG1, после чего передаются к контроллеру в команде Notify.

11. Полученное сообщение подтверждается шлюзом.

12. Далее контроллер MGC анализирует цифры номера вызываемого абонента, полученные от шлюза MG1, и определяет, что соединение должно проходить через шлюз MG2, к которому подключен вызываемый абонент. К вновь образованному контексту в шлюзе MG1 добавляются при помощи команды Add физический порт (аналоговый абонентский интерфейс) и виртуальный порт (RTP-порт). В этот момент шлюз, к которому прикреплен вызывающий абонент, не имеет информации о шлюзе MG2 (такой как IP-адрес, RTP-порт и поддерживаемые алгоритмы декодирования принимаемой речевой информации), поэтому контроллер MGC предписывает шлюзу MG1 только принимать информацию (режим ReceiveOnly). Кроме того, контролер MGC специфицирует в команде Add предпочтительные для использования алгоритмы кодирования.

13. Шлюз MG1 создает новый виртуальный порт (RTP-порт) и указывает его транспортный адрес. Кроме того, шлюз выбирает алгоритмы кодирования информации, которые будут использоваться в соединении, основываясь на предпочтениях контроллера.

14. Контроллер MGC посылает команду Add и создает в шлюзе MG2 контекст для установления дуплексного соединения (режим SendReceive) с вызывающим пользователем.

15. Создание контекста подтверждается, физический порт шлюза MG2 соединяется с указанным UDP/RTP портом. Отметим, что RTP-порт имеет номер отличный от номера порта Megaco/H.248, по которому производится сигнальный обмен.

16. Контроллер, командой Modify предписывает шлюзу MG1 начать передачу вызывающему абоненту акустического сигнала «Контроль посылки вызова (КПВ)».

17. Шлюз MG1 подтверждает передачу указанного акустического сигнала в физический порт.

18. Контроллер MGC предписывает физическому порту шлюза MG2 начать передачу вызывного сигнала.

19. Шлюз MG2 подтверждает передачу сигнала «Посылка вызова» вызываемому абоненту.

20. На этом этапе обоим абонентам, участвующим в соединении, посылаются соответствующие сигналы, и шлюз MG2 ждет, пока вызы-

ваемый абонент примет входящий вызов, после чего между двумя шлюзами будут организованы двунаправленные разговорные каналы.

21. Шлюз MG2 обнаружил, что вызываемый абонент поднял трубку, и извещает об этом контроллер MGC командой Notify.

22. Контроллер подтверждает получение команды Notify.

23. Далее контроллер MGC командой Modify предписывает шлюзу MG2 прекратить передачу вызывного сигнала.

24. Шлюз MG2 подтверждает выполнение команды.

25. Далее, контроллер командой Modify разрешает шлюзу MG1 не только принимать, но и передавать информацию (режим SendReceive), и останавливает передачу вызывающему абоненту акустического сигнала «КПВ».

26. Шлюз MG1 подтверждает выполнение команды.

27. После этого начинается разговорная фаза соединения, в течение которой участники обмениваются речевой информацией. Следующим шагом контроллер MGC может проверить RTP-порт в шлюзе MG2, отправив команду AuditValue.

28. Шлюз MG2 выполняет команду. В ответе на команду AuditValue передается вся запрашиваемая информация, в том числе статистика, собранная за время соединения.

29. Вызываемый абонент первым завершает соединение, и шлюз MG2 извещает об этом контроллер MGC командой Notify.

30. Контроллер MGC подтверждает получение сообщения Notify.

31. Получив информацию от любого из шлюзов о том, что один из абонентов положил трубку, контроллер MGC завершает соединение. К обоим шлюзам передается команда Subtract.

32. В ответе на команду Subtract каждый из портов, участвующих в соединении на шлюзах MG1 и MG2, возвращает статистику, собранную за время соединения. В общем случае, контроллер может запрашивать статистическую информацию только у одного из портов.

4.6. Контрольные вопросы

1. Функция протоколов MGCP и MEGACO
2. Кто разработал протокол MEGACO?
3. Функциональные элементы распределенного шлюза.

4. Показать пример сети на базе архитектуры распределенного шлюза.

5. Почему решили разработать MEGACO взамен MGCP?

6. Какими логическими объектами оперирует модель установления соединения MEGACO?

7. Какими атрибутами обладает контекст?

8. Что такое дескрипторы? Их назначение.

9. Что описывает дескриптор LocalControl?

10. Назначение команды Add.

11. Структура сообщений MEGACO

12. Что такое «пакеты» MEGACO?

4.7. Контрольные задания

Задание 1. Как изменится сценарий работы протокола MEGACO если в процедуре, описанной в п. 4.5, вместо резидентных шлюзов будут стоять транспортные, включенные в цифровые АТС и поддерживающие ОКС7?

5. ЛАБОРАТОРНЫЕ РАБОТЫ

5.1. Принципы построения шлюза IP-телефонии

Для проведения этих лабораторных работ рекомендуется использовать учебную лабораторную установку шлюза «Протей». Последующие лабораторные работы включают изучение процедур установления соединений, операционной системы Linux, на которой построено программное обеспечение шлюза, и техобслуживания.

Каждая лабораторная работа содержит теоретическую часть и практические задания, выполняемые на терминале шлюза Протей-ITG.

После выполнения лабораторной работы необходимо составить отчет и ответить на контрольные вопросы.

5.1.1. Основы построения шлюза

Шлюз Протей-ITG (рис. 5.1) предназначен для организации доступа абонентов существующей телефонной аналого-цифровой сети общего пользования к сети Интернет через цифровую коммутационную станцию в соответствии с требованиями Минсвязи России к аппаратуре, реализующей функции передачи речевой информации по сетям передачи данных с протоколом IP.

Рис. 5.1. Шлюз Протей-ITG
производства ЛОНИИС

Основным функциональным назначением шлюза является преобразование речевой информации, поступающей со стороны ТфОП с постоянной скоростью передачи, в вид, пригодный для передачи по сетям с маршрутизацией пакетов IP.

Шлюз может использоваться операторами связи (сервис-провайдерами) для предоставления услуг IP-телефонии посредством доступа к сети Интернет.

Оборудование шлюза реализует передачу речевого трафика и факсимильной информации по сетям с маршрутизацией пакетов IP в соответствии с рекомендацией ITU-T H.323 v2, выполняя функции:

* кодирования и упаковки речевой информации в пакеты RTP/UDP/IP;

* конвертирования сигнальных сообщений систем сигнализации E-DSS1и ОКС-7 (ISUP-R – российская версия) в сигнальные сообщения H.323 и обратного преобразования в соответствии с рекомендацией ITU-T H.246;

* обработки сигналов DTMF; распознавания и обработки тоновых сигналов.

В оборудовании шлюза реализованы функции поддержки настройки параметров с использованием обычного Web-браузера (Web-администрирование).

Для работы шлюза в сети IP-телефонии без привратника реализована функция преобразования номера ТфОП в IP-адрес.

Оборудование шлюза обеспечивает совместимость с H.323 шлюзами (Cisco) и клиентскими программами (Microsoft Netmeeting 3.0).

Состав лабораторной установки

В состав оборудования (рис. 5.2) шлюза входят:

- материнская плата с процессором (Celeron 500 MHz) и оперативной памятью (64Мбайт);

- жесткий диск (10 Гбайт),

- плата внутрисистемного интерфейса, обеспечивающая аппаратную обработку речевого пакетизированного сигнала и обработку HDLC по сигнальным каналам;

- плата преобразования речи (количество плат зависит от числа подключенных ИКМ-трактов);

- кабель для подключения ИКМ-трактов;

- сетевая плата (2), обеспечивающая сетевой интерфейс;

- плата ОКС, обеспечивающая обработку сигнализации ОКС7 и согласование с платой внутрисистемного интерфейса.

Программное обеспечение лабораторной установки (табл. 5.1) можно разделить на:

- системное;

- взаимодействия с пользователем через Web-интерфейс (далее – интерфейс пользователя);

- собственно шлюза, обеспечивающее обработку вызовов.

Таблица 5.1

Компоненты ПО	Характеристика
Системное программное обеспечение: - операционная система	Red Hat Linux 6.2
Интерфейс техобслуживания	telnet
ПО управления функциями шлюза: - модуль телефонной сигнализации (DSS1, SS7), - модуль сигнализации H.323, - модуль обработки вызова, - модуль обработки сигнализации ОКС7	ПО диалогового режима

Плата преобразования речи выполняет функции подготовки речевого сигнала, поступающего из ТфОП/ЦСИО для дальнейшей его передачи по сети с маршрутизацией пакетов IP. Основными функциями платы являются: преобразование речевого сигнала в соответствии с алгоритмом кодирования (G.711, G.723.1, G.726, G.728, G.729), обнаружение активных периодов и пауз в речи, адаптация воспроизведения и эхокомпенсация. Кроме того, в модуле реализованы функции детектирования и генерации сигналов DTMF, а также обработки факсимильных и модемных сигналов.

Плата ИКМ обеспечивает физический стык по G.703 шлюза с цифровой системой передачи E1.

Плата интерфейса с телефонной сетью обеспечивает интерфейс с материнской платой, а также взаимодействие платы ИКМ и платы преобразования речи.

Материнская плата содержит процессор (Celeron, 500 МГц), жесткий диск, (10 Гбайт), оперативную память (64 Мбайт) и обеспечивает согласованную работу всех плат шлюза.

Сетевые платы обеспечивают стык шлюза с сетью, использующей технологию пакетной передачи. *Сетевая плата 1* обеспечивает интерфейс

с сетью оператора IP-телефонии. *Сетевая плата 2* обеспечивает интерфейс с оператором системы техобслуживания сети. В упрощенной учебной установке шлюз содержит только одну сетевую плату.

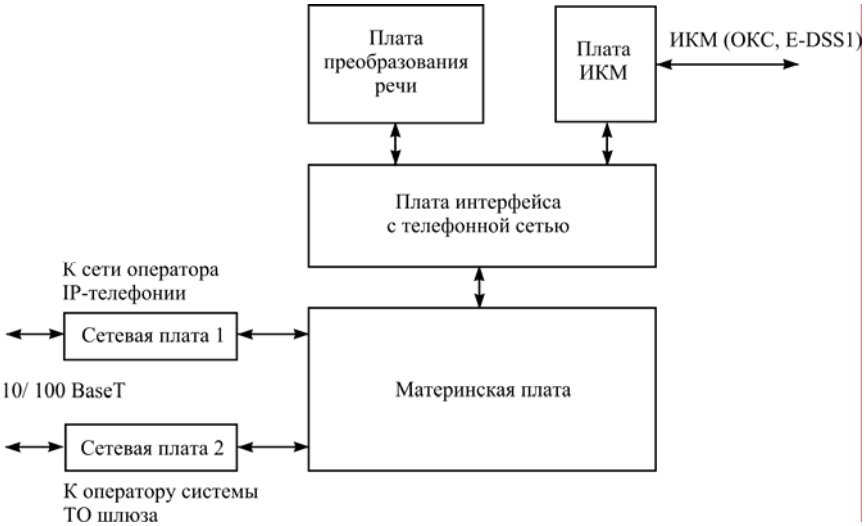


Рис. 5.2. Структурная схема шлюза «Протей-ITG»

Оборудование шлюза реализует передачу речевого трафика и факсимильной информации по сетям с маршрутизацией пакетов IP в соответствии с рекомендацией ITU-T H.323 v2, выполняя функции:

- кодирования и упаковки речевой информации в пакеты RTP/UDP/IP;

- конвертирования сигнальных сообщений систем сигнализации E-DSS1 и ОКС7 (ISUP-R – российская версия) в сигнальные сообщения H.323 и обратного преобразования в соответствии с рекомендацией ITU-T H.246;

- обработки сигналов DTMF; распознавания и обработки тоновых сигналов.

Для работы шлюза в сети IP-телефонии без привратника реализована функция преобразования номера ТфОП в IP-адрес.

Оборудование шлюза обеспечивает совместимость с H.323 шлюзами (Cisco) и клиентскими программами (Microsoft Netmeeting 3.0).

Общие технические характеристики шлюза приведены в табл. 5.2.

Таблица 5.2

Наименование характеристики	Значение
1	2
Емкость системы	До 2 трактов E1
Интерфейс оборудования для подключения к сети ТфОП. Параметры физического уровня: - скорость цифрового потока, кбит/с - линейный код - амплитуда импульса на нагрузке 120 Ом, В - ширина импульса, нс	Симметричный, 120 Ом (рек. ITU-T G.703) 2048±0,1 HDB3 3±0,3 244±25
Скорость передачи данных, кбит/с	30×64 (PRI)
Интерфейс оборудования для подключения к сети с маршрутизацией пакетов IP	Ethernet 10/100 BaseT
Протоколы	TCP/IP, RTP/RTCP, UDP
Системы сигнализации	H.323 v2, H.225 (RAS, Q.921), H.245; DSS1 (Q.921, Q.931); ОКС7 (Российские национальные спецификации ISUP-R, MTP)
Алгоритмы кодирования речи	G.711, G.723.1, G729
Питание: - напряжение, В - частота, Гц	 60 ± 6 50 ± 2,5
Техническое обслуживание	telnet

Характеристики аппаратной части шлюза приведены в табл. 5.3.

Таблица 5.3

Устройство	Характеристика
Процессор	Celeron, 500 MHz
Жесткий диск, Гбайт	10
Оперативная память, Мбайт	64

Характеристики ИКМ-платы приведены в табл. 5.4.

Таблица 5.4

Характеристики платы	Значение
Интерфейс	Цифровой интерфейс ИКМ-30
Скорость передачи	2048 кбит/с
Линейный код	HDB3
Электрические характеристики интерфейса	G.703(симметричный)

Шлюз Протей-ITG подключается к опорной АТС по линиям первичного доступа PRI (уровень 1 в соответствии с рекомендацией ITU-T-T I.431 и стандартом ETSI ETS 300 011) с использованием системы сигнализации DSS1 (уровень 2 в соответствии с рекомендацией ITU-T-T Q.921, уровень 3 в соответствии с рекомендацией ITU-T-T Q.931) и системы сигнализации ОКС 7 (ISUP). К сетям с маршрутизацией пакетов IP шлюз подключается при помощи интерфейса Ethernet 10/100BaseT.

5.1.2. Задание на лабораторную работу

Отчет должен содержать структурную схему шлюза, описание его назначения и основных блоков. При защите необходимо ответить на контрольные вопросы.

Контрольные вопросы

1. Пояснить назначение шлюза «Протей-ITG».
2. Перечислить основные компоненты шлюза, пояснить их назначение.
3. Как шлюз подключается к телефонной сети, а как к сети коммутации IP-пакетов?
4. Какие системы сигнализации поддерживает шлюз (со стороны ТфОП и со стороны IP-сети)?
5. Перечислить функциональные характеристики шлюза.
6. Нарисовать схемы подключения шлюза и их соединения между собой.

5.2. Сценарий установления соединения шлюзом без привратника

5.2.1. Теоретический материал

Типовой сценарий установления соединения без привратника показан на рис. 5.3

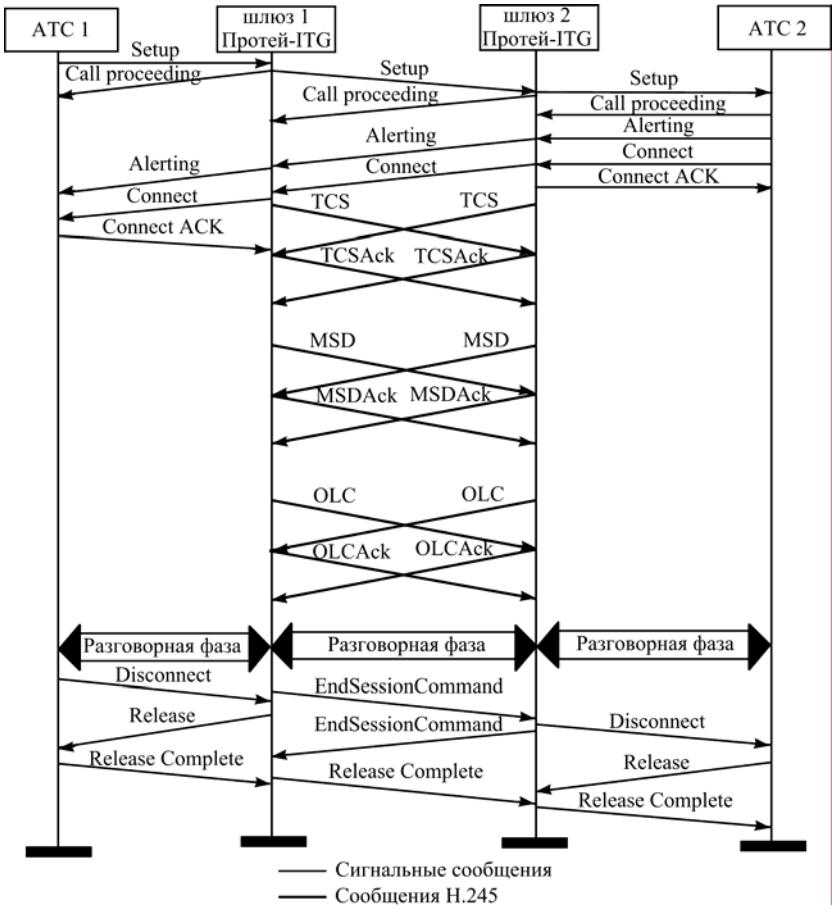


Рис. 5.3. Типовой сценарий установления соединения без привратника

АТС 1 посылает сообщение Q.931 Setup на шлюз 1, в котором указывается номер вызывающего и вызываемого пользователей. Шлюз 1 принимает сообщение Q.931 Setup, обрабатывает его на основании адресной информации, находящейся в поле Called Party Number. ПО шлюза

обращается к файлу *callroute.cfg* (см. работу 3), по которому определяется IP-адрес встречного шлюза и который может обслужить данный вызов. Шлюз 2 принимает сообщение, если IP-адрес (или часть адреса), с которого оно передано, находится в файле *permissions.cfg*. Из сообщения H.225 Setup берется номер вызываемого пользователя, который (номер) отправляется в сообщении Q.931 Setup на АТС 2. Вызываемое оборудование отвечает на Setup сообщением Call Proceeding.

Вызываемому абоненту выдается сигнал посылки вызова, а на шлюз 2 передается сообщение Q.931 Alerting. Шлюз 2 посылает сообщение H.225 Alerting шлюзу 1. На АТС 1 передается сообщение Q.931 Alerting, а абоненту А выдается сигнал контроль посылки вызова (КПВ). После ответа АТС 2 генерирует сообщение Q.931 Connect. Шлюз 2 подтверждает прием Q.931 Connect сообщением Q.931 Connect ACK. Шлюз 2 посылает сообщение H.225 Connect шлюзу 1 с указанием транспортного адреса управляющего канала H.245, после чего он открывается. Шлюз 1 генерирует сообщение Q.931 Connect и посылает его АТС 1. После получения транспортного адреса управляющего канала H.245, устанавливается TCP-соединение, по которому передаются сообщения протокола H.245.

После открытия управляющего канала H.245 начинается обмен данными о функциональных возможностях оборудования. Шлюзы обмениваются сообщениями TerminalCapabilitySet, в которых указываются возможные алгоритмы декодирования принимаемой информации. Следует отметить, что сообщение TerminalCapabilitySet должно быть первым сообщением, передаваемым по управляющему каналу. Оборудование, принявшее сообщение TerminalCapabilitySet от другого оборудования, подтверждает его получение передачей сообщения TerminalCapabilitySetAck.

Затем инициируется процедура определения ведущего/ведомого оборудования, необходимая для разрешения конфликтов, возникающих между двумя устройствами при организации конференции, когда оба они могут быть активными контроллерами конференций, или между двумя устройствами, пытающимися одновременно открыть двунаправленные логические каналы. В ходе процедуры устройства обмениваются сообщениями **masterSlaveDetermination**.

В ответ на полученные сообщения **masterSlaveDetermination** оба устройства передают сообщения **masterSlaveDeterminationAck**, в кото-

рых указывается, какое из этих устройств является для данного соединения ведущим, а какое – ведомым.

После обмена данными о функциональных возможностях и определения ведущего и ведомого оборудования может выполняться процедура открытия однонаправленных логических каналов. В требовании открыть логический канал (в нашем случае – прямой логический канал) **openLogicalChannel** оборудование указывает вид информации, который будет передаваться по этому каналу, и алгоритм кодирования. В ответ на сообщение **openLogicalChannel** оборудование должно передать подтверждение **openLogicalChannelAck**, указывающее транспортный адрес, на который передающей стороне следует посылать RTP пакеты, а также транспортный адрес канала RTCP.

Далее открывается разговорная сессия. Оборудование вызывающего пользователя передает речевую информацию, упакованную в пакеты RTP/UDP/IP, на транспортный адрес RTP-канала оборудования вызванного пользователя, а вызванный пользователь передает пакетизированную речевую информацию на транспортный адрес RTP-канала оборудования вызывающего пользователя. При помощи канала RTCP ведется контроль передачи информации по RTP каналам.

После окончания разговорной фазы начинается фаза разрушения соединения. Оборудование пользователя, инициирующего разъединение, прекращает передачу речевой информации, закрывает логические каналы и передает по управляющему каналу сообщение H.245 endSessionCommand, означающее, что пользователь хочет завершить соединение. Ожидается сообщение endSessionCommand от встречного оборудования, после чего управляющий канал H.245 закрывается. Следующим шагом, если сигнальный канал открыт, передается сообщение Release Complete, и сигнальный канал закрывается.

Пользователь, получивший команду endSessionCommand от пользователя, инициировавшего разъединение, должен прекратить передачу речевой информации, закрыть логические каналы и передать сообщение endSessionCommand. Далее, если сигнальный канал остался открытым, передается сообщение Release Complete, сигнальный канал закрывается, и обслуживание вызова считается завершенным.

Более подробную информацию о процессе установления соединения можно найти в [1, 6].

5.2.2. Задание на лабораторную работу

Отчет должен содержать сценарий установления соединения. При защите необходимо пояснить назначение каждого из представленных сообщений и ответить на контрольные вопросы.

Контрольные вопросы

1. Стандарт H.323. Архитектура сети IP-телефонии на основе рекомендации H.323.
2. Стандарт H.323. Элементы сети IP-телефонии на основе рекомендации H.323.
3. Сигнализация H.323: Сигнальный канал H.225.0 (функции, основные команды).
4. Сигнализация H.323: Управляющий канал H.245 (функции, основные команды).

5.3. Сценарий установления соединения шлюзом с привратником

5.3.1. Теоретический материал

Данный сценарий похож на сценарий рис. 5.3, за исключением начальной и конечной фаз установления соединения. Для взаимодействия с привратником используется протокол RAS. После приема сообщения Q.931 Setup шлюз 1 с помощью протокола RAS обращается к привратнику (рис. 6.4) за доступом к сетевым ресурсам (сообщение ARQ).

Если привратник разрешает использовать сетевые ресурсы шлюзу, он посылает ему сообщение ACF.

То же самое происходит на втором шлюзе при приеме сообщения H.225 Setup.

При завершении сеанса связи шлюзы посылают сообщение DRQ на привратник, который подтверждает их прием сообщением DCF.

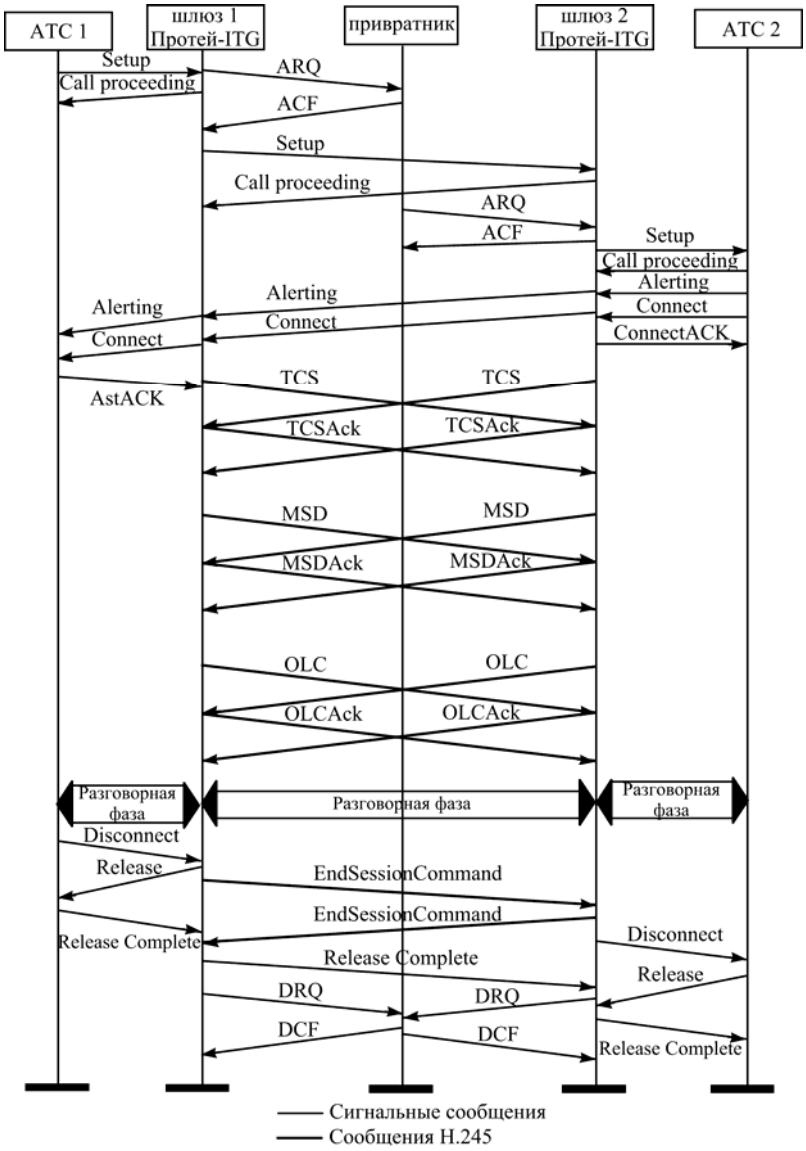


Рис. 5.4. Типовой сценарий установления соединения с участием привратника

5.3.2. Задание на лабораторную работу

Отчет должен содержать сценарий установления соединения. При защите необходимо пояснить назначение каждого из представленных сообщений и ответить на контрольные вопросы.

Контрольные вопросы

1. В чем отличие сценариев с участием и без участия привратника?
2. Какие функции выполняет привратник?
3. Какие функции выполняет протокол RAS?
4. Зачем необходимы сообщения ARQ и ACF, DRQ и DCF?

5.4. Изучение операционной системы Linux

5.4.1. Теоретический материал

Linux – это современная Unix – подобная операционная система для персональных компьютеров и рабочих станций. Это многопользовательская сетевая операционная система с сетевой оконной графической системой X Window System. ОС Linux поддерживает стандарты открытых систем и протоколы сети Internet и совместима с системами Unix, DOS, MS Windows. Все компоненты системы, включая исходные тексты, распространяются с лицензией на свободное копирование и установку для неограниченного числа пользователей. ОС Linux широко распространена на платформах Intel PC 386/486/Pentium/Pentium Pro. Разработка ОС Linux выполнена Линусом Торвалдсом из университета Хельсинки и большой командой из тысяч пользователей сети Internet, сотрудников исследовательских центров, фондов, университетов и т. д.

Техобслуживание шлюза осуществляется посредством удаленного доступа к нему через локальную сеть с использованием протокола telnet. Для этого необходимо иметь персональный компьютер со специализированным ПО протокола.

В качестве такого ПО может служить встроенное в операционные системы семейства MICROSOFT® WINDOWS приложение, реализующее протокол telnet (вызывается с помощью команды telnet). Для лабораторной работы используется более удобная программа PuTTY (рис. 5.5).

Из списка устройств необходимо выбрать шлюз «Протей-ITG» (конкретное устройство укажет преподаватель). Для соединения с ним необходимо дважды нажать кнопку на соответствующем имени в поле Stored Sessions. После этого появится окно (рис. 5.6). Компьютер под-

ключился к операционной системе Linux, что видно из первой строки экрана.

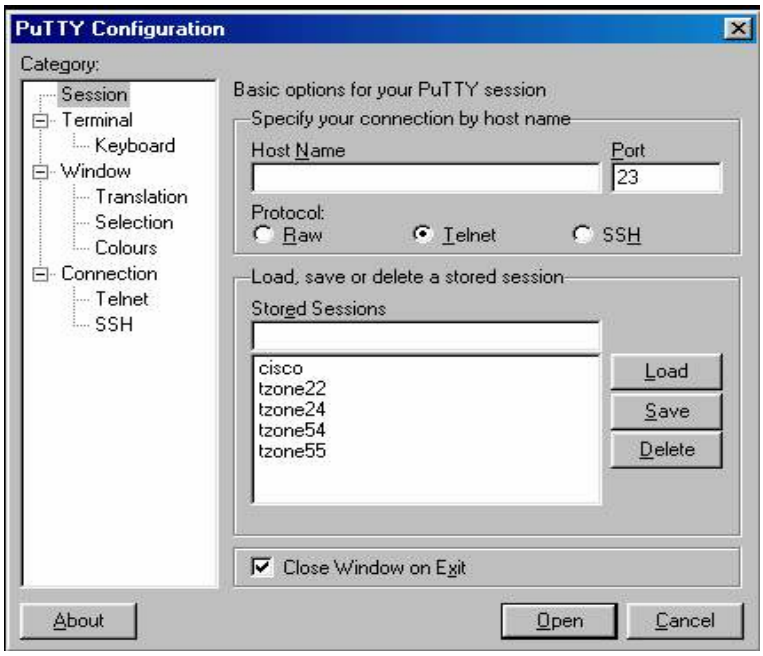


Рис. 5.5. Внешний вид программы PuTTY

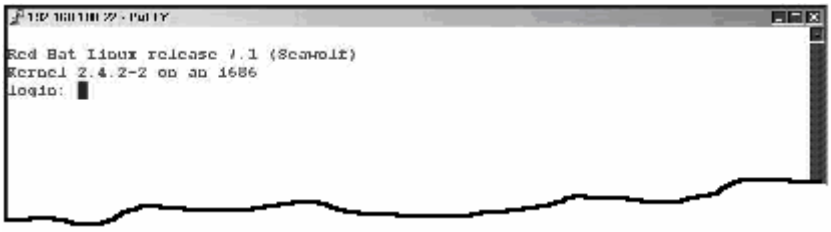


Рис. 5.6. Вход в систему

Данное окно является окном идентификации пользователей операционной системы Linux, на базе которой работает шлюз «Протей-ITG». Необходимо ввести имя пользователя и пароль. Если пароль правильный,

на экране появляется командная строка операционной системы Linux (рис. 5.7).

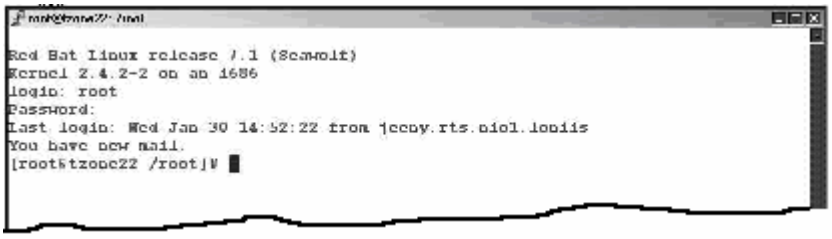


Рис. 5.7. Командная строка

Для более удобной работы необходимо запустить оболочку Midnight Commander, используя команду **мс**. На экране появится рабочая панель этой оболочки (рис. 5.8). Работа с ней подобна работе с Norton Commander для операционной системы DOS (ПО шлюза расположено в определенной директории, имя которой будет указано преподавателем).

Перемещение по меню осуществляется с помощью клавиш ⇐,⇑,⇒,⇓,PageUp, PageDown, Home, End. Для того чтобы зайти в директорию, нужно использовать клавишу Enter. Для просмотра файлов необходимо нажать клавишу F3, а для того чтобы изменить какие-либо значения – клавишу F4. После нажатия клавиши F4 можно с помощью клавиатуры вводить необходимые значения.

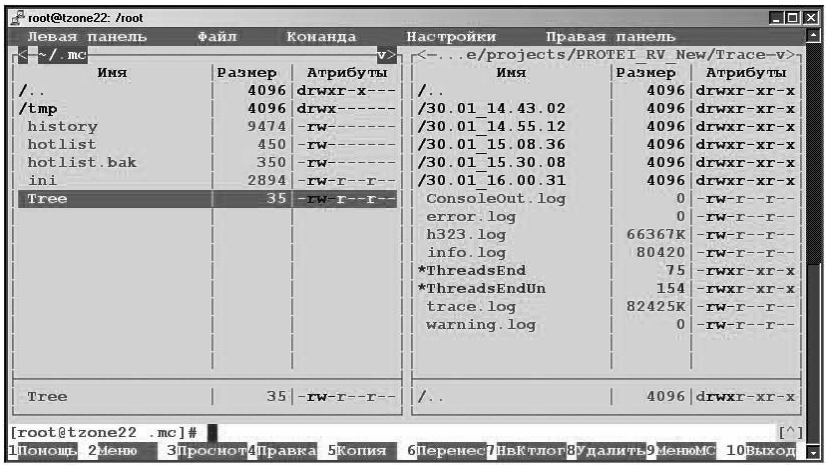


Рис. 5.8. Панель Midnight Commander

5.4.2. Задание на лабораторную работу

Отчет должен содержать краткое описание операционной системы Linux. А также ответы на контрольные вопросы.

Контрольные вопросы

1. На базе какой операционной системы работает шлюз?
2. Каким образом осуществляется подключение к шлюзу?
3. Что такое протокол telnet?
4. Что такое Midnight Commander? Как с ним работать?

При защите необходимо показать, каким образом можно просматривать и изменять содержание файлов.

5.5. Изучение системы техобслуживания шлюза

5.5.1. Теоретический материал

Конфигурация шлюза задается посредством набора конфигурационных файлов, состоящего из следующих двух групп.

В первую группу входят конфигурационные файлы, разработанные на основе одноименных файлов платформы Протей:

common.cfg

◊ DSS1.cfg

◊ physical.cfg

◊ protei.cfg

◊ SS7.cfg

Во вторую группу входят конфигурационные файлы, разработанные специально для шлюза:

- gateway.cfg (основные параметры шлюза),
- callroute.cfg (правила маршрутизации вызова),
- permissions.cfg (правила доступа к шлюзу из сети IP),
- H323.cfg (настройка процедур протоколов H.225 и H.245 и процедур, связанных с передачей аудиоинформации в соответствии с рекомендацией H323).

П р и м е ч а н и е . Во всех файлах после символа «#» следует текстовое описание значения данного поля, которое необходимо техническому персоналу.

Настройка основных параметров шлюза – файл gateway.cfg

Общая (General) – это обязательная секция, которая описывает основные параметры шлюза:

- Name – строковое имя шлюза (обязательный параметр), которое присутствует в качестве «alias» в сигнальных сообщениях H.323;

- IP-IP – адрес шлюза (обязательный параметр), куда приходят сигнальные сообщения;

- Port – номер порта TCP, используемый для установления телефонных вызовов из IP-сети на шлюз (значение по умолчанию 1720);

- Prefixes – набор префиксов телефонных номеров в сети ТфОП, на которые шлюз способен направить вызовы (для Санкт-Петербурга – 812), и которые необходимы для регистрации на привратнике (значение по умолчанию – пустой список);

- MaxCall – максимальное число вызовов, которые может обслужить шлюз.

Секция (Audio) – настройки, общие для всех кодеков. Это необязательная секция, которая содержит параметры:

* SilenceSupression – подавление пауз в разговоре. Значения (0/1) – соответствуют: используется/не используется (значение по умолчанию – 1);

* Codecs – (g729/ g723/ g711/ gsm) – это обозначения применяемых кодеков в порядке приоритетов использования (значение по умолчанию – g729, g711). Пока реализован только g729.

Секция привратник (Gatekeeper) – это необязательная секция, которая описывает параметры использования привратника:

✓ UseGatekeeper – (0/1) – использовать/не использовать привратник (значение по умолчанию – 0);

✓ AutomaticGatekeeperDiscovery – (0/1) – ручное или автоматическое задание привратника (значение по умолчанию – 1).

В случае ручного задания привратника:

o IP – IP-адрес привратника (значение по умолчанию – 0.0.0.0)

o Port – UDP порт, используемый для передачи сообщений RAS-сигнализации (значение по умолчанию 1719).

Правила маршрутизации вызова – файл callroute.cfg

Файл содержит таблицу маршрутизации вызовов из ТфОП в H.323 по префиксам телефонных номеров либо по полным телефонным номе-

рам. Первый столбец таблицы – префикс или номер, второй – адрес шлюза, на который следует направить данный вызов.

Не допускается запись, при которой одному префиксу соответствует два разных IP-адрес.

Формат номера – последовательность цифр (0, ..., 9). Формат префикса – последовательность цифр, заканчивающаяся символом *.

Правила доступа к шлюзу из IP-сети – файл permissions.cfg

Файл содержит список (черный или белый) IP-адресов, с которых разрешен выход на шлюз для установления соединения:

- AccessRule – секция в которой определены правила доступа для всех IP-адресов за исключением упомянутых в списке исключений. Параметр секции GeneralRule может принимать значение: GeneralRule = ALLOWED/DENIED – разрешить/запретить доступ по умолчанию;
- ExceptList – секция в которой определен список исключений для описанных в предыдущей секции правил доступа. Цифра, записанная через косую черту /, означает, сколько бит в IP-адресе, начиная слева, являются обязательными при анализе номера.

Настройка процедур протоколов H.225 и H.245 и процедур, связанных с передачей аудиоинформации в соответствии с рекомендацией H323 – файл H323.cfg.

Настройке подлежат следующие секции.

Секция H.225 содержит настраиваемые параметры:

- FastStart – принимает значения (0/1) – используется/не используется процедура Fast Connect (значение по умолчанию – 0);

- MediaWaitForConnect – принимает значения (0/1) – допускается/не допускается передача речи до приема сообщения Connect (значение по умолчанию – 0).

Секция H.245 содержит настраиваемые параметры:

- H245Tunneling – принимает значения (0/1) – используется/не используется туннелирование сообщений сигнализации H.245 в канале сигнализации H.225 (значение по умолчанию – 1);

- EarlyH245 – принимает значения (0/1) – допускается/допускается инициирование процедур H.245 до установления соединения, т. е. Connect (значение по умолчанию – 0).

Секция параметров обработки речи (Audio) содержит настраиваемые параметры джиттер-буфера и аудиокодеков.

Для настройки джиттер-буфера используются следующие параметры:

* AdaptiveJitter – принимает значения (0/1) – используются/не используются алгоритмы адаптивного изменения джиттер-буфера (значение по умолчанию – 0);

* InitialJitter – начальный размер джиттер-буфера в мс (значение по умолчанию – 60).

Для настройки аудиокодеков используются следующие параметры.

Кодек G.711:

- PacketizationIntrerval – длительность одного генерируемого речевого пакета в мс (значение по умолчанию – 30).

Кодек G.723.1:

- PacketizationIntrerval – длительность одного генерируемого речевого пакета в мс, которая должна быть кратна 30 мс (длительность фрейма G.723.1 – 30 мс), значение по умолчанию – 30;

- Rate – скорость работы кодека: 0 – 5.3 кбит/с, 1 – 6.3 кбит/с (значение по умолчанию – 0).

Кодек G.729:

- PacketizationIntrerval – длительность генерируемого речевого пакета, кратная 10 мс (длительность фрейма G.729 – 10 мс), значение по умолчанию – 30.

Примеры файлов конфигурации

Gateway.cfg

```
# general gateway parameters
[General]
Name=Niits
IP=192.168.100.4
Port=1720
Prefixes=7812
MaxCalls=5

# gatekeeper parameters
[Gatekeeper]
UseGatekeeper=1
```

```
# Gatekeeper discovery method
# 0 – manual discovery
# 1 – automatic discovery
AutomaticGatekeeperDiscovery=0
#manually set gatekeeper address
IP=192.168.100.21
Port=1719

#Audio parameters
[Audio]
SilenceSuppression=1
Codecs=g729,g723
```

Callroute.cfg

```
[CallRouting]
# prefix gateway
7095* 195.239.254.13 # Moscow /Teleross
```

Permissions.cfg

```
[AccessRule]
GeneralRule = DENY
```

[ExceptList]

```
194.85.131.3/32 # from Moscow
195.205.33.11/32 # from Arkhangelsk
195.205.35.24/32 # from Severodvinsk
192.168.100.0/24 # from our subnet
```

H323.cfg

```
#Protocol options
[H.225]
FastStart=1
MediaWaitForConnect=1

[H.245]
H245Tunneling=1
EarlyH245=0
```

```
#Speech processing parameters
[Audio]
AdaptiveJitter=0
InitialJitter=60 #60 ms

[G.711]
PacketizationIntrerval=30 #30 ms

[G.729]
PacketizationIntrerval=30 #3 frames, 10 ms per frame

[G.723.1]
PacketizationIntrerval=30 #1 frame, 30 ms per frame
# Speech rate:
# 0 – low-rate speech (5.3 kb/s)
# 1 – high-rate speech (6.3 kb/s)
Rate=1
```

5.5.2. Задание на лабораторную работу

Отчет должен содержать название и назначение конфигурационных файлов. Необходимо описать, какие изменения и в каких файлах необходимо сделать в следующих режимах работы шлюза:

1) все вызовы направляются на удаленное устройство с IP-адресом: 192.168.100.104;

2) шлюз принимает вызовы только со следующих IP-адресов:192.168.100.104 и 192.168.100.22;

3) по номерам, начинающимся с цифр 10 и 11, вызовы отправляются на IP-адрес 192.168.100.104, а по цифрам 20 и 21 – на IP-адрес 192.168.100.22;

4) шлюз может обрабатывать только кодек G.711;

5) не используется процедура FastStart [1];

6) шлюз использует привратник с IP-адресом 192.168.100.25.

При защите необходимо ответить на контрольные вопросы.

Контрольные вопросы

1. Каким способом осуществляется подключение к шлюзу Протей-ITG?

2. В каком виде хранится конфигурация шлюза?

3. Перечислите название и назначение конфигурационных файлов.

4. Каким образом можно задать определенную маршрутизацию вызовов?

5. Каким образом можно ограничить доступ к шлюзу?

6. Где задается IP-адрес шлюза?

7. Префикс и его использование в шлюзе.