ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ

Федеральное государственное
образовательное бюджетное учреждение
высшего профессионального образования
«САНКТ-ПЕТЕРБУРГСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ
им. проф. М. А. БОНЧ-БРУЕВИЧА»

Б. С. Гольдштейн, В. Ю. Гойхман
Ю. В. Столповская

ПРОТОКОЛЫ IP-ТЕЛЕФОНИИ: RTP, RTCP

УЧЕБНОЕ ПОСОБИЕ

СПб ГУТ)))

САНКТ-ПЕТЕРБУРГ
2014

УДК 621.395(075.8)
ББК 32.882я73
Г63

Рецензенты:
кандидат технических наук, доцент, заведующий кафедрой «Сети связи и системы коммутации» СКФ МТУСИ
А. А. Манин,
доктор технических наук, главный научный сотрудник ЛО ЦНИИС
Н. А. Соколов

Утверждено
редакционно-издательским советом университета
в качестве учебного пособия

Гольдштейн, Б. С.
Г63 Протоколы IP-телефонии: RTP, RTCP : учебное пособие / Б. С. Гольдштейн, В. Ю. Гойхман, Ю. В. Столповская ; СПбГУТ. – СПб., 2014. – 59 с.

Содержит учебный материал о протоколах IP-телефонии RTP, RTCP. Процесс обучения строится на основе исследовательского полигона технологий и протоколов СОТСБИ-У. Материал учебного пособия представлен в виде теоретической и практической частей, содержит рекомендации для проведения практических и лабораторных занятий, а также необходимую литературу.

Предназначены для студентов, обучающихся по направлению 210700 «Инфокоммуникационные технологии и системы связи». 231000 «Программная инженерия»

УДК 621.395(075.8)
ББК 32.882я73

© Гольдштейн Б. С., Гойхман В. Ю., Столповская Ю. В., 2014

© Федеральное государственное образовательное бюджетное учреждение высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», 2014

СОДЕРЖАНИЕ

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ 4
1. ПРОТОКОЛЫ IP-ТЕЛЕФОНИИ: RTP, RTCP 6
1.1. Принципы пакетной передачи 6
1.2. Процесс передачи речи по IP-сети 7
1.3. Качество IP-телефонии 9
1.4. Принципы кодирования речи 11
1.5. Кодирование видео 16
1.6. Оценка качества передачи речи и видео в IP-сетях 17
1.7. Обеспечение качества обслуживания в IP-сетях 22
1.8. Протокол RTP 23
1.9. Протокол RTCP 31
2. ИССЛЕДОВАТЕЛЬСКИЙ ПОЛИГОН ТЕХНОЛОГИЙ И ПРОТОКОЛОВ «СОТСБИ-У» 45
2.1. Назначение 45
2.2. Компоненты полигона СОТСБИ-У 45
3. ПРАКТИЧЕСКИЕ ЗАНЯТИЯ 47
3.1. Базовый вызов в режиме «точка-точка» (без участия SIP-сервера) 48
3.2. Базовый вызов через SIP-сервер Asterisk 49
3.3. Видеовызов в режиме «точка-точка» (без участия SIP-сервера) 49
3.4. Видеовызов через SIP-сервер Asterisk 51
3.5. Типы аудиокодеков IP-телефонии 52
3.6. Типы видеокодеков IP-телефонии 55
3.7. Типы терминалов 57
СПИСОК ЛИТЕРАТУРЫ 58

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

ACELP – Algebraic Code-Excited Linear Prediction. Популярный алгоритм компрессии речевого сигнала (скорость передачи 8 кбит/с)

ADPCM – Adaptive Differential PCM. Адаптивная дифференциальная ИКМ

CS-ACELP– Conjugate Structure – Algebraic Code – Excited Linear Prediction. Технология CS-ASELP применяется в кодеках G.729, используемых для передачи речи по сетям Frame Relay. Обеспечивает скорость передачи 8 кбит/с при длительности кадра 10 мс

DiffServ – Differentiated Services. Система дифференцированного обслуживания графика разных классов, разработанная комитетом IETF

ETSI – European Telecommunications Standards Institute. Европейский институт телекоммуникационных стандартов

H.323 – Рекомендация ITU-T, которая определяет системы мультимедийной связи в сетях с пакетной коммутацией, не обеспечивающие гарантированное качество обслуживания

IP – Internet Protocol. Протокол сетевого уровня сети Интернет

MOS – Mean Opinion Score. Характеристика качества передачи речи с применением кодека того или иного типа, получаемая как среднее значение результатов оценки качества большой группой экспертов по пятибалльной шкале

MPLS – Multi-Protocol Label Switching. Многопротокольная коммутация по меткам. Основана на том, что пакеты, поступающие в пограничный маршрутизатор сети MPLS извне, разделяются на «классы эквивалентности пересылки». Каждому классу назначается система меток – коротких заголовков, используемых для маршрутизации пакетов внутри сети MPLS вместо длинных заголовков сетевого уровня

QoS – Quality of Service. Качество обслуживания

RTCP – Real-Time Transport Control Protocol. Протокол контроля транспортировки информации в реальном времени (IETF)

RTP – Real-Time Transport Protocol. Протокол транспортировки информации в реальном времени (IETF RFC 1889)

SDP – Session Description Protocol. Протокол описания сеансов связи

TCP – Transmission Control Protocol. Протокол управления передачей

UDP – User Datagram Protocol. Протокол передачи дейтаграмм Пользователя

VAD – Voice Activity Detector. Детектор речевой активности. Используется в кодеках со сжатием речевой информации для определения момента окончания паузы в речи.

VoIP – Voice over Internet Protocol. Технология, позволяющая использовать IP-сеть для передачи речевой информации

АЦП – Аналого-цифровое преобразование

МСЭ – Международный союз электросвязи

СОТСБИ – Сертифицированное оборудование телекоммуникационных сетей – банк информации

ЦАП – Цифроаналоговое преобразование

1. ПРОТОКОЛЫ IP-ТЕЛЕФОНИИ: RTP, RTCP

1.1. Принципы пакетной передачи

Технология коммутации пакетов является относительно новой по сравнению с коммутацией каналов и была разработана в 60-е гг. для передачи данных между вычислительными машинами сети Управления перспективных научно-исследовательских разработок ARPANet (США). В отличии от сетей с коммутацией каналов, где канал, обычно с полосой пропускания 64 кбит/с, выделяется пользователю на все время установления соединения, при коммутации пакетов пропускная способность канала, выделенного для передачи данных, разделяется между пакетами от различных источников. Данные, которые необходимо передать, разбиваются на части, к каждой части присоединяется заголовок, содержащий полную информацию, необходимую для доставки данных по назначению. Такими частями (единицами информации) могут быть пакеты, кадры или ячейки (в зависимости от протокола). Пакеты доставляются от отправителя к получателю через сетевые узлы (маршрутизаторы, router), которые на основании таблиц маршрутизации определяют путь до следующего узла, хранят пакеты, пока этот путь не будет доступен, иногда при перегрузке сети – отбрасывают пакеты.

В сетях с коммутацией пакетов существует две технологии:

- передача пакетов без установления соединения – метод дейтаграмм (пакеты, принадлежащие одному сообщению, доставляются к узлу назначения по произвольным маршрутам);
- передача пакетов с установлением соединения (перед транспортировкой пакетов, принадлежащих одному сообщению, осуществляется процедура установления соединения. После этого все пакеты к узлу назначения доставляются по одному и тому же виртуальному каналу).

Примером сети с коммутацией пакетов является сеть на базе протокола IP. Все данные в IP-сети – голос, текст, видео – передаются в виде пакетов. Любой компьютер и терминал такой сети имеет свой уникальный IP-адрес, и передаваемые пакеты маршрутизируются к получателю в соответствии с этим адресом, указываемом в заголовке. Маршрутизация пакетов на основании сетевого адреса протокола IP является механизмом технологии без установления соединения.

Технология передачи речи по пакетной сети на базе протокола IP получила название IP-телефония или VoIP. Но в процессе развития сетей и появления новых услуг реальные возможности технологии VoIP стали значительно шире ее формального названия. По существу эта технология представляет собой средство для передачи мультимедийной информации (речь, изображение, данные в любых комбинациях) с использованием протокола IP.

В отличие от традиционных телефонных сетей, построенных на базе технологии коммутации каналов:

– стоимость передачи речи по IP-сети не зависит от расстояния;

– использование IP-сети для передачи речи ведет к сокращению капитальных затрат, средств для организации каналов доступа, расходов на текущее обслуживание и ремонт сети;

– используя технологию VoIP, возможно передавать любой тип трафика: видео, данные.

В качестве терминала сети IP-телефонии – может использоваться любое оконечное устройство, осуществляющее преобразование пользовательских данных в пакеты IP-сети и организацию двустороннего мультимедийного сеанса связи с помощью различных протоколов, например, H.323, SIP или H.248/MEGACO.

1.2. Процесс передачи речи по IP-сети

Процесс передачи речи по IP-сети состоит из нескольких этапов (рис. 1.1). В терминале, подключенном к IP-сети и оснащенном микрофоном, телефоном и программно-аппаратными средствами мультимедиа, происходит кодирование речи:

– АЦП (аналого-цифровое преобразование) сигналов, поступающих от микрофона;

– компрессия сигнала (для уменьшения требуемой полосы пропускания).

Эти преобразования осуществляются в кодеках. Кодеки могут обеспечивать скорость передачи речи от 1,2 до 64 кбит/с.

Для формирования пакетов необходимо накопить определенный объем данных, к которым добавляется служебная информация – адрес получателя, порядковый номер пакета на случай, если будет нарушена последовательность доставки, и дополнительные данные для коррекции ошибок.

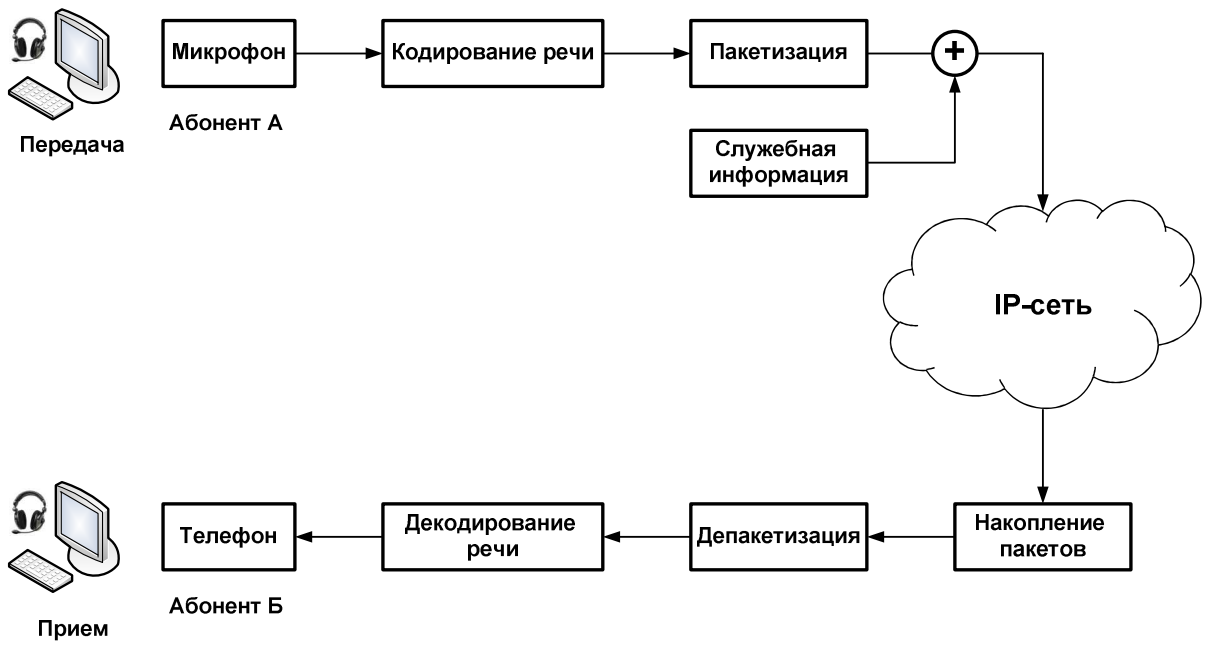


Рис. 1.1. Процесс передачи речи по IP-сети

Поскольку стек протоколов UDP/IP оказывает услугу передачи пакетов без установления соединения, пакеты со старшими порядковыми номерами могут прийти раньше, более того, интервал времени между пакетами также может колебаться. Поэтому на приеме для восстановления исходной последовательности и выравнивания интервалов между принятыми пакетами, происходит накопление пакетов.

Затем удаляются все заголовки пакетов и осуществляется декодирование речи: подавление эха, подавление периодов молчания, генерация комфортного шума, полученная последовательность данных декомпрессируется и подвергается ЦАП (цифроаналоговое преобразование).

В случае, если в процессе телефонного соединения участвуют две сети (сеть с коммутацией каналов и сеть с коммутацией пакетов), преобразование пакетов в сигнал TDM осуществляется в оборудовании медиа-шлюза (рис. 1.2). Причем функция «декодирования» в этом примере не осуществляет цифроаналогового преобразования.

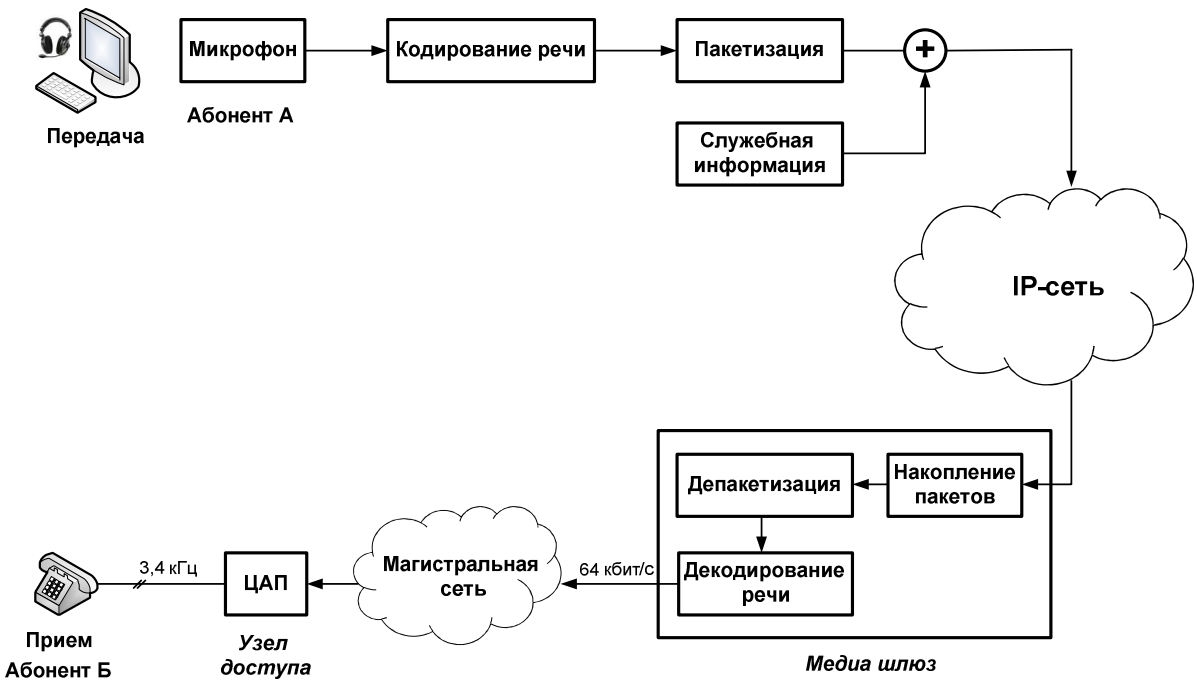


Рис. 1.2. Процесс передачи речи
между абонентом сети с КК и абонентом сети с КП

1.3. Качество IP-телефонии

IP-телефония является одной из областей передачи данных, где все процессы передачи информации должны происходить в режиме реального времени. Поэтому перед сетью VoIP стоит задача обеспечения качества доставки (Quality of Service, QoS) мультимедийной информации. Требования к качеству доставки пакетной информации зависят от типа приложений. Такие приложения включают аудио- и видеоконференции, распространение живого видео (для немедленного воспроизведения), удаленную диагностику в медицине, компьютерную телефонию, распределенное интерактивное моделирование, игры и мониторинг в реальном времени. Некоторые приложения устойчивы к потере пакетов, причем небольшую их часть можно даже восстановить на основе принятых данных. Для таких видов мультимедийного трафика как сжатые аудио и видеосигналы характерна очень большая чувствительность к потере пакетов и для них допустимый процент потери пакетов, как правило, не должен превышать 1 %.

Качество IP-телефонии обеспечивается эффективными методами кодирования сигнала и различными методами передачи информации (уменьшение транзитных маршрутизаторов, резервирование сетевых ресурсов, дифференцированное обслуживание разного типа трафика).

Качество обслуживания в IP-сетях определяется следующими параметрами:

• полоса пропускания – максимальный объем данных, которые могут быть переданы в данном направлении;

• задержка – промежуток времени, за который осуществляется передача пакета через сеть;

• джиттер – изменение задержки между двумя последовательными пакетами;

• потеря пакетов – пакеты, потерянные при передаче через сеть.

Задержки

Общая задержка – время передачи пакета от говорящего до слушающего, включает задержку, создаваемую сетью, и задержку, вносимую терминальным оборудованием пользователя. Задержка создает неудобство при ведении диалога, приводит к перекрытию разговоров и возникновению эха. Стандарт ITU-T G.114 рекомендует величину задержки при передаче голоса в одном направлении не более 150 мс. Так же стандарт рекомендует рассматривать задержку от 150 до 400 мс как приемлемую, если говорящий и слушающий понимают наличие задержки и готовы с ней смириться. Стандарт ITU-T G.114 также устанавливает, что при передаче голоса задержка более чем 450 мс является неприемлемой.

Причины возникновения задержки при передаче речи от источника к приемнику

Задержка сети доступа:

– задержка кодирования. Величина задержки кодирования определяется типом речевого кодека, который выполняет данную операцию, и изменяется от небольших величин (0,125 мс в G.711) до единиц миллисекунд;

– задержка пакетизации. Вносится при сборе кадров (закодированных речевых интервалов) в пакеты, причем число кадров в пакете определяется максимально допустимой задержкой;

– задержка постановки в очередь и передачи пакетов является переменной задержкой.

Сетевая задержка обусловлена наличием очередей в маршрутизаторах (при большой нагрузке сети), большим количеством транзитных коммутаторов и линий в сети (топология сети), используемыми технологиями переноса информации в сетях с коммутацией пакетов, которые определяют время обработки пакета в маршрутизаторе (X.25, Frame Relay, ATM, IP).

Джиттер

Джиттер – изменение задержки между двумя последовательными пакетами. Наличие джиттера воспринимается слушателем как треск и щелчки.

При распространении по IP-сети пакеты прибывают в пункт назначения через разные промежутки времени. Это может быть вызвано различными факторами, например:

– протокол IP, используемый для транспортировки пакетов через сеть, не имеет механизма установления соединения, по этой причине пакеты одного сеанса связи могут передаваться по разным маршрутам;

– время нахождения пакета в узле маршрутизации зависит от параметров загрузки сети.

Джиттер-буфер, находящийся в терминале пользователя или шлюзе, предназначен компенсировать влияние джиттера. Он накапливает определенное количество пакетов, восстанавливает их очередность и выравнивает промежутки времени между пакетами с пользовательской информацией.

1.4. Принципы кодирования речи

При переходе от аналоговых к цифровым сетям связи возникла необходимость преобразовать аналоговый электрический сигнал в цифровой формат на передающей стороне, т. е. закодировать, и затем после приема перевести обратно в аналоговую форму, т. е. декодировать.

Цель любой схемы кодирования – получить такую цифровую последовательность, которая требует минимальной скорости передачи и из которой декодер может восстановить исходный речевой сигнал с минимальными искажениями. Первой стандартной технологией была ИКМ (PCM) с пропускной способностью канала 64 кбит/с, которая обеспечивает передачу речи с очень хорошим качеством. Соответствующие процедуры кодирования и декодирования стандартизированы Международным союзом электросвязи ITU-T в рекомендации G.711. Однако такое высокое качество передачи речи достигнуто в системах ИКМ за счет явно избыточной скорости передачи информации. Чтобы уменьшить избыточность, последовательность чисел, полученная в результате преобразования речевого аналогового сигнала в цифровую форму, подвергается математическим преобразованиям, т. е. осуществляется компрессия – преобразование потока G.711 в поток с меньшей скоростью.

Все существующие кодеки характеризуются следующими параметрами:

– используемая полоса пропускания канала. Полосой пропускания цифрового канала называют максимальную скорость передачи информации по данному каналу в битах. Для эффективного использования пропускной способности IP-сетей необходимо уменьшить полосу пропускания одного разговорного канала. При уменьшении скорости передачи информации (полосы пропускания) уменьшается и качество воспроизводимого в аналоговой форме сигнала. Скорость передачи, которую обеспечивают имеющиеся сегодня узкополосные кодеки, лежит в пределах 1,2–64 кбит/с;

– подавление периодов молчания. Участник диалога говорит в среднем 35 % времени. Если применить алгоритмы, уменьшающие объем информа-

ции, передаваемой в периоды молчания, то можно значительно сузить необходимую полосу пропускания. В двустороннем разговоре такие меры позволяют достичь сокращения объема передаваемой информации до 50 %;

– размер кадра – это минимальная теоретически определенная методом кодирования задержка передачи информации. Кодеки с большей длиной кадра более эффективны, так как чем дольше наблюдается речевой сигнал, тем лучше он может быть смоделирован;

– чувствительность к потерям кадров. Существуют кодеки, минимизирующие чувствительность к потере пакетов;

– функция «Генератора комфортного шума» является составной частью функции «Подавление периодов молчания», т. е. когда абонент молчит, информация не передается и чтобы слушающий абонент не слышал «гробовую тишину» декодер генерирует комфортный шум с уровнем, отмеченным в период речевой активности.

Одним из важных факторов эффективного использования пропускной способности IP-канала, является выбор оптимального алгоритма кодирования/декодирования речевой информации – кодека.

Все существующие сегодня типы речевых кодеков по принципу действия можно разделить на три группы: кодеки с импульсно-кодовой модуляцией (ИКМ) и адаптивной дифференциальной импульсно-кодовой модуляцией (АДИКМ); кодеки с вокодерным преобразованием речевого сигнала; комбинированные (гибридные) кодеки. На рис. 1.3 представлена усредненная субъективная оценка качества кодирования речи для вышеперечисленных кодеков.

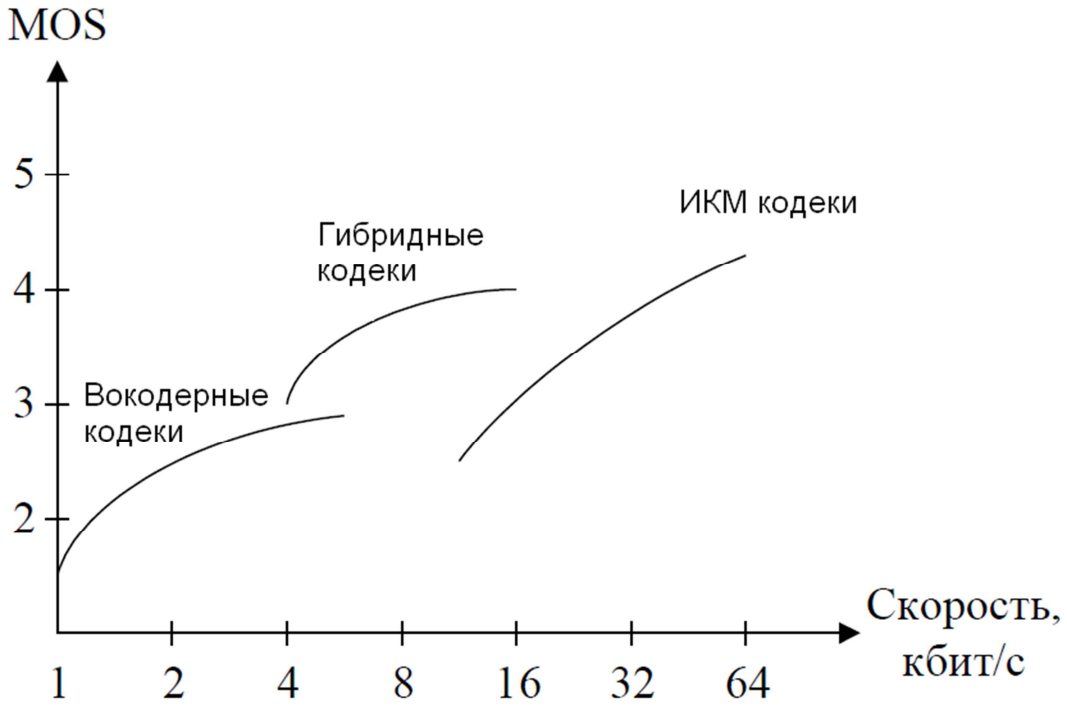


Рис. 1.3. Усредненная субъективная оценка качества кодирования речи для различных типов кодеков

Кодеки могут быть как лицензионными, так и открытыми, свободными от лицензионных отчислений. Лицензионными кодеками являются G.729, G.723, G.723.1. К открытым кодекам относятся: GSM, G.711 μ-law, G.711 A-Law, G.722, G.726, Speex, iLBC.

Наибольшее распространение получили кодеки следующих типов.

Кодек G.711

Рекомендация ITU-T G.711, утвержденная в 1972 г., описывает кодек, использующий ИКМ преобразование аналогового сигнала с тактовой частотой 8 кГц, с А или μ законом кодирования амплитуды дискретных отсчетов с использованием 8 бит. Скорость потока данных на выходе преобразователя составляет 64 кбит/с (8 бит × 8 кГц). Использование G.711 в системах IP-телефонии обосновано лишь в тех случаях, когда требуется обеспечить максимальное качество кодирования речевой информации при небольшом числе одновременных разговоров. Данный кодек используется в шлюзах сети IP-телефонии, обеспечивающих взаимодействие с сетью с коммутацией каналов.

Кодек G.726

Рекомендация ITU-T G.726, принятая в 1990 г., описывает кодек, использующий алгоритм сжатия речи ADPCM – адаптивная дифференциальная ИКМ. Этот алгоритм дает практически такое же качество воспроизведения речи, как и ИКМ, однако для передачи информации при его использовании требуется полоса всего в 16, 24, 32 или 40 кбит/с. Метод основан на том, что в аналоговом сигнале, передающем речь, невозможны резкие скачки интенсивности. Поэтому, если кодировать не саму амплитуду сигнала, а ее изменение по сравнению с предыдущим значением, то можно обойтись меньшим числом разрядов. Кодек предназначен для использования в системах видеоконференций.

Кодек G.728

Гибридный кодек, описанный в рекомендации ITU-T G.728 в 1992 г., использует технологию с малой задержкой LD-CELP – Low Delay – Code Excited Linear Prediction. Кодеки G.728 в качестве входного сигнала использует ИКМ сигнал со скоростью 64 кбит/с, обеспечивает скорость преобразования 16 кбит/с, вносит задержку при кодировании от 3 до 5 мс. Кодек предназначен для использования, в основном, в системах видеоконференций. В устройствах IP-телефонии данный кодек применяется достаточно редко.

Кодек G.729

Семейство включает кодеки, описанные в рекомендациях ITU-T G.729, G.729 Annex A, G.729 Annex B (содержит VAD и генератор комфортного шума). В кодеках G.729 применяется технология CS-ACELP-Conjugate Structure – Algebraic Code Excited Linear Prediction. Скорость кодированного речевого сигнала составляет 8 кбит/с. В устройствах VoIP

данный кодек занимает лидирующее положение, обеспечивая наилучшее качество кодирования речевой информации при достаточно высокой компрессии.

Кодек G.723.1

Рекомендация G.723.1, утвержденная ITU-T в ноябре 1995 г., описывает гибридные кодеки, использующие технологию кодирования речевой информации, сокращенно называемую – MP-MLQ (Multy-Pulse – Multy Level Quantization). Данные кодеки можно охарактеризовать, как комбинацию АЦП/ЦАП и вокодера. Кодек имеет две скорости и два варианта кодирования: 6,3 кбит/с с алгоритмом MP-MLQ и 5,3 кбит/с с алгоритмом CELP. Первый вариант предназначен для сетей с пакетной передачей голоса и обеспечивает лучшее качество кодирования по сравнению с вариантом CELP, но менее адаптирован к использованию в сетях со смешанным типом трафика (голос/данные).

Кодек Speex

Speex – это открытый программный кодек для сжатия речевого сигнала, который может использоваться в приложениях IP-телефонии. Проект Speex был начат 13.02.2002 г., версия Speex 1.0 была анонсирована 24.03.2003 г. Speex относится к классу кодеков, построенных на основе технологии Code Excited Linear Prediction (CELP), а также позволяет использовать переменную степень сжатия сигнала и поддерживает сигналы с различной шириной полосы: сверхширокополосный (ultra-wideband, частота дискретизации 32 кГц), широкополосный (wideband, 16 КГц) и узкополосный (narrowband, 8 кГц).

Кодек iLBC

iLBC (internet Low Bitrate Codec) – это открытый программный кодек для передачи речи по IP-сетям. iLBC описан в стандарте в RFC 3951. Кодек предназначен для узкополосных интернет-каналов, со скоростью передачи аудиосигнала (человеческой речи) 13.33 кбит/с при длине кадра в 30 мс или 15.20 кбит/с при 20 мс. Кодек iLBC позволяет добиться хорошего качества передачи аудиосигнала даже при некоторых искажениях, которые происходят в связи с потерей или задержкой пакетов.

1.5. Кодирование видео

Для передачи видео по IP-сети также возникает необходимость кодирования и последующего декодирования видеосигнала. Для этих целей используются кодеки с различными алгоритмами кодирования.

Алгоритмы кодирования видео применяются для цифрового представления, сжатия, хранения, передачи и обработки видеоинформации в самых различных системах. Большинство из этих алгоритмов связано с деятельностью двух организаций: MPEG (Motion Picture Experts Group), работающей под эгидой Международной организации по стандартизации ISO, и

VCEG (Video Coding Experts Group), работающей в составе Международного союза электросвязи ITU. Первая группа выпускает стандарты MPEGxx (–1, –2, –4, –7, –21), вторая – создает рекомендации ITU Hxx (.261, .263, .263+, .263++, .264).

Наиболее популярными на сегодняшний день являются следующие кодеки:

- стандарт H.261 – разработан Международным союзом электросвязи ITU. На практике, первый кадр в стандарте H.261 всегда представляет собой изображение стандарта JPEG, компрессированное с потерями и с высокой степенью сжатия;
- стандарт H.263 – это стандарт сжатия видео, предназначенный для передачи видео по каналам с довольно низкой пропускной способностью (обычно ниже 128 кбит/с). Применяется в программном обеспечении для видеоконференций;
- стандарт H.264 – это новый расширенный кодек, также известный как AVC и MPEG-4, часть 10;
- стандарт H.264 High Profile – это самый производительный профайл H.264 с алгоритмом сжатия видео Context Adaptive Binary Arithmetic Coding (CABAC), впервые внедрен на оборудовании Polycom, позволяет устраивать HD видеоконференции на канале от 512 Kbps;
- группа специалистов MPEG (Moving Picture Experts Group), сформированная Международной организацией по стандартизации ISO, стандартизировала следующие стандарты сжатия:
    - MPEG-1 – стандарт описывает принципы кодирования, компрессии и передачи аудио, видео и потоков данных в последовательности составных пакетов данных. Принципы кодирования видео в основном те же, что и в кодеках H.26X-серий. Кодек MPEG-1 поддерживает кодирование видео с разрешением 352 × 288 и частотой смены кадров 25 Гц, а также 352 × 240 с частотой смены кадров 30 Гц;
    - MPEG-2 – стандарт был разработан для кодирования видео с последующей передачей его по цифровым каналам наземного и спутникового телевидения, а так же по широкополосным сетям;
    - MPEG-3 – стандарт предназначался для использования в системах телевидения высокой четкости (high-defenition television, HDTV) со скоростью потока данных 20–40 Мбит/с, но позже стал частью стандарта MPEG-2 и отдельно теперь не упоминается;
    - MPEG-4 – международный стандарт, используемый преимущественно для сжатия цифрового аудио и видео. Предназначен для решения трех проблем: цифровое телевидение, интерактивные графические приложения и интерактивное мультимедиа (World Wide Web);

• Theora – это бесплатный и открытый видеокодек от команды Xiph.org Foundation. Разрабатывался как альтернатива платным и закрытым современным кодекам – H.264 (AVC), MPEG-4 и т. д. Theora поддерживает широкий набор разрешений (вплоть до HD).

1.6. Оценка качества передачи речи и видео в IP-сетях

Передача речевой и видеоинформации по IP-сетям в режиме реального времени или IP-телефония (VoIP), предъявляет к сетевой инфраструктуре гораздо более жесткие требования, чем любое другое приложение. Степень доступности сети, потеря пакетов и временные задержки могут оказывать существенное влияние на качество речевой и видеосвязи.

Первичным критерием качества аудио- и видеоинформации является восприятие качества услуги пользователем. Определение качества услуг может базироваться как на субъективных, так и на объективных оценках.

Субъективная оценка

Степень воздействия эха, задержек, потерь пакетов на передаваемый по сети речевой сигнал определяют качество речи. Одним из способов оценки качества речи является усредненная субъективная оценка MOS (Mean Opinion Score), алгоритм определения которой был разработана ITU-T. Алгоритм MOS, изложенный в спецификации ITU-T P.800, основан на 5-балльной шкале – от единицы (самое плохое качество связи) до пяти (самое хорошее качество). Оценка MOS формируется как среднее значение результатов оценки качества на основе большого числа испытаний, в каждом их которых участвует множество экспертов. В соответствии с этим алгоритмом группа людей оценивает качество звучания тестовых речевых шаблонов, передаваемых через сеть.

Для методики MOS оценка качества речи осуществляется в соответствии со следующей пятибалльной шкалой:

- 5 – отлично,
- 4 – хорошо,
- 3 – приемлемо,
- 2 – плохо,
- 1 – неприемлемо.

Оценка 3,5 баллов и выше соответствует высокому (стандартному) качеству речи, 3,0...3,5 – приемлемому, 2,5...3,0 – синтезированному звуку. Для передачи речи с хорошим качеством целесообразно ориентироваться на оценку MOS не ниже 3,5 баллов.

Хотя методика MOS, основанная на субъективных оценках, является достаточно надежным инструментом для оценки качества обслуживания при передаче речи, в ней отсутствует возможность количественно учесть

влияющие на качество речи факторы: сквозная задержка, джиттер, влияние потерь пакетов.

Качество восприятия видео (QoE) определяется на уровне передаваемых данных. Самый известный показатель – оценка Mean Opinion Score Video (MOS_V), которая, как и в случае обычного («телефонного») MOS, имеет субъективный характер. Комиссия экспертов оценивает качество видеокартинки по 5-балльной шкале: от 0 (неприемлемо) до 5 (отлично). Применяется и комбинированная оценка MOS-AV, характеризующая качество услуги аудио и видеосвязи с учетом синхронизации аудио и видеопотоков.

Объективная оценка

В настоящее время существует три основных метода объективной оценки качества предоставляемой аудио и видеоинформации на сетях операторов связи:

- активный (интрузивный, PESQ, POLQA);
- пассивный (неинтрузивный, P.563);
- моделируемый (E-model).

Активный метод

PESQ (Perceptual Evaluation of Speech Quality) – оценка восприятия качества передачи речи. Данный алгоритм представляет собой объективную методику определения качества речевой связи в телефонных системах, которая прогнозирует результаты субъективной оценки качества этого вида связи слушателями-экспертами. Для определения качества передачи речи в PESQ предусмотрено сравнение входного или эталонного (reference) сигнала с его искаженной (degraded) версией на выходе системы связи. Этот процесс схематично показан на рис. 1.4.

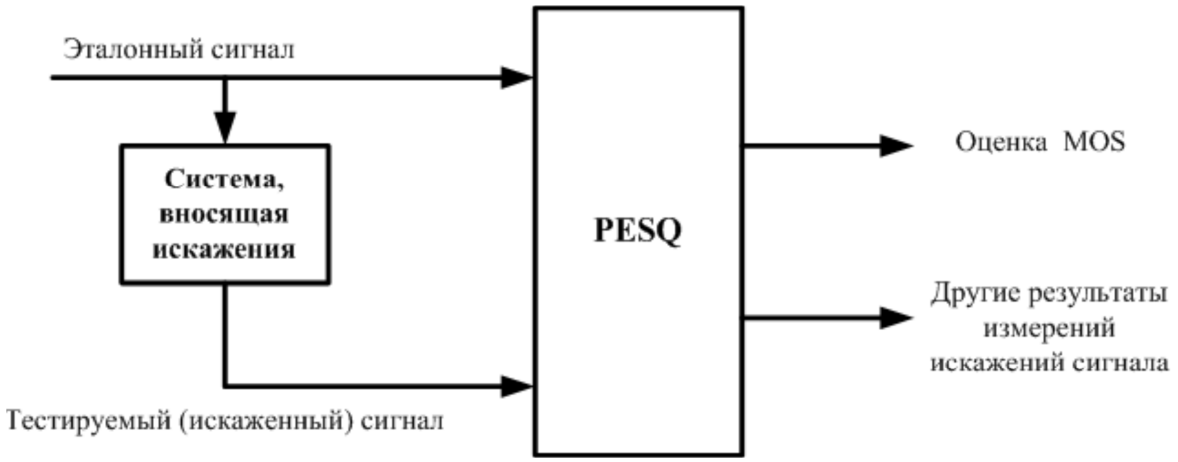


Рис. 1.4. Принцип работы PESQ

Результатом сравнения входного и выходного сигналов является оценка качества связи, которая аналогична усредненной субъективной оценке MOS, определяемой группой слушателей-экспертов согласно спецификации ITU-T P.800. В процессе разработки стандарта PESQ специалисты ITU-

Т отбирали лучшие методы определения качества речевой связи с точки зрения корреляции даваемых ими результатов с оценками MOS при различных условиях связи, что является гарантией хорошей работы стандартизированного алгоритма при тестировании обычных (фиксированных и мобильных) сетей и систем передачи пакетных данных. Коэффициент корреляции между оценками PESQ и оценками, выставленными реальными экспертами, как правило, принимает значение 0,95.

В декабре 2003 г. ITU-T одобрил алгоритм PESQ в качестве стандарта P.862. PESQ может использоваться как для определения качества сквозной (end-to-end) передачи речи, так и для оценки влияния на качество связи отдельных элементов сетевого оборудования, включая кодеки.

Альтернативой алгоритма PESQ является алгоритм POLQA (Perceptual Objective Listening Quality Analysis) – объективная оценка слышимого качества речи (спецификация ITU-T P.863).

POLQA является технологией оценки качества речи нового поколения для фиксированных, подвижных и IP-сетей. POLQA может использоваться в сетях 3G, 4G/LTE и для оценки качества голоса/видео высокой четкости (HD).

Пассивный метод

В отличие от алгоритма PESQ, который предполагает сопоставление эталонного сигнала высокого качества, и сигнала, искаженного в процессе передачи по сети, на базе теоретической модели восприятия речи, пассивный метод (спецификация ITU-T P.563, утвержденная в мае 2004 г.) оценивает качество искаженного речевого сигнала без сравнения с эталонным сигналом.

Коэффициент корреляции между оценками P.563 и оценками, выставляемыми реальными экспертами, варьируется от 0,85 до 0,9.

Конечно, алгоритм P.563 не так точен, как PESQ, но при этом он достаточно эффективен.

Моделируемый метод (E-model)

В 1998 г. Международный союз электросвязи ITU принял Рекомендацию G.107, в которой был описан подход к объективной оценке качества услуг в телекоммуникациях. В его основу положена так называемая Е-модель, которая открыла новое направление в оценке качества услуг, связанное с измерением характеристик терминалов и сетей. Результатом вычислений в соответствии с Е-моделью является число, называемое R-фактором.

Для объективной оценки качества передачи речи в соответствии с Е-моделью R-фактор определяется в диапазоне значений от 0 до 100, где 100 соответствует самому высокому уровню качества. При расчете R-фактора учитываются более 20 различных параметров, в числе которых: однонаправленная задержка, коэффициент потери пакетов, влияние эха и др. Сначала R-фактор вычисляется для идеальной сети, учитываются только искажения, вносимые при преобразовании речи в цифровой сигнал (и

обратно). Значение R-фактора с учетом этих искажений уменьшается от 100 до 93,2, что соответствует оценке MOS, равной 4,4. Таким образом, при использовании E-модели оценка 4,4 в системе MOS является максимально возможной оценкой качества речи в сети без искажений. Величина R-фактора меняется от 0 до 93,2, что соответствует изменению оценок MOS от 1 до 4,4.

Формула для вычисления R-фактора:

$$R = R_0 - I_s - I_d - I_e + A,$$

где $R_0 = 93,2$ – исходное значение R-фактора;

I_s – искажения, вносимые кодеками и шумами в канале;

I_d – искажения за счет суммарной сквозной задержки в сети;

I_e – искажения, вносимые оборудованием, включая и потери пакетов;

A – фактор преимущества, отражающий ожидания пользователей от качества телефонного разговора.

Значения R-фактора однозначно сопоставляются с оценками MOS (рис. 1.5). Данный метод имеет неплохую корреляцию с субъективными замерами MOS, но по точности уступающую алгоритму P.563.

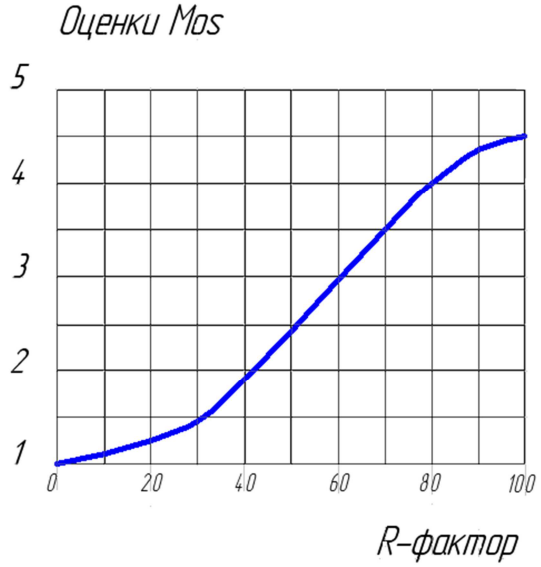


Рис. 1.5. Зависимость
между оценкой MOS и R-фактором

Применение методов

Применение указанных методов оценки качества речи на действующих сетях операторов связи должно выполняться в соответствии с поставленной целью:

- при проектировании сети связи – моделируемый метод (E-model);
- при тестировании сегмента связи перед вводом в эксплуатацию – активный метод (PESQ, POLQA);
- при мониторинге сети связи – все описанные выше методы.

1.7. Обеспечение качества обслуживания в IP-сетях

Основной проблемой IP-телефонии является обеспечение гарантированного качества обслуживания.

Существует несколько различных методов обеспечения гарантированного качества доставки информации от источника к приемнику:

- протокол резервирования ресурсов RSVP (Resource Reservation Protocol) применяется для резервирования ресурсов сети в зависимости от передаваемого типа трафика. Система, с помощью данного механизма, для передачи конкретного вида трафика, может запросить: необходимую пропускную способность, предсказуемую задержку, максимальный уровень потерь. Используется при одноадресной и многоадресной рассылках;
- технология MPLS (Multiprotocol Label Switching) – многопротокольная коммутация по меткам – является протоколом уровня 2,5. В целях обеспечения гарантированного качества обслуживания каждый пакет снабжается меткой, определяющей класс обслуживания данного пакета. Метка указывает определенный сетевой маршрут, который предлагает требуемый пакетом уровень качества услуг QoS. Маршрутизатор сети MPLS направляет пакеты, используя содержимое метки MPLS, не анализируя содержимое пакета IP. MPLS также позволяет сократить время на обработку маршрутной информации в узлах сети и, следовательно, уменьшить задержку сигнала;
- механизм дифференцированного обслуживания (DiffServ) используется на сетевом уровне. Заголовок IP пакета Type of Service используется для задания класса, определяющего уровень обслуживания в каждом из сетевых узлов. Пакеты каждого класса должны обрабатываться в соответствии с определенными для данного класса требованиями к качеству обслуживания;
- протокол транспортного уровня RTP (Real-time Transport Protocol) позволяет компенсировать влияние джиттера на качество речевой и видеоинформации. В протоколе предусматривается индикация типа передаваемой информации и номера пакета в потоке, а также применение временных меток. Отправитель помечает каждый RTP-пакет временной меткой, получатель на основании принятой метки вычисляет суммарную задержку. Разница в задержке принятых пакетов позволяет определить джиттер и уменьшить его влияние при передаче пакета получателю (все пакеты получателю передаются с одинаковой задержкой);
- в протоколе IPv6, по сравнению с IPv4, кроме расширения адресного пространства до 128 бит, был изменен формат заголовка, были введены дополнительные заголовки, которые, например, обеспечили использование маршрутизации, управляемой отправителем, что освободило сетевые

маршрутизаторы от просмотра адресных таблиц для выбора следующего маршрутизатора, тем самым снизив время задержки пакета в сети.

1.8. Протокол RTP

Протокол RTP был разработан IETF (RFC 1889) для переноса в реальном времени речевой и видеоинформации по сети с коммутацией пакетов. Совместно с протоколом UDP, RTP реализует функции транспортного уровня (рис. 1.6). Протокол UDP осуществляет сервис доставки пакетов без установления соединения и предоставляет протоколу RTP услуги мультиплексирования и обнаружения ошибок на основе контрольной суммы. При обнаружении ошибок поврежденные сегменты отбрасываются, а функции упорядочивания пакетов ложатся на RTP, который осуществляет нумерацию пакетов в потоке. Протокол RTP также предусматривает индикацию типа полезной нагрузки, а наличие временной метки пакета, позволяет компенсировать негативное влияние джиттера. В качестве протоколов транспортного уровня RTP может использовать и другие протоколы.

Рис. 1.6. Уровни протокола RTP/UDP/IP

Протокольные блоки данных RTP называются пакетами. Пакеты, формируемые в соответствии с протоколом RTP и служащие для передачи мультимедийных данных, называются информационными пакетами или пакетами данных. Пакет состоит из заголовка пакета и полезной нагрузки (сжатые речь, видео). Протокол RTP не имеет собственных механизмов, гарантирующих своевременную доставку пакетов или другие параметры качества услуг – это осуществляют нижележащие протоколы. Он даже не обеспечивает все те функции, которые обычно предоставляют транспортные протоколы, в частности, функции по исправлению ошибок или управлению потоком.

Так как мультмедийная сессия позволяет передавать различные типы данных (аудио, видео и т. д.), для передачи каждого типа трафика независимо от другого спецификацией протокола вводится понятие сеанса связи RTP. Сеанс определяется конкретной парой транспортных адресов назначения, т. е. один сетевой адрес и два порта для RTP и RTCP. Так, для ви-

деоконференции необходимо аудио и видео передавать в разных сеансах с соответственно разными портами назначения. Никакого непосредственного соединения на уровне RTP между аудио и видеосеансами связи не имеется, за исключением того, что пользователь, участвующий в обоих сеансах, должен использовать одно и то же каноническое имя в RTCP пакетах для обоих сеансов так, чтобы сеансы могли быть связаны.

Несмотря на разделение, синхронное воспроизведение мультимедийных данных источника (звука и видео) может быть достигнуто при использовании информации таймера (из поля, где указывается значение таймера), которая переносится в пакетах RTCP для обоих сеансов.

Формат пакета RTP

Пакет RTP включает в свой состав фиксированный заголовок, необязательное расширение заголовка с переменной длиной и поле данных. Структура пакета RTP показана на рис. 1.7.

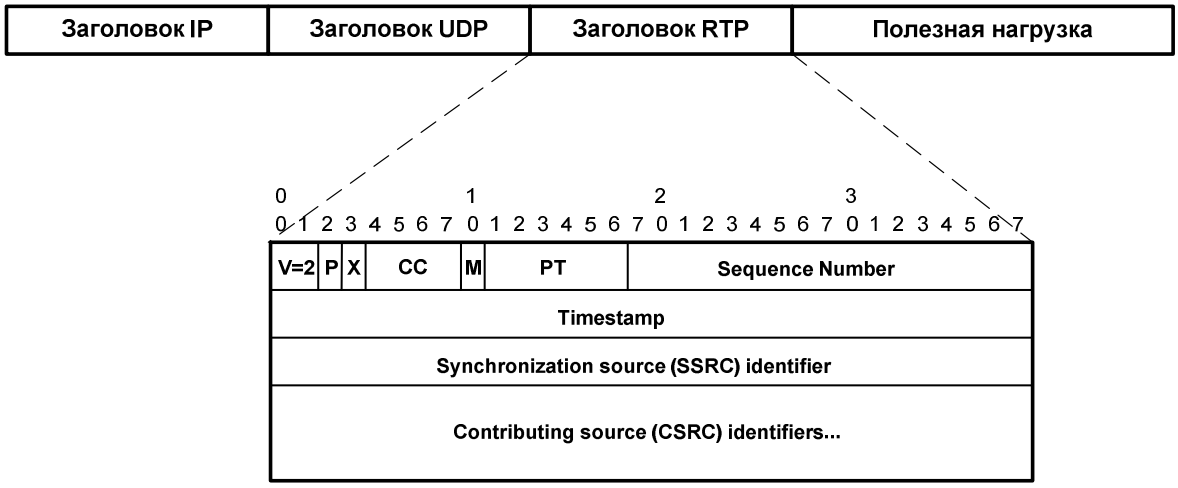


Рис. 1.7. Формат пакета RTP

Он состоит, как минимум, из 12 байтов. Поля заголовка имеют следующие значения.

Версия (V): 2 бита. Это поле идентифицирует версию протокола RTP. Текущая версия протокола – вторая (величина 1 использовалась в первой черновой версии RTP).

Дополнение (P): 1 бит. Если бит дополнения установлен в единицу, то пакет в конце содержит один или более октетов дополнения, которые не являются частью трафика. Последний октет дополнения содержит указание на число таких октетов, которые должны впоследствии игнорироваться. Дополнение может требоваться некоторым алгоритмам шифрования с фиксированными размерами блока или для переноса нескольких пакетов RTP в одном блоке данных протокола нижележащего уровня.

Расширение (X): 1 бит. Если бит расширения установлен в единицу, то за фиксированным заголовком следует дополнительный заголовок, используемый в экспериментальных расширениях протокола RTP.

Счетчик CSRC (CC): 4 бита. Счетчик CSRC содержит число идентификаторов включаемых источников CSRC, которые следуют за фиксированным заголовком. CSRC (contributing source) – список отправителей, чьи данные передаются в данном RTP пакете.

Маркер (M): 1 бит. Обычно используется для указания границ потока данных. Смысл бита маркера зависит от типа полезной нагрузки. В случае передачи видеоинформации он определяет конец кадра. При передаче речевой информации маркер указывает начало периода активности после периода молчания.

Тип трафика (PT): 7 бит. Идентифицирует тип полезной нагрузки и формат данных, включая сжатие и шифрование, необходимые для приложения. По содержимому данного поля приложение определяет тип мультимедийной информации и способ декодирования. В стационарном состоянии отправитель использует только один тип полезной нагрузки в течение сеанса, но он может его изменить в ответ на изменение условий, если об этом сигнализирует протокол контроля транспортировки информации в реальном времени RTCP (Real-Time Transport Control Protocol).

Порядковый номер (Sequence Number): 16 бит. Значение порядкового номера увеличивается на единицу с каждым отправленным информационным пакетом RTP и может использоваться получателем для обнаружения потерь пакетов и восстановления их исходной последовательности. Начальная величина порядкового номера выбирается случайным образом.

Временная метка (Timestamp): 32 бита. Указывает момент времени, в который был создан первый октет данных полезной нагрузки. Используется для вычисления задержки при приеме разных пакетов, позволяет определить джиттер и смягчить его влияние, отправляя пакеты получателю с одинаковой задержкой. Единицы, в которых время указывается в этом поле, зависят от типа полезной нагрузки. Значение определяется по локальным часам отправителя.

Идентификатор SSRC (Synchronization Source Identifier): 32 бита. Определяет источник синхронизации (SSRC) – источник потока пакетов RTP. Источниками синхронизации могут служить источники первичного сигнала (микрофоны или видеокамеры), а также устройства смешивания информации при конференции (смеситель). SSRC идентификатор представляет собой случайное число, которое является уникальным для данной RTP-сессии и не зависит от сетевого адреса источника. Участник сессии не должен использовать один и тот же SSRC идентификатор для всех RTP-сессий мультимедийного сеанса. Если участник формирует несколько потоков в рамках одной RTP-сессии (например, от нескольких видеокамер), каждый поток должен быть снабжен уникальным SSRC идентификатором.

Первые двенадцать октетов присутствуют в каждом пакете RTP, в то время как поле идентификаторов включаемых источников CSRC (contributing source) присутствует только тогда, когда оно вставлено смесителем.

Идентификатор CSRC (Contributing Source Identifier): включает от 0 до 15 полей, 32 бита каждое. Список источников (contributing source) содержит перечень SSRC идентификаторов источников (максимум 15), которые участвовали в формировании данного пакета. Число идентификаторов задается полем CC. Примером может служить речевая конференция, в которой передаются RTP-пакеты с речью всех участников, каждый со своим идентификатором SSRC. Они-то и образуют список идентификаторов CSRC, а вся конференция имеет общий идентификатор SSRC. Пример использования идентификаторов CSRC приведен на рис. 1.8, где показан смеситель, который получает RTP пакеты от двух различных источников и комбинирует их. Поток на выходе смесителя включает SSRC-сигналы от самого смесителя и сигналы от двух источников – S-A и S-C. Поля CSRC смеситель использует для идентификации исходных компонентов. Благодаря смесителям устройства, обладающие различными возможностями, могут получать из потока то, что им требуется.

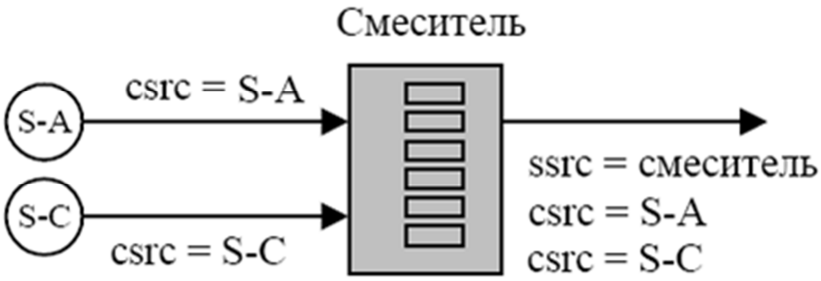


Рис. 1.8. Потоки после смесителя

Расширение заголовка RTP

Для обеспечения возможности экспериментировать с новыми функциями протокола RTP предусмотрен механизм расширения заголовка пакета. Этот механизм разработан так, чтобы расширение заголовка могло игнорироваться другими взаимодействующими приложениями, которым оно не требуется.

Если бит X в заголовке RTP установлен в единицу, то к фиксированному заголовку RTP присоединяется расширение заголовка с переменной длиной (рис. 1.9). Только одно расширение может быть добавлено к фиксированному заголовку информационного пакета RTP. Для того чтобы обеспечить работу различных приложений с различными расширениями заголовка или чтобы обеспечить работу с более чем одним типом расширений, первые 16 бит расширения заголовка остаются свободными для выбора идентификаторов или параметров. Формат этих 16 бит определяется спецификацией профиля, с которым работает приложение.

Рис. 1.9. Расширение заголовка RTP

За заголовком следует полезная нагрузка. Формат полезной нагрузки должен быть определен приложением и соотвествующим профилем, которые описаны в RFC 3550 и 3551.

Профиль RTP и спецификация формата полезной нагрузки

Как говорилось ранее, RTP является гибким протоколом, он открыт для внедрения новых форматов полезной нагрузки и новых мультимедийных приложений. Для этих целей в протоколе RTP предусмотрено понятие профиля.

Профиль (profile) – это набор параметров протоколов RTP и RTCP для конкретного класса приложений, определяющий особенности их функционирования. В профиле определяется использование отдельных полей заголовков пакетов, типы трафика, дополнения к заголовкам и расширения заголовков, типы пакетов, услуги и алгоритмы обеспечения безопасности связи, особенности использования протокола нижележащего уровня и т. д. Для каждого приложения в профиле описываются значения параметров, которые они могут принимать. Никакой явной индикации типа профиля номером порта, идентификатором протокола и т.п. не предусмотрено.

Таким образом, полная спецификация RTP для конкретного приложения должна включать дополнительные документы, к которым относятся описание профиля, а также описание формата трафика, определяющее, как трафик конкретного типа, такой как аудио или видео, будет обрабатываться в RTP (спецификация полезной нагрузки). При этом один и тот же формат трафика может использоваться для множества профилей и может быть определен независимо от профиля.

RTP профиль и спецификация полезной нагрузки для аудио и видео (RTP/AVP)

Приложение, использующее RTP, должно определить профиль и необходимый формат полезной нагрузки. Табл. 1.1 содержит краткое описание профиля, определенного для аудио и видео. В табл. 1.1 указаны пункты, которые могут быть определены или изменены в профиле, и их описание.

Таблица 1.1

Пункт профиля	**RTP/AVP – specific – Описание**
Заголовок информаци-	Используется стандартный формат фиксированного заголовка

онного пакета RTP	информационных пакетов RTP (один бит маркера)
Тип полезной нагрузки	Определен ниже в табл. 1.2
Дополнения заголовков информационных пакетов RTP	К заголовкам информационных пакетов RTP не присоединяются никакие дополнительные фиксированные поля
Расширения заголовков информационных пакетов RTP	Никакие расширения заголовка информационных пакетов RTP не определены, но приложения, использующие этот профиль, могут использовать такие расширения. Т. е., в приложениях не должно быть принято, что бит X заголовка RTP всегда имеет нулевое значение. Приложения должны быть готовы игнорировать расширение заголовка. Если расширение заголовка определится в будущем, то должно быть задано содержимое первых 16 битов таким образом, чтобы можно было идентифицировать множество различных расширений
Типы пакетов RTCP	Никаких дополнительных типов пакетов RTCP в этой спецификации профиля не определено
Интервал отчетности RTCP	При вычислении интервала отчетности RTCP должны использоваться константы, предложенные в RFC 1889

Окончание табл. 1.1

Пункт профиля	RTP/AVP – specific – Описание
Расширения пакетов SR/RR	Расширения для пакетов SR и RR протокола RTCP не определены
Использование SDES	Приложения могут использовать любой из описанных пунктов SDES. В то время как информация о каноническом имени (CNAME) посылается в каждом отчетном интервале, другие пункты должны передаваться только в каждом пятом интервале отчетности
Безопасность	Заданные по умолчанию службы безопасности RTP также определяются по умолчанию этим профилем
Нижележащий протокол	Профиль определяет использование RTP над протоколом UDP в двухстороннем и групповом режимах
Протокол нижних уровней	UDP, TCP
Транспортное соответствие	Используется стандартное соответствие RTP и RTCP адресам транспортного уровня
Инкапсуляция	Инкапсуляция пакетов RTP не определена

Табл. 1.2 содержит образец форматов полезной нагрузки, определенных для аудио и видео (полная спецификация определяется в RFC 3551).

В первом столбце таблицы указывается тип нагрузки – он может быть статическим или динамическим. Поскольку размер поля для описания типа полезной нагрузки в заголовке пакета RTP ограничен, то только очень распространенным алгоритмам кодирования может быть присвоен статический тип. Это, как правило, алгоритмы кодирования аудио и видео, утвержденные Международными органами по стандартизации, такие как, например, серия G.XXX международного союза электросвязи ITU для кодирования аудиоданных. В RTP A/V профиле статический тип нагрузки определяется с фиксированным идентификационным номером, тактовой частотой и числом каналов.

Динамическому типу полезной нагрузки выделяются номера в диапазоне от 96 до 127. В отличие от статического типа нагрузки, динамический тип полезной нагрузки назначается для аудио и видео алгоритмов кодирования только на продолжительность RTP сессии. Механизмы для определения динамической нагрузки указываются в протоколе описания сеанса связи SDP или других протоколах, как например рекомендация ITU-T H.323/H.245. Эти механизмы связывают зарегистрированное название алгоритма кодирования /формата полезной нагрузки, а также некоторые дополнительные необходимые параметры, такие как временная метка RTP, частота и количество каналов, с номером типа полезной нагрузки. Эта связь действует только в течение RTP сессии, для которой динамическое связывание типа полезной нагрузки производится. Эта связь распространяется только на RTP сессии, на которой она сделана.

Таблица 1.2

PT (тип нагрузки)	Алгоритм кодирования	Тип данных	Тактовая частота, кГц	Число каналов
0	PCMU	Аудио	8000	1
3	GSM	Аудио	8000	1
4	G723	Аудио	8000	1
Dynamic	L8	Аудио	переменная	переменное
26	JPEG	Видео	90000	–
31	H261	Видео	90000	–
34	H263	Видео	90000	–
Dynamic	H263-1998	Видео	90000	–
96–127	Dynamic	A/V	?	–

Новые типы трафика назначаются статически (постоянно), если выполнены следующие условия:

- кодирование в большой степени интересует сообщество сети Internet;
- оно предлагает выгоды, сравнимые с существующими кодированиями и/или требуется для взаимодействия с существующими, широко используемыми системами конференцсвязи или мультимедийными системами;
- описание достаточно для создания декодера.

1.9. Протокол RTCP

Протокол контроля транспортировки информации в реальном времени RTCP (Real-Time Transport Control Protocol) формирует отчеты, содержащие информацию о сеансах связи RTP. Протокол RTCP передает сведения (как от приемника, так и от отправителя) о числе переданных и потерянных пакетов, значении джиттера, задержке и т. д., поддерживая связь между отправителем и получателем путем обмена пакетами – отчет приемника и отчет источника. RTCP всегда используется вместе с RTP для контроля качества и для передачи информации об участниках существующей сессии.

Чаще всего для RTP сессии назначается четный порт, а для RTCP сообщений следующий нечетный порт. Использование RTCP отчетов не является обязательным для всех RTP сессий, но рекомендуется. RTCP использует тот же стек протоколов, что и RTP (UDP/IP).

Протокол RTCP выполняет четыре основные функции.

1. Главная функция – обеспечение обратной связи (пакеты отчет приемника, отчет источника) для оценки качества передачи данных, например числа потерянных пакетов. При получении информации об увеличении потерь пакетов отправитель может снизить скорость кодирования. Отчет отправителя всегда содержит информацию о том, когда был сгенерирован последний RTP-пакет (она включает как внутреннюю метку, так и «реальное» время). Эта информация позволяет получателю координировать и синхро-

низировать 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. Идентификация отправителя. Так как выбираемый случайным образом идентификатор SSRC в процессе сеанса может изменяться, например, при обнаружении конфликта, для идентификации источника синхронизации требуются сведения о его неизменяемом каноническом имени (поле CNAME в пакете SDES). Как и идентификатор SSRC, идентификатор CNAME также должен быть уникальным для всех участников в рамках одного сеанса связи RTP. Поле CNAME должно иметь следующий формат: «пользователь@хост» или «хост».

3. Масштабирование. Предусмотрен механизм ограничивающий частоту передачи управляющих пакетов RTCP. Для каждого сеанса предполагается, что трафик данных соответствует агрегированному пределу, называемому полосой пропускания сеанса связи, которая совместно используется всеми участниками. Вычисления полосы пропускания для трафика управления и данных выполняются с учетом нижележащих протоколов транспортного и сетевого уровней (например, UDP и IP). Трафик управления должен быть ограничен малой частью полосы пропускания сеанса, чтобы не пострадала основная функция транспортного протокола – передача данных. Предполагается, что часть полосы пропускания сеанса, выделяемая для RTCP, должна быть установлена равной 5 %. Все участники сеанса должны использовать одинаковую величину полосы пропускания RTCP, чтобы вычисленные значения интервала передачи пакетов управления были одинаковыми.

4. Управление сеансом. Четвертая, дополнительная функция RTCP должна обеспечивать передачу информации управления сеансом (например, идентификацию участника), которая будет отражена в интерфейсе пользователя. Наиболее вероятно, что это будет полезным в «свободно управляемых» сеансах, где участники присоединяются к сеансу связи и покидают его без согласования параметров и характеристик.

Типы пакетов RTCP

Для передачи различного рода информации управления определено несколько типов пакетов RTCP:

- SR-пакет – отчет отправителя, используется для передачи статистической информации о передаче и приеме пакетов участниками, которые являются активными отправителями;
- RR-пакет – отчет получателя, используется для передачи статистической информации о приеме пакетов от участников, которые не являются активными отправителями. Также RR используется совместно с SR для пере-

дачи статистической информации о передаче и приеме пакетов от участников, которые являются активными отправителями, в случае если число источников больше 31;

- SDES-пакет – описания источника, включая CNAME;
- BYE-пакет – завершения сессии RTCP, указывает на то, что один или более источников покинули сессию;
- APP-пакет, определяемый приложением.

Каждый пакет RTCP начинается с фиксированной части (подобной фиксированной части информационных пакетов RTP). За ней следуют структурные элементы, которые могут иметь переменную длину согласно типу пакета, но всегда выравниваются по 32-разрядной границе. Требование выравнивания и включение поля длины в фиксированную часть предназначены обеспечить «наращиваемость» пакетов RTCP.

Несколько пакетов RTCP могут соединяться без каких-либо разделителей, формируя составной пакет RTCP, который передается в одном блоке данных протокола нижележащего уровня, например, протокола UDP. Какого-либо указателя на количество отдельных пакетов RTCP в составном пакете не предусмотрено, так как протоколы нижележащего уровня для определения окончания составного пакета содержат сведения о его полной длине.

Каждый отдельный пакет RTCP в составном пакете может обрабатываться отдельно без каких-либо требований относительно порядка или комбинации пакетов. Однако для корректного выполнения функций протокола все пакеты RTCP должны передаваться в составном пакете, включающем, по крайней мере, два индивидуальных пакета: SR/RR и SDES. Первый пакет RTCP в составном пакете должен всегда быть пакетом отчета, чтобы облегчить проверку корректности заголовка. Это требуется, даже если никакие данные не были ни отправлены, ни получены и если единственный пакет RTCP в составном пакете – это пакет BYE (тогда посылается пустой пакет RR). Если число источников, для которых передается статистика приема, превышает 31 (максимальное число источников, отмечаемых в одном пакете SR или RR), то за начальным пакетом отчета должны следовать дополнительные пакеты RR. Пакет SDES, содержащий поле CNAME, должен включаться в каждый составной пакет RTCP. Если требуется конкретным приложением, то дополнительно и другие пункты описания источника могут быть включены в пакет SDES в соответствии с ограничениями полосы пропускания. Другие типы пакетов RTCP могут следовать в любом порядке, за исключением того, что пакет BYE должен быть последним пакетом, отправленным с данным идентификатором SSRC/CSRC.

Пакет отчета отправителя SR

Пакет отчета отправителя содержит три основных секции и может содержать дополнительную четвертую определяемую профилем секцию расширения (рис. 1.10).

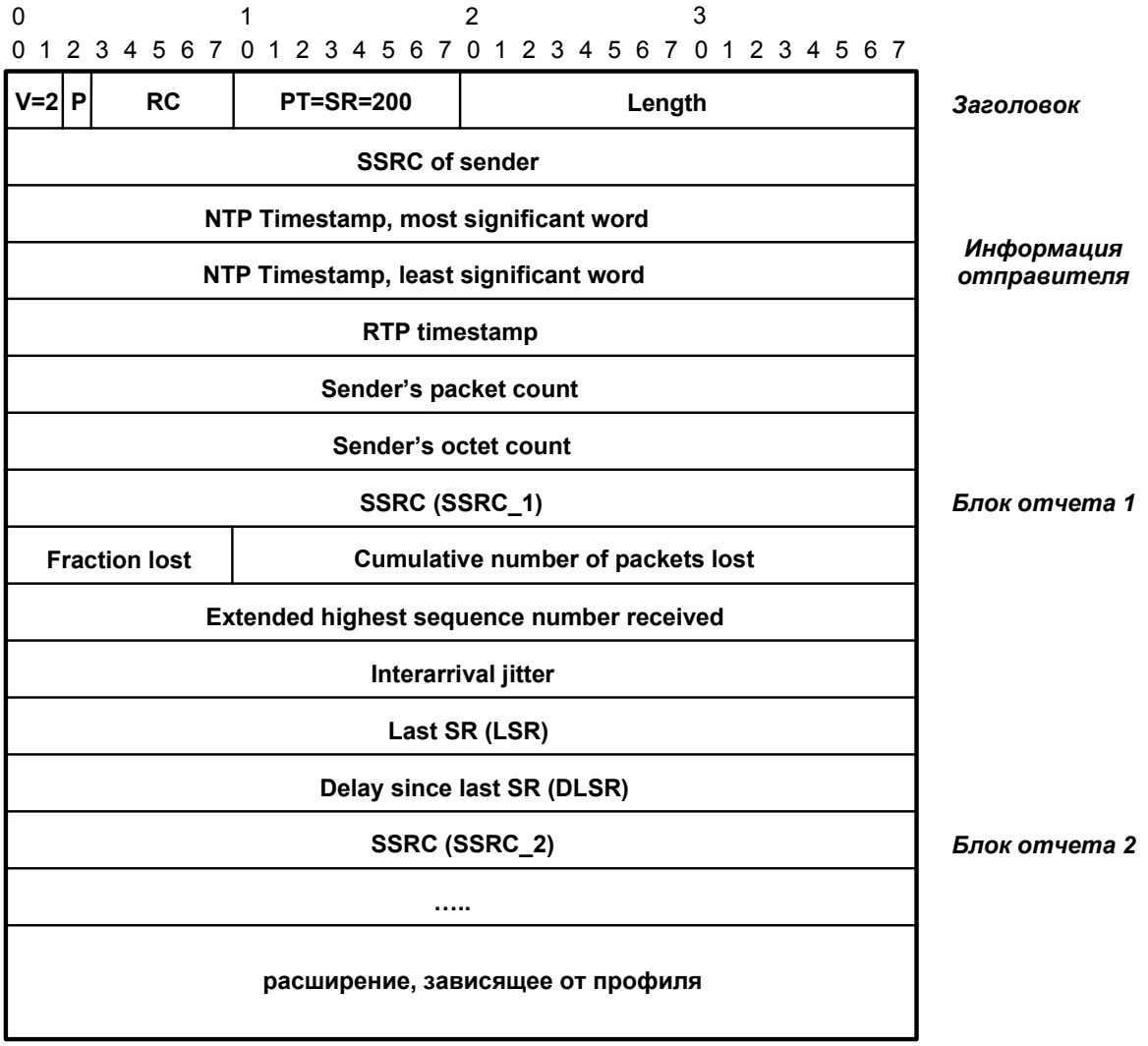


Рис. 1.10. Формат пакета SR

Заголовок имеет длину 8 октетов. Поля секции имеют следующие значения.

Версия (V – version): 2 бита. Идентифицирует версию RTP, которая является одинаковой в пакетах RTCP и информационных пакетах RTP. Текущая версия протокола – 2.

Дополнение (P – padding): 1 бит. Если бит дополнения установлен в 1, то этот пакет RTCP в конце содержит некоторые октеты дополнения, которые не являются частью информации управления. Последний октет дополнения – это счетчик дополнительных октетов, которые должны игнорироваться. Дополнение может требоваться некоторыми алгоритмами шифрования с фиксированными размерами блока. В составном пакете RTCP дополнение должно использоваться только в последнем индивидуальном пакете, потому что составной пакет шифруется в целом.

Число информационных блоков (RC – reception report count): 5 бит. Число блоков отчетов приема, содержащихся в данном пакете. Нуль – возможное значение RC.

Тип пакета (PT – packet type): 8 бит. Содержит константу 200 для идентификации пакета, как пакета SR протокола RTCP.

Длина (Length): 16 бит. Длина данного пакета RTCP в 32-разрядных словах минус одно слово, включая заголовок и любое дополнение (смещение на единицу делает нуль допустимой величиной и предотвращает возможность бесконечного зацикливания при просмотре составного пакета RTCP, с другой стороны, подсчет 32-разрядных слов исключает проверку допустимости значения длины на предмет кратности четырем).

SSRC: 32 бита. Идентификатор источника синхронизации для источника данного пакета SR.

Секция информации отправителя имеет длину 20 октетов и присутствует в каждом пакете отчета отправителя. Она подытоживает факты передачи данных от этого отправителя. Поля второй секции имеют следующие значения.

Временная метка NTP (NTP Timestamp): 64 бита. Указывает абсолютное время, когда был послан этот отчет так, что она может использоваться в комбинации с временными метками, возвратившимися в отчетах приема от других получателей, чтобы измерить время передачи на маршруте туда и обратно для этих получателей. Получатели должны ожидать, что точность измерения временной метки может быть принята гораздо меньшей, чем разрешение временной метки NTP.

Временная метка RTP (RTP timestamp): 32 бита. Соответствует тому же самому времени, что и временная метка NTP, но выражается в тех же единицах и с тем же самым случайным смещением, что и временные метки RTP в информационных пакетах. Это соответствие может использоваться для внешней и внутренней мультимедийной синхронизации источников, чьи временные метки NTP синхронизированы и могут использоваться независимыми от типа трафика получателями для оценки номинальной частоты таймера RTP.

Счетчик пакетов отправителя (Sender’s packet count): 32 бита. Общее количество информационных пакетов RTP, переданных отправителем от момента начала передачи вплоть до времени генерации пакета SR. Счетчик сбрасывается, если отправитель изменяет свой идентификатор SSRC.

Счетчик октетов отправителя (Sender’s octet count): 32 бита. Общее число октетов трафика (т. е. октетов пакета, не включая заголовок и дополнение), переданных в информационных пакетах RTP отправителем с момента начала передачи вплоть до времени генерации этого пакета SR. Счетчик обнуляется, если отправитель изменяет свой идентификатор SSRC. Это поле может использоваться для оценки средней скорости передачи трафика.

Секция блока отчета содержит нуль или более блоков отчета приема (начиная с последнего отчета) в зависимости от количества других источников, которых «видит» этот отправитель. Каждый блок отчета приема пе-

редает статистическую информацию о приеме пакетов RTP из одного источника синхронизации.

SSRC_n (идентификатор источника): 32 бита. Идентификатор SSRC источника, к которому относится информация в этом блоке отчета приема.

Доля потерь (Fraction lost): 8 бит. Часть информационных пакетов RTP из источника SSRC_n, потерянных, начиная с момента отправки предыдущего пакета SR или RR, представленная в виде целого числа с фиксированной точкой без знака (в виде целой части числа после умножения доли потерянных пакетов на 256). Эта доля определяется как число потерянных пакетов, разделенное на число ожидаемых пакетов. Если величина потерь – отрицательная из-за наличия дубликатов пакетов, то доля потерь приравнивается к нулю.

Общее число потерянных пакетов (Cumulative number of packets lost): 24 бита. Общее число информационных пакетов RTP из источника SSRC_n, которые были потеряны с момента начала приема. Это число является разностью между числом пакетов, ожидаемых к получению, и числом фактически полученных пакетов. В число полученных пакетов входят любые пакеты, в том числе опоздавшие и дубликаты. Таким образом, пакеты, которые прибывают поздно, не причисляются к числу потерянных, а число потерь может быть отрицательным, если имеются дубликаты. Число ожидаемых пакетов определяется как разность последнего полученного порядкового номера и начального полученного порядкового номера.

Расширенный наибольший полученный порядковый номер (Extended highest sequence number received): 32 бита. Младшие 16 битов содержат наибольший порядковый номер, полученный в пакете RTP из источника SSRC_n, а старшие 16 битов расширяют этот порядковый номер соответствующим количеством переполнения счетчиков пакета.

Джиттер прибытия (Interarrival jitter): 32 бита. Это статистическая оценка разницы относительного времени прибытия информационных пакетов RTP, измеряемая в единицах временной метки и выражаемая целым числом без знака.

Временная метка последнего SR (Last SR (LSR)): 32 бита. Средние 32 бита из 64 битов временной метки NTP, полученные как часть самых последних пакетов отчетов отправителя RTCP (SR) из источника SSRC_n. Если SR еще не был получен, то временная метка LSR имеет нулевое значение.

Задержка с момента последнего SR (Delay since last SR (DLSR): 32 бита. Задержка в приемнике пакетов, выраженная в единицах, равных 1/65536 с, между получением последнего пакета SR из источника SSRC_n и посылкой этого блока отчета о приеме. Если пакет SR еще не был получен от SSRC_n, то поле DLSR имеет нулевое значение.

Идентификатор SSRC источника второго блока отчета. Формат второго блока отчета аналогичен формату первого блока отчета.

Пакет отчета отправителя может содержать дополнительную определяемую профилем секцию расширения, которая следует за блоками отчетов.

Формат пакета отчета получателя RR

Формат пакета отчета получателя RR такой же, как и формат пакета SR, за исключением того, что поле типа пакета содержит константу, равную 201, а пять полей информации отправителя отсутствуют. Оставшиеся поля имеют то же самое значение, что и для пакета SR. Когда нет никакой передачи данных или приема, о которых можно было бы сообщить, во главу составного пакета RTCP помещается пустой пакет RR (RC = 0).

Формат пакета описания источника

Пакет SDES протокола RTCP состоит из заголовка и нуля или более частей, каждая из которых включает поля, описывающие источник, идентифицированный в этой части (рис. 1.11).

Заголовок пакета включает следующие поля.

Версия (V – version), дополнение (P – padding), длина (Length): данные поля соответствуют полям пакета SR.

Количество блоков SDES (SC – source count): 5 бит. Определяет число описываемых в этом пакете SDES источников SSRC/CSRC. Нулевая величина является допустимой, но неиспользуемой.

Тип пакета (PT – packet type): 8 бит. Содержит константу 202 для идентификации пакета, как пакета SDES протокола RTCP.

Каждая часть пакета SDES состоит из идентификатора SSRC/CSRC, за которым следует список из нуля или более полей с информацией о SSRC/CSRC. Каждая часть выровнена по 32-разрядной границе.

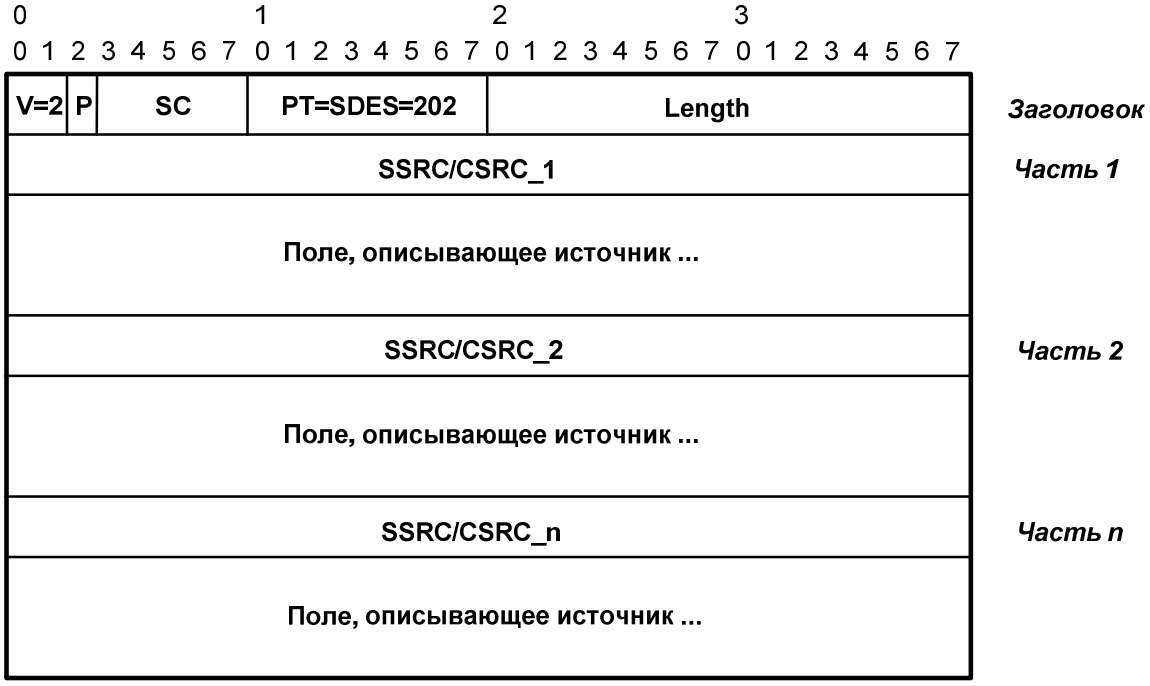


Рис. 1.11. Формат пакета описания источника SDES

Каждое поле, описывающее источник, состоит из 8-разрядного поля типа, 8-разрядного счетчика октетов, указывающего на длину текста (не включая этот двухоктетный заголовок), и непосредственно текста (рис. 1.12). Поле, описывающее источник, может содержать следующие данные:

• CNAME: каноническое имя оконечной точки. Так как выбираемый случайным образом идентификатор SSRC может в процессе работы изменяться при обнаружении конфликта или перезапуска программы, то для обеспечения идентификации источника сообщений требуются сведению о его неизменяемом каноническом имени (требуется пункт CNAME в пакете SDES). Как и идентификатор SSRC, идентификатор CNAME также должен быть уникальным для всех участников в рамках одного сеанса связи RTP. Чтобы обеспечить взаимодействие множества мультимедийных программных средств, используемых одним участником (для каждой программы – свой сеанс RTP), этот участник должен иметь единый идентификатор CNAME. Пункт CNAME должен иметь следующий формат: «пользователь@хост» или «хост». Примеры идентификатора CNAME для многопользовательской системы: «doe@sleepy.megacorp.com» или «doe@192.0.2.89». Примеры для системы без имени пользователя: «sleepy.megacorp.com» или «192.0.2.89». Пункт канонического имени оконечной точки (CNAME) является обязательным.

• NAME: Имя пользователя. Пункт имени пользователя (NAME) пакета SDES содержит реальное имя, используемое для описания источника, например, «John Doe, Bit Recycler, Megacorp». Оно может быть в любой определяемой пользователем форме. Для приложений типа конференцсвязи, эта форма имени может быть наиболее желательна при заполнении списков участников и, следовательно, могла бы передаваться гораздо чаще, чем CNAME. Профили могут устанавливать подобного рода приоритеты. Значение NAME остается постоянным, по крайней мере, в течение сеанса связи. Не следует полагать, что оно обязательно будет уникальным среди всех участников сеанса связи.

• EMAIL: Адрес электронной почты. Адрес электронной почты формируется согласно RFC 822, например, «John.Doe@megacorp.com». Величина EMAIL в течение сеанса связи остается постоянной.

• PHONE: Телефонный номер. Номер телефона должен формироваться со знаком «+» заменяющим код международного префикса. Например, +1 908 555 1212.

• LOC: Географическое местоположение пользователя. В зависимости от приложения, этому пункту соответствуют различные степени подробности. Для приложений конференцсвязи такая строка, как «Murray Hill, New

Jersey» может быть достаточна, в то время как для активной системы поиска могла бы подойти строка типа Room 2A244, AT.

• TOOL: Имя приложения. Пункт TOOL пакета SDES включает строку, содержащую имя и, возможно, версию приложения, генерирующего поток, например, «videotool 1.2». Эта информация может быть полезна для целей отладки и подобна заголовкам SMTP типа «Mailer» или «Mail-System-Version». В течение всего сеанса связи значение пункта TOOL остается постоянным.

• NOTE: Заметка/статус. Для этого пункта определена следующая семантика (профилем может быть задана другая). Пункт NOTE предназначен для кратковременных сообщений, описывающих текущее состояние источника, например, «говорить по телефону не может». В течение телеконференции этот пункт также может использоваться для передачи ее названия, темы. Пункт NOTE предназначен для передачи только исключительной информации и не должен постоянно использоваться всеми участниками, потому что это снизило бы интенсивность передачи отчетов приема и CNAME, и ухудшило бы характеристики протокола. В частности, пункт NOTE не должен включаться как пункт в файле конфигурации пользователя или автоматически периодически генерироваться.

• PRIV: Частные расширения. Пункт частных расширений (PRIV). Этот пункт используется для определяемых приложением расширений SDES. Пункт содержит префикс, состоящий из пары: поле длины и поле строки, за которым следует строка величин, заполняющая остаток пункта и содержащая интересующую информацию. Строка префикса – это имя, выбранное человеком, определившим пункт PRIV, являющееся уникальным относительно других пунктов PRIV, которые данное приложение могло бы получить. Разработчик приложения может в качестве строки префикса задать имя приложения плюс дополнительный идентификатор подтипа, если это необходимо. Заметим, что префикс использует некоторое пространство в пределах общей длины пункта 255 октетов, так что он должен быть по возможности более коротким. Это средство и получаемая полоса пропускания RTCP не должны быть перегружены; оно не предназначено для удовлетворения всех требований управления связи всех приложений.

NAME: Имя пользователя	NAME=2	Length	Имя источника ...	
EMAIL: Адрес электронной почты	EMAIL=3	Length	Адрес электронной почты ...	
PHONE: Телефонный номер	PHONE=4	Length	Телефонный номер источника ...	
LOC: Географическое местоположение пользователя	LOC=5	Length	Географическое местоположение ...	
TOOL: Имя приложения	TOOL=6	Length	Имя приложения ...	
NOTE: Заметка/ статус	NOTE=7	Length	Заметка об источнике ...	
PRIV: Частные расширения	PRIV=8	Length	Длина префикса	Строка префикса
	...	Строка величин ...		

Рис. 1.12. Формат поля, описывающего источник

Пакет завершения сеанса связи BYE

Пакет BYE указывает, что один или более источников становятся не активными. В составе пакета имеются следующие поля (рис. 1.13).

0				1				2				3			
0 1 2 3				4 5 6 7				0 1 2 3				4 5 6 7			
V=2	P	SC		PT=BYE=203				Length							
SSRC/CSRC_1															
...															
Длина				Причина завершения сеанса связи											

Рис. 1.13. Формат пакета завершения связи BYE

Версия (V – version), дополнение (P – padding), длина (Length): данные поля соответствуют полям пакета SR.

Счетчик источника (SC): 5 бит. Число идентификаторов SSRC/CSRC также включено в пакет BYE. Нулевая величина допустима, но не используется.

Тип пакета (PT): 8 бит. Содержит константу 203 для распознавания этого пакета, как пакета BYE протокола RTCP.

Идентификатор SSRC/CSRC определяет вышедший из сеанса источник. Если отключаются все источники конференции, в пакете BYE перечисляются идентификаторы всех источников, вносивших информацию в поток, а также идентификатор SSRC смесителя (конференции). Нулевая величина допустима, но не используется.

Если пакет BYE получен микшером, то микшер передает пакет BYE с неизменным идентификатором (идентификаторами) SSRC/CSRC.

Пакет BYE может также включать (необязательно) 8-разрядный счетчик октетов, за которым передается соответствующее количество октетов текста с указанием причины завершения связи, например, «неисправность видеокамеры» или «обнаружение зацикливания RTP». Строка имеет тот же тип кодирования, что описан для SDES. Если строка не заполняет пакет до 32-разрядной границы, то она дополняется нулевыми октетами.

Пакет, определяемый приложением (APP)ss

Пакет APP предназначен для экспериментального использования при разработке новых приложений и программных средств без регистрации новой величины типа пакета. Пакеты APP с нераспознанными именами должны игнорироваться. Пакет APP включает следующие поля (рис. 1.14).

0 1 2 3 4 5 6 7			0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7
V=2	**P**	**подтип**	**PT=APP=204**	**Length**
SSRC/CSRC_1				
Имя (ASCII)				
Информация, определяемая приложением				

Рис. 1.14. Формат пакета, определяемого приложением (APP)ss

Версия (V – version), дополнение (P – padding), длина (Length): данные поля соответствуют полям пакета SR.

Подтип: 5 бит. Может использоваться, как подтип для предоставления множеству пакетов APP возможности иметь одно уникальное имя или для любых данных, определяемых приложением.

Тип пакета (PT): 8 бит. Содержит константу 204 для распознавания данного пакета, как пакета APP протокола RTCP.

Идентификаторы SSRC/CSRC также включены в пакет APP.

Имя: 4 октета. Имя, выбранное разработчиком приложения, определяет множество пакетов APP и является уникальным по отношению ко всем другим пакетам APP, которые это приложение может получать. Имя интерпретируется как последовательность четырех символов ASCII (символы верхнего и нижнего регистра при этом трактуются различно).

Данные, определяемые приложением: переменная длина. Данные, зависимые от приложения, могут появляться или не появляться в пакете APP. Они интерпретируется приложением, а не непосредственно протоколом RTP. Длина этого поля должна быть кратна 32 битам.

2. ИССЛЕДОВАТЕЛЬСКИЙ ПОЛИГОН ТЕХНОЛОГИЙ И ПРОТОКОЛОВ «СОТСБИ-У»

2.1. Назначение

Исследовательский полигон технологий и протоколов «СОТСБИ-У» предназначен для проведения практических и исследовательских работ по изучению сетей NGN. Исследовательский полигон позволяет организовать полноценную работу с реальным оборудованием, начиная от настройки оборудования до имитации и анализа различных ситуаций взаимодействия элементов полигона между собой.

2.2. Компоненты полигона СОТСБИ-У

Сеть VoIP полигона СОТСБИ-У, используемая для проведения практических и исследовательских занятий (схему см. на вклейке).

Оборудование SIP» состоит из следующих основных элементов:

- сервер IP PBX Asterisk;
- сервер IP PBX Freeswitch;
- сервер GnuGK;
- сервер OpenIMSCore;
- рабочие места учащихся, оборудованные периферийными устройствами для приема и передачи мультимедийной информации (гарнитура и видеокамера).

Рабочее место

Рабочее место магистра для выполнения практических работ представляет собой совокупность аппаратных и программных средств. Аппаратные средства представлены персональным компьютером и набором периферийных устройств, в том числе для приема и передачи мультимедийной информации (гарнитура и видеокамера).

Программные средства представлены программным IMS терминалом Monster, средствами программного мониторинга сетевого трафика Wireshark, программными SIP телефонами SJPhone, Ekiga, Linphone и Twinkle.

На рабочем столе персонального компьютера (рис. 2.1) расположены следующие ярлыки:

- для запуска программы мониторинга сетевого трафика Wireshark локально (ярлык «Wireshark»);
- для запуска программы мониторинга сетевого трафика Wireshark на SIP-сервере (ярлык «Wireshark на сервере»);
- для запуска программного IMS терминала Monster;
- для запуска программного телефона SJPhone;
- для запуска программного телефона Ekiga;
- для запуска программного телефона Twinkle;

- для запуска программного телефона Linphone;
- среды эмуляции СОТСБИ-SIPp;
- для запуска трафик-генератора СОТСБИ-APA;
- для запуска web-интерфейса IP PBX Asterisk – СОТСБИ-X;
- для запуска web-интерфейса OpenIMSCore HSS;
- электронной библиотеки СОТСБИ-Lib, содержащей различную дополнительную литературу, необходимую при выполнении практической и исследовательской работы – библиотека.

Имена и IP-адреса рабочих мест указаны на табличках рядом с персональным компьютером.

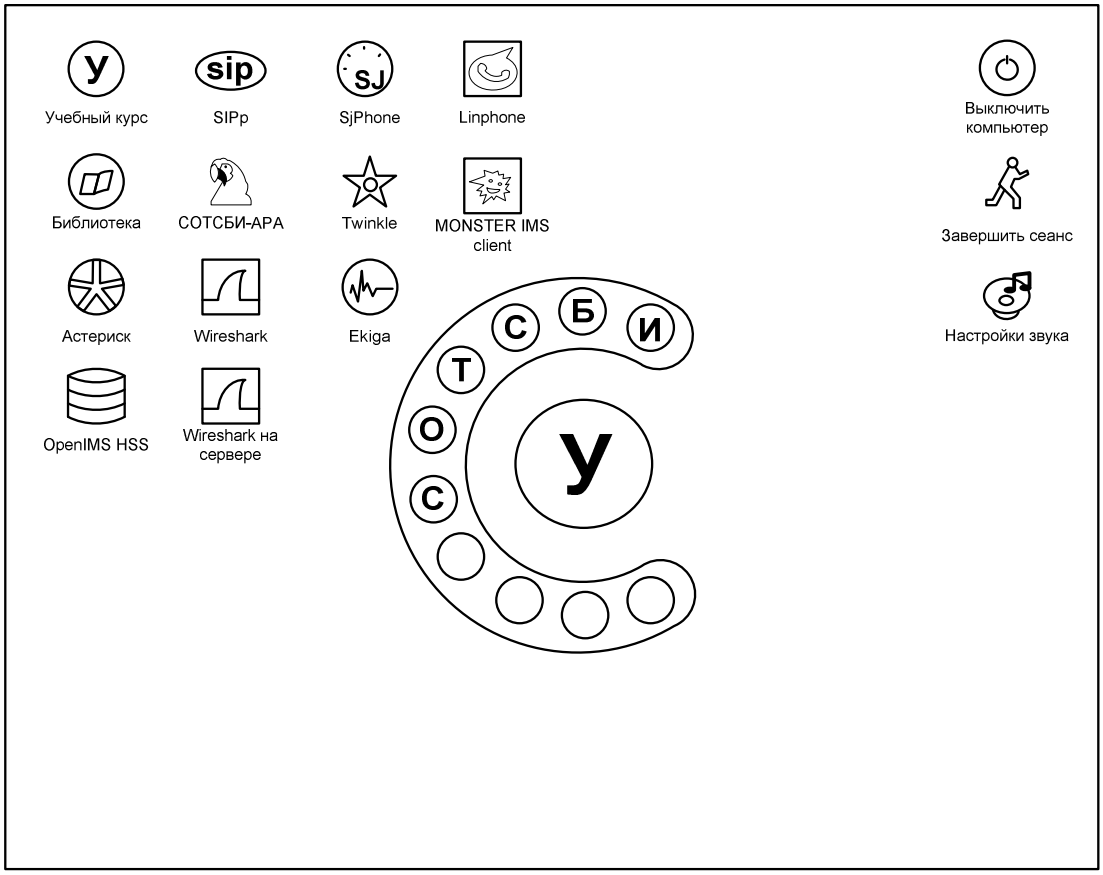


Рис. 2.1. Рабочий стол

3. ПРАКТИЧЕСКИЕ ЗАНЯТИЯ

В данной практической работе необходимо рассмотреть процесс передачи речи и видео в IP-сети при организации различных типов вызовов и определить, от каких параметров зависит качество передачи речи и видео.

Для выполнения практических занятий формируются бригады из расчета по 2 рабочих места на одну бригаду (далее – РМ 1, РМ 2).

Практические задания выполняются с использованием софтфонов Twinkle, Ekiga, SJPhone или LinPhone.

Перед выполнением заданий необходимо ознакомится с пользовательским интерфейсом программы мониторинга сетевого трафика Wireshark, программных телефонов, используемых на полигоне СОТСБИ-У.

Перед началом практической работы, а также после ее завершения, убедиться, что настройки всех программных продуктов (Wireshark, софтфоны) находятся в исходном состоянии.

Софтфоны, используемые на полигоне СОТСБИ-У, могут работать в двух режимах: с регистрацией на SIP-сервере и в режиме «точка-точка».

При работе телефона через SIP-сервер, сервер занимается обслуживанием входящих и исходящих вызовов с этого телефона. При этом все сообщения протокола SIP, сгенерированные в процессе обслуживания вызова, обрабатываются SIP-сервером. Данные о SIP-сервере должны быть указаны в настройках телефона. Информация об абоненте может быть представлена либо непосредственно в виде номера абонента, либо в виде имени пользователя, либо в виде URI пользователя (в формате: имя_пользователя@адрес_sip-сервера).

В режиме «точка-точка» связь с удаленным терминалом осуществляется напрямую. В этом случае все сообщения протокола транслируются непосредственно между телефонами. Для организации вызова в режиме «точка-точка» необходимо знать текущие IP-адреса терминалов. Формат данных вызываемого абонента в этом случае будет IP-адрес вызываемого абонента или имя@IP-адрес, где IP-адрес – адрес вызываемого абонента.

Перед началом выполнения практической работы необходимо настроить звуковые устройства (ярлык «Настройка звука» на рабочем столе (рис. 2.1)).

В случае если между двумя софтфонами установлено соединение, но звук отсутствует необходимо проверить в настройках софтфона:

− используемые кодеки (для некоторых софтфонов не все типы кодеков совместимы друг с другом);

− выбранное звуковое устройство.

Настоятельно рекомендуется запускать другое программное приложение (софтфон) только после полного закрытия предыдущего программного приложения (софтфона). В случае одновременного запуска двух софтфонов, последний может выдать сообщение о том, что порт 5060 для сигнализации SIP занят другим приложением, и в этом случае требуется корректно завершить работу всех запущенных софтфонов или перезагрузить РМ. При закрытии софтфона нажатием на системную кнопку «закрыть приложение» или при исчезновении его на панели задач, софтфон продолжает свою работу (занимая порт 5060), и доступен из трэя в правом нижнем углу экрана.

3.1. Базовый вызов в режиме «точка-точка» (без участия SIP-сервера)

Для осуществления вызова напрямую между SIP-терминалами необходимо знать текущий IP-адрес вызываемого терминала.

1. Настроить терминалы (Linphone, Twinkle или SJPhone) на РМ 1, 2 для работы в режиме без регистрации на SIP-сервере («точка-точка»).
2. Запустить Wireshark (локально).
3. Установить соединение от абонента РМ 1 к абоненту РМ 2.
4. Ответ абонента РМ 2, разговор, отбой абонента РМ 1.
5. По трейсам, полученным с помощью программы Wireshark, проанализировать пакеты протокола, предназначенного для передачи речи в IP-сетях:
   - определить протокол, предназначенный для передачи речи по IP-сети;
   - определить транспортный протокол для передачи пакетов протокола RTP;
   - определить количество RTP пакетов, переданных от вызываемого пользователя и от вызывающего;
   - определить тип кодека, используемый для кодирования речи.

3.2. Базовый вызов через SIP-сервер Asterisk

1. На терминалах (Linphone, Twinkle или SJPhone) на РМ 1, 2 осуществить регистрацию пользователей с именами (номерами) XXX, YYY соответственно (номера пользователей должны быть выбраны из списка зарегистрированных на SIP-сервере Asterisk).
2. На РМ 1 запустить Wireshark локально, на РМ 2 запустить Wireshark на сервере.
3. Установить соединение от абонента РМ 1 к абоненту РМ 2.
4. Ответ абонента РМ 2, разговор, отбой абонента РМ 1.
5. По трейсам, полученным с помощью программы Wireshark локально (запущена на РМ 1) отфильтровать пакеты по протоколу RTP, проанализировать пакеты протокола RTP:
   - определить путь передачи RTP-трафика (напрямую между терминалами или через SIP-сервер);
   - определить длительность разговора, используя данные о времени отправки пакетов (предполагается, что задержка прохождения пакетов по сети – нулевая);
   - с помощью меню Telephony – RTP – Stream Analysis программы Wireshark определить джиттер, потери пакетов RTP, число пакетов RTP, переданных вызывающей и вызываемой сторонами.

3.3. Видеовызов в режиме «точка-точка» (без участия SIP-сервера)

1. Настроить терминал (Linphone) на РМ 1, 2 для работы в режиме без регистрации на SIP-сервере («точка-точка»).

2. Запустить Wireshark (локально).

3. Установить видеовызов от абонента РМ 1 к абоненту РМ 2.

4. Ответ абонента РМ 2, разговор, отбой абонента РМ 1.

5. По трейсам, полученным с помощью программы Wireshark, проанализировать пакеты протокола RTP:

- определить, как передаются аудио и видеоданные: в одном RTP сеансе или в разных;
- определить сколько RTP сеансов установлено;
- определить тип кодека, используемый для кодирования речи;
- определить тип кодека, используемый для кодирования видео;

6. По трейсам, полученным с помощью программы Wireshark, проанализировать пакеты протокола RTCP:

- определить транспортный протокол для передачи пакетов протокола RTCP;
- определить для скольких RTP сеансов передаются пакеты RTCP;
- для каждого переданного RTCP пакета определить:

– тип пакета RTCP (для составного пакета RTCP указать все типы);

– для пакета отчета отправителя SR указать:

a) идентификатор источника синхронизации для источника пакета SR;

b) число блоков отчета приема;

c) идентификатор источника синхронизации, к которому относится информация в блоке отчета приема (указать IP-адрес пользователя, для которого передается статистическая информация в блоке отчета приема и для какой RTP-сессии (аудио или видео))[1];

d) статистическую информацию, содержащуюся в блоке отчета приема (доля потерь, общее число потерянных пакетов, расширенный наибольший полученный порядковый номер (сравнить с данными RTP-сессии), джиттер прибытия).

– для пакета описания источника SDES указать:

a) типы идентификаторов, описывающих источник и их формат.

---

[1] Чтобы определить тип RTP-сессии (аудио или видео) и IP-адрес пользователя, для чьего потока передается статистическая информация в блоке отчета приема пакета RTCP, следует значение идентификатора источника синхронизации в блоке Source1 пакета RTCP , сравнить со значениями идентификаторов источника синхронизации (поле SSRC) пакетов RTP для каждого типа RTP-сессии (аудио и видео) и каждого ее источника.

3.4. Видеовызов через SIP-сервер Asterisk

1. На терминале (Linphone) на РМ 1, 2 осуществить регистрацию пользователей с именами (номерами) XXX, YYY соответственно (номера пользователей должны быть выбраны из списка зарегистрированных на SIP-сервере Asterisk и поддерживающих возможность осуществления видеовызовов).

2. На РМ 1 запустить Wireshark локально, на РМ 2 запустить Wireshark на сервере.

3. Установить видеовызов от абонента РМ 1 к абоненту РМ 2.

4. Ответ абонента РМ 2, разговор, отбой абонента РМ 1.

5. По трейсам, полученным с помощью программы Wireshark локально (запущена на РМ 1) проанализировать пакеты протокола RTP:

- определить, как передаются аудио и видеоданные: в одном RTP сеансе или в разных;
- определить сколько RTP сеансов установлено;
- определить путь передачи RTP-трафика (напрямую между терминалами или через SIP-сервер);
- определить тип кодека, используемый для кодирования речи;
- определить тип кодека, используемый для кодирования видео;

6. По трейсам, полученным с помощью программы Wireshark, проанализировать пакеты протокола RTCP:

- определить для скольких RTP сеансов передаются пакеты RTCP;
- для каждого переданного RTCP пакета определить:
  - тип пакета RTCP (для составного пакета RTCP указать все типы);
  - для пакета отчета отправителя SR указать:
    - a) идентификатор источника синхронизации для источника пакета SR;
    - b) число блоков отчета приема;
    - c) идентификатор источника синхронизации, к которому относится информация в блоке отчета приема (указать IP-адрес пользователя, для которого передается статистическая информация в блоке отчета приема и для какой RTP-сессии (аудио или видео))[2];
    - d) статистическую информацию, содержащуюся в блоке отчета приема (доля потерь, общее число потерянных пакетов, расширенный наибольший полученный порядковый номер (сравнить с данными RTP-сессии), джиттер прибытия).
  - для пакета описания источника SDES указать:
    - a) типы идентификаторов, описывающих источник и их формат.

[2] Чтобы определить тип RTP-сессии (аудио или видео) и IP-адрес пользователя, для чьего потока передается статистическая информация в блоке отчета приема пакета RTCP, следует значение идентификатора источника синхронизации в блоке Source1 пакета RTCP , сравнить со значениями идентификаторов источника синхронизации (поле SSRC) пакетов RTP для каждого типа RTP-сессии (аудио и видео) и каждого ее источника.

3.5. Типы аудиокодеков IP-телефонии

Оценить зависимость качества передачи речи по IP-сети от типа используемого кодека и типа организации вызова.

Для аудиовызова в режиме «точка-точка»

1. Запустить Wireshark (локально).

2. Установить последовательно три соединения Linphone – Linphone, Twinkle – Twinkle и SJPhone – SJPhone в режиме «точка-точка», используя на вызываемой и вызывающей стороне одинаковый тип кодека, указанный в задании для каждого терминала, оценить (субъективно) качество передачи речи. Номер выполняемого задания для каждой бригады необходимо узнать у преподавателя (табл. 3.1).

Таблица 3.1

Номер задания	Используемый кодек для SJPhone	Используемый кодек для Twinkle	Используемый кодек для Linphone
1	GSM 6.10	Speex – wb (32 kHz)	PCMU 8000
2	iLBC codec – 30 ms	Speex – wb (16 kHz)	PCMA 8000
3	iLBC codec – 20 ms	Speex – nb (8 kHz)	Speex 32000 Hz
4	Speex codec – 15.2 k	G.726 16 кбит/с	Speex 16000 Hz
5	Speex codec – 15.2 k 40 ms	G.726 24 кбит/с	Speex 8000 Hz
6	Speex codec – 8.0 k 40 ms	G.726 32 кбит/с	GSM
7	G.711 – A-law	G.726 40 кбит/с	Speex 32000 Hz
8	G.711 – u-law	GSM	Speex 16000 Hz
9	GSM 6.10	G.711 – A-law	Speex 8000 Hz
10	iLBC codec – 30 ms	G.711 – u-law	Speex 32000 Hz

3. В полученном с помощью программы Wireshark трейсе отфильтровать пакеты по протоколу RTP и с помощью меню Statistics – Summary определить величину полосы пропускания для RTP-потока и сопоставить с величиной скорости передачи (кбит/с) используемого кодека. Для вычисления полосы пропускания необходимо брать значение из столбца Displayed и делить его на 2, так как в столбце Displayed указывается значение для двунаправленного RTP-потока (от источника к получателю и обратно).

4. Установить последовательно три соединения Linphone – Linphone, Twinkle – Twinkle и SJPhone – SJPhone в режиме «точка-точка», используя на вызываемой и вызывающей стороне разные типы кодеков, указанные в задании для каждого терминала. В случае установления соединения оценить (субъективно) качество передачи речи. В случае если соединения не установлено, указать причину. Определить зависимость возможности установления соединения от типа терминала и типа используемого кодека. Номер выполняемого задания для каждой бригады необходимо узнать у преподавателя (табл. 3.2).

Таблица 3.2

Номер задания	Используемый кодек для SJPhone	Используемый кодек для Twinkle	Используемый кодек для Linphone
1	G.711 – A-law G.711 – u-law	G.726 16 кбит/с G.711 – A-law	PCMU 8000 Speex 32000 Hz
2	Speex codec – 15.2 k Speex codec – 8.0 k 40 ms	G.726 24 кбит/с GSM	PCMA 8000 Speex 16000 Hz
3	Speex codec – 15.2 k Speex codec – 8.0 k 40 ms	G.726 32 кбит/с Speex – wb (32 kHz)	Speex 8000 Hz GSM
4	Speex codec – 15.2 k Speex codec – 8.0 k 40 ms	G.726 40 кбит/с Speex – nb (8 kHz)	GSM Speex 32000 Hz
5	Speex codec – 15.2 k Speex codec – 8.0 k 40 ms	GSM G.726 16 кбит/с	PCMU 8000 PCMA 8000
6	G.711 – A-law G.711 – u-law	GSM G.711 – u-law	Speex 16000 Hz Speex 8000 Hz
7	G.711 – A-law G.711 – u-law	Speex – wb (32 kHz) G.711 – u-law	GSM Speex 16000 Hz
8	Speex codec – 15.2 k Speex codec – 8.0 k 40 ms	G.726 16 кбит/с G.726 40 кбит/с	PCMU 8000 Speex 8000 Hz
9	G.711 – A-law G.711 – u-law	Speex – nb (8 kHz) G.726 16 кбит/с	PCMA 8000 GSM
10	G.711 – A-law G.711 – u-law	G.711 – A-law G.711 – u-law	Speex 32000 Hz Speex 8000 Hz

Для аудиовызова через SIP-сервер Asterisk

1. Запустить Wireshark (локально).

2. Установить последовательно три соединения между одинаковыми софтфонами (Linphone, Twinkle и SJPhone) в режиме с регистрацией на SIP-сервере, используя на вызываемой и вызывающей стороне одинаковый тип кодека, указанный в задании для каждого терминала, оценить (субъективно) качество передачи речи. Номер выполняемого задания для каждой бригады необходимо узнать у преподавателя (табл. 3.3).

Таблица 3.3

Номер задания	Используемый кодек для SJPhone	Используемый кодек для Twinkle	Используемый кодек для Linphone
1	GSM 6.10	Speex – wb (32 kHz)	PCMU 8000
2	iLBC codec – 30 ms	Speex – wb (16 kHz)	PCMA 8000
3	iLBC codec – 20 ms	Speex – nb (8 kHz)	Speex 32000 Hz
4	Speex codec – 15.2 k	G.726 16 кбит/с	Speex 16000 Hz
5	Speex codec – 15.2 k 40 ms	G.726 24 кбит/с	Speex 8000 Hz
6	Speex codec – 8.0 k 40 ms	G.726 32 кбит/с	GSM
7	G.711 – A-law	G.726 40 кбит/с	Speex 32000 Hz
8	G.711 – u-law	GSM	Speex 16000 Hz
9	GSM 6.10	G.711 – A-law	Speex 8000 Hz
10	iLBC codec – 30 ms	G.711 – u-law	Speex 32000 Hz

3. По трейсам, полученным с помощью программы Wireshark, проанализировать пакеты протокола RTP:

- определить путь передачи RTP-трафика (напрямую между терминалами или через SIP-сервер).

4. В полученном с помощью программы Wireshark трейсе отфильтровать пакеты по протоколу RTP и с помощью меню Statistics – Summary определить величину полосы пропускания и сопоставить с величиной скорости передачи (кбит/с) используемого кодека.

5. Установить последовательно три соединения между одинаковыми софтфонами (Linphone, Twinkle и SJPhone) в режиме с регистрацией на SIP-сервере, используя на вызываемой и вызывающей стороне различные типы кодеков, указанные в задании для каждого терминала. В случае установления соединения оценить (субъективно) качество передачи речи и по трейсам, полученным с помощью программы Wireshark, проанализировать пакеты RTP и определить тип используемого кодека. В случае если соединения не установлено, определить причину. Номер выполняемого задания для каждой бригады необходимо узнать у преподавателя (табл. 3.4).

Таблица 3.4

Номер задания	Используемый кодек для SJPhone	Используемый кодек для Twinkle	Используемый кодек для Linphone
1	GSM 6.10 iLBC codec – 30 ms	G.726 16 кбит/с G.711 – A-law	PCMU 8000 PCMA 8000
2	iLBC codec – 20 ms Speex codec – 8.0 k 40 ms	G.726 24 кбит/с GSM	Speex 8000 Hz Speex 16000 Hz
3	G.711 – A-law iLBC codec – 30 ms	G.726 32 кбит/с Speex – wb (32 kHz)	Speex 8000 Hz Speex 32000 Hz
4	G.711 – u-law iLBC codec – 20 ms	G.726 40 кбит/с Speex – nb (8 kHz)	Speex 16000 Hz Speex 32000 Hz
5	Speex codec – 15.2 k Speex codec – 8.0 k 40 ms	GSM G.726 16 кбит/с	PCMU 8000 PCMA 8000
6	iLBC codec – 20 ms Speex codec – 15.2 k	GSM G.711 – u-law	Speex 16000 Hz Speex 8000 Hz
7	iLBC codec – 30 ms iLBC codec – 20 ms	Speex – wb (32 kHz) G.711 – u-law	PCMU 8000 PCMA 8000
8	GSM 6.10 G.711 – A-law	G.726 16 кбит/с G.726 40 кбит/с	Speex 16000 Hz Speex 32000 Hz
9	iLBC codec – 30 ms Speex codec – 15.2 k 40 ms	Speex – nb (8 kHz) G.726 16 кбит/с	PCMU 8000 PCMA 8000
10	GSM 6.10 Speex codec – 15.2 k 40 ms	G.711 – A-law G.711 – u-law	Speex 32000 Hz Speex 8000 Hz

6. Сделать выводы о зависимости качества передачи речи от типа используемого кодека и от типа организации вызова (напрямую или через SIP-сервер).

3.6. Типы видеокодеков IP-телефонии

Оценить зависимость качества передачи видео по IP-сети от типа используемого кодека и типа организации вызова.

Для видеовызова в режиме «точка-точка»

1. Запустить Wireshark (локально).
2. Совершить видеовызовы с заданного терминала (Linphone), используя различные типы видеокодеков, оценить (субъективно) качество передачи речи и видеоинформации.
3. Совершить видеовызовы с заданного терминала (Linphone), изменяя полосу пропускания видео от минимального до максимального значения, оценить (субъективно) качество передачи речи и видеоинформации (поле Bandwidth control в разделе Codecs программного терминала Linphone).
4. Совершить видеовызовы с заданного терминала (Linphone), изменяя разрешение видеоизображения, оценить (субъективно) качество передачи видеоинформации (поле Preferred video resolution в разделе Codecs программного терминала Linphone).
5. Сделать выводы о зависимости качества передачи видео от типа используемого кодека, полосы пропускания и разрешения видеоизображения.

Для видеовызова через SIP-сервер Asterisk

1. Запустить Wireshark (локально).
2. Совершить видеовызовы с заданного терминала (Linphone), используя различные типы видео кодеков, оценить (субъективно) качество передачи речи и видеоинформации.
3. Совершить видеовызовы с заданного терминала (Linphone), изменяя полосу пропускания видео от минимального до максимального значения, оценить (субъективно) качество передачи речи и видеоинформации (поле Bandwidth control в разделе Codecs).
4. Совершить видеовызовы с заданного терминала (Linphone), изменяя разрешение видеоизображения, оценить (субъективно) качество передачи видеоинформации (поле Preferred video resolution в разделе Codecs).
5. Сделать выводы о зависимости качества передачи видео от типа используемого кодека, полосы пропускания и разрешения видеоизображения.

3.7. Типы терминалов

Оценить зависимость качества передачи речи по IP-сети от типа используемого терминала. Для данного задания используются терминалы двух типов: программные и аппаратные.

1. Установить соединение с программного терминала (Linphone, Twinkle или SJPhone) на аппаратный терминал и оценить (субъективно) качество передачи речи.

2. С аппаратных терминалов установить соединение и оценить (субъективно) качество передачи речи.

3. Сделать выводы о зависимости качества передачи речи от типа используемого терминала.

СПИСОК ЛИТЕРАТУРЫ

1. *Гольдштейн, Б. С.* IP-телефония / Б. С. Гольдштейн, А. В. Пинчук, А. Л. Суховицкий. – М. : Радио и связь, 2001.

2. *Гольдштейн, А. Б.* Softswitch / А. Б. Гольдштейн, Б. С. Гольдштейн. – СПб. : БХВ-Санкт-Петербург, 2006.

3. *Яновский, Г. Г.* Оценка качества передачи речи в сетях IP / Г. Г. Яновский // Вестник связи. – 2008. – № 2. – С. 91–94.

4. *Гольдштейн, Б. С.* Сети связи / Б. С. Гольдштейн, Н. А. Соколов, Г. Г. Яновский. – СПб. : БХВ-Санкт-Петербург, 2010.

5. http://www.iks.sut.ru

6. http://www.niits.ru

7. http://www.sotsbi.ru

Гольдштейн Борис Соломонович
Гойхман Вадим Юрьевич
Столповская Юлия Владимировна

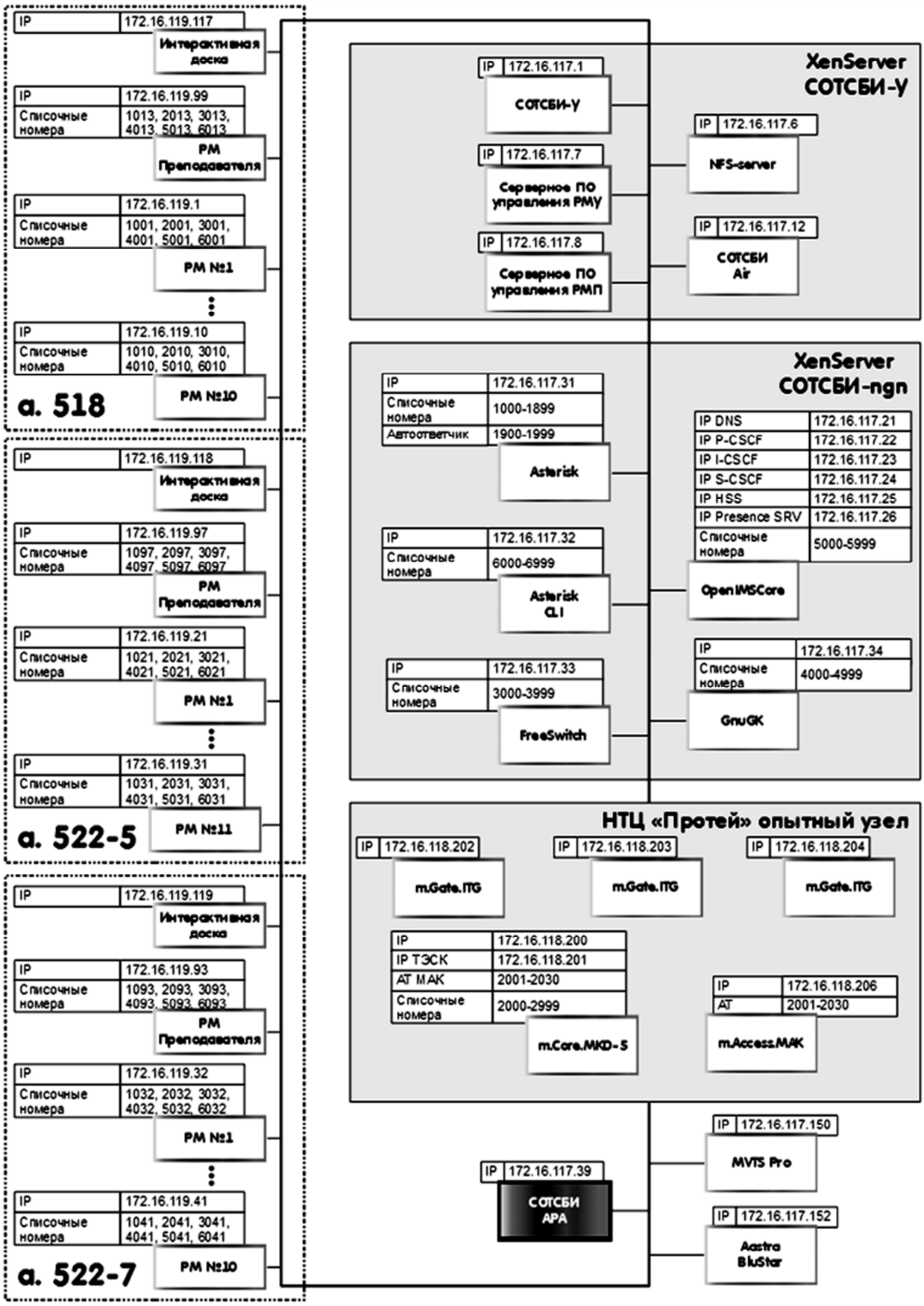
ПРОТОКОЛЫ IP-ТЕЛЕФОНИИ RTP, RTCP

Учебное пособие

Редактор *Л. А. Медведева*

Верстка *Н. А. Ефремовой*

План 2014–2015 гг., п. 17

Подписано к печати 27.02.2014
Объем 3,75 усл.-печ. л. Тираж 30 экз. Заказ 447
Редакционно-издательский центр СПбГУТ. 191186 СПб., наб. р. Мойки, 61
Отпечатано в СПбГУТ

Исследовательский полигон технологий и протоколов «СОТСБИ-У»