ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ УЗБЕКИСТАН

Сети телекоммуникаций

ПРОТОКОЛ РЕАЛЬНОГО ВРЕМЕНИ (RTP)

Основные требования

Издание официальное

«O‘ZSTANDART» AGENTLIGI
«AXBOROT-MAVLUMOT MARKAZI»
Mo‘yorliy hujjatlar Davlat fondini yuritish bo‘limi
ENGICHIL NUSXASI

Узбекское агентство стандартизации, метрологии и сертификации

Ташкент

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, METROLOGIYA
VA SERTIFIKATLASHTIRISH
AXBOROT-TEXNOLOGIYALAR
JORIY ETISH BO‘LIMI

Предисловие

1 РАЗРАБОТАН Государственным унитарным предприятием Центр научно-технических и маркетинговых исследований – «UNICON.UZ» (ГУП «UNICON.UZ»)

2 ВНЕСЕН Техническим комитетом по стандартизации в сфере связи, информатизации и телекоммуникационных технологий № 7

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ постановлением Узбекского агентства стандартизации, метрологии и сертификации (агентство «Узстандарт») от 03.12.2014 № 05-591

4 ВВЕДЕН ВПЕРВЫЕ

Информация о введении в действие (прекращении действия) настоящего стандарта и изменений к нему на территории Узбекистана публикуется в указателе, издаваемом агентством «Узстандарт». В случае пересмотра или отмены настоящего стандарта соответствующая информация будет опубликована в информационном указателе, издаваемом агентством «Узстандарт».

Исключительное право официального опубликования настоящего стандарта на территории Узбекистана принадлежит агентству «Узстандарт»

Содержание

1 Область применения 1
2 Нормативная ссылка 1
3 Термины, определения и сокращения 2
4 Общие положения 4
5 Протокол RTP 6
6 Протокол управления реального времени RTCP 11
7 Трансляторы и микшеры 32
8 Назначение и использование SSRC-идентификатора 37
9 Обеспечение безопасности 39
10 Перечень констант протокола 43
11 Описание профиля и формата трафика 44
12 Профиль RTP для аудио и видеоконференций с минимальным управлением 46

O'ZSTANDART AGENTLIGA
STANDARTLASHTIRISH, BAYLAT
NAZORATINI RIVOJLANTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ УЗБЕКИСТАН

Телекоммуникациялар тармоқлари
РЕАЛ ВАҚТ ПРОТОКОЛИ (RTP)
Асосий талаблар

954

Сети телекоммуникаций
ПРОТОКОЛ РЕАЛЬНОГО ВРЕМЕНИ (RTP)
Основные требования

Telecommunications networks
Real-Time Protocol (RTP)
General requirements

Дата введения 05. 12. 2014

1 Область применения

Настоящий стандарт устанавливает общие требования к структуре, формату и функциям протокола RTP и связанного с ним протокола управления реального времени, процедурам управления соединениями, а также к обеспечению безопасности на сетях телекоммуникаций Узбекистана при использовании протокола RTP, и предназначен для поставщиков (производителей) оборудования, использующего протокол RTP, и операторов телекоммуникаций, эксплуатирующих соответствующее оборудование.

Требования настоящего стандарта распространяются на сети следующего поколения и являются обязательными при использовании оборудования, использующего протокол реального времени, на территории Республики Узбекистан.

Требования настоящего стандарта являются обязательными при проведении сертификационных испытаний оборудования, использующего протокол RTP.

2 Нормативная ссылка

В настоящем стандарте использована ссылка на следующий стандарт:

O‘z DSt 2818:2014 Сети телекоммуникаций. Термины и определения

Издание официальное

O'ZSTANDART AGENTLIGI
5306 son bilan
«03» 12 2014 yilda
Davlat ro'yxatiga olindi

Примечание – При пользовании настоящим стандартом необходимо проверить действие ссылочного стандарта по указателю стандартов, составленному по состоянию на 1 января текущего года и по соответствующим информационным указателям, опубликованным в текущем году. Если ссылочный документ заменен (изменен), то при пользовании настоящим стандартом следует руководствоваться замененным (измененным) стандартом. Если ссылочный документ отменен без замены, то положение, в котором дана ссылка на него, применяется в части, не затрагивающей эту ссылку.

3 Термины, определения и сокращения

3.1 В настоящем стандарте применены термины по O‘z DSt 2818, а также следующие термины с соответствующими определениями:

3.1.1 **включаемый источник;** CSRC: Источник потока RTP-пакетов, который вносит вклад в общий поток, формируемый RTP- микшером.

3.1.2 **джиттер пакетов:** Разность во времени прохождения последовательных пакетов.

3.1.3 **дейтаграмма**: Пакет в сети передачи данных, передаваемый через сеть независимо от других пакетов без установления логического соединения и квитирования.

3.1.4 **идентификатор SSRC:** Случайное число, которое является уникальным для данного сеанса RTP.

3.1.5 **источник синхронизации;** SSRC: Источник потока пакетов RTP, идентифицированный 32-разрядным числовым идентификатором SSRC, который передается в заголовке RTP, независимо от сетевого адреса. Все пакеты с одним источником синхронизации используют единый интервал таймирования и единое пространство порядковых номеров, так что получатель группирует пакеты для воспроизведения с помощью источника синхронизации.

3.1.6 **микшер**: Промежуточная система, которая получает пакеты RTP от одного или более источников, возможно, изменяет формат данных, объединяет пакеты в новый пакет RTP и затем передает его. Так как множество источников сигналов в общем случае не синхронизировано, микшер корректирует таймирование составляющих потоков и генерирует собственную синхронизацию для объединенного потока. Все информационные пакеты, сформированные микшером, идентифицируются, как имеющие микшер в качестве их источника синхронизации.

3.1.7 **монитор**: Приложение, которое получает пакеты RTCP, посланные участниками сеанса RTP, в частности, отчеты приема, и оценивает текущее качество обслуживания для контроля распределения, обнаружения ошибок и долговременной статистики.

3.1.8 **оконечная система**: Приложение, которое генерирует содержимое, передаваемое в пакетах RTP, и/или которое потребляет

O‘STANDART AGENTLIGI
STANDARTLASHTIRISH, QAYTA
KAZORATLIK MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

содержимое полученных пакетов RTP. Оконечная система может действовать как один или более (но обычно только один) источников синхронизации в каждом сеансе RTP.

3.1.9 **октет:** Группа из восьми разрядов, синоним слова byte.

3.1.10 **пакет RTP:** Протокольный блок данных, состоящий из фиксированного заголовка RTP, возможно, пустого списка включаемых источников, расширения и поля данных.

3.1.11 **пакет RTCP:** Управляющий пакет, состоящий из фиксированной части заголовка, подобной заголовкам информационных пакетов протокола RTP, за которой следуют структурные элементы, изменяемые в зависимости от типа пакета RTCP.

3.1.12 **поле данных RTP:** Информация, пересылаемая в пакете RTP, например фрагменты звука или сжатые видео данные.

3.1.13 **порт:** Абстракция, используемая протоколами транспортного уровня для различения множества адресатов в пределах одного компьютера. Порт определяется своим номером. Номер порта - это число, определяющее конкретное приложение, которому предназначены пересылаемые данные.

3.1.14 **профиль**: Набор параметров протоколов RTP и RTCP для класса приложений, определяющий особенности их функционирования.

3.1.15 **режим реального времени:** Режим обработки данных, при котором обеспечивается взаимодействие вычислительной системы с внешними по отношению к ней процессами в темпе, соизмеримом со скоростью протекания этих процессов.

3.1.16 **сеть IP:** Сеть с пакетной коммутацией, использующая стек протоколов TCP/IP для обмена данными.

3.1.17 **сеанс связи RTP**: Период с момента установления группы участников RTP-обмена до ее исчезновения.

3.1.18 **средства не-RTP**: Протоколы и механизмы, которые могут быть необходимы в дополнение к протоколу RTP, чтобы обеспечить приемлемое обслуживание.

3.1.19 **список CSRC:** Список SSRC-идентификаторов, вставляемый микшером в заголовок RTP-пакетов, которые идентифицируют парциальные источники.

3.1.20 **транслятор**: Промежуточная система, которая переадресует RTP-пакеты, не изменяя их идентификаторы источника синхронизации.

3.1.21 **транспортный адрес**: Комбинация сетевого адреса и порта, которая идентифицирует конечную точку канала (например, IP-адрес и UDP-порт). Пакеты следуют от транспортного адреса отправителя к транспортному адресу получателя.

3.1.22 **трафик RTP:** Мультимедийные данные, передаваемые в пакете протокола RTP, например, звуковые отсчеты или сжатые видеоданные.

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DANLAT
NAZORATIN, AXBOROT
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

3.2 В настоящем стандарте применены следующие сокращения:

AES - Advanced Encryption Standard (симметричный алгоритм блочного шифрования);

ASCII - American Standart Code for Information Interchange (Американский стандартный код для обмена информацией);

CBC - Cipher block chaining (цепочка шифруемых блоков, режим стандарта шифрования данных DES);

CNAME - Canonical name (каноническое имя);

CSRC - Contributing Source (источник потока);

DES - Data Encryption Standard (стандарт шифрования данных);

DLSR - Delay since last sender report (задержка с момента последнего отчета отправителя);

IANA - Internet Assigned Numbers Authority (сообщество назначения номеров Internet);

IP - Internet Protocol (Интернет протокол);

IPM - IP Multicast (групповая передача с использованием протокола IP);

LSR - Last sender report (последний отчет отправителя);

NGN - Next Generation Networks (сети следующего поколения);

NTP - Network Time Protocol (сетевой протокол времени);

MPEG - Moving Picture Experts Group (экспертная группа по движущемуся изображению);

PT - Payload Type (тип трафика);

RR - Receiver Report (отчет получателя);

RTCP - Real-Time Control Protocol (протокол управления реального времени);

RTP - Real-Time Protocol (протокол реального времени);

SDES - Source description items (пакет описания источника);

SR - Sender Report (отчет отправителя);

SRTP - Secure Real-time Transport Protocol (безопасный транспортный протокол реального времени);

SSRC - Synchronization Source (источник синхронизации);

TCP - Transport Control Protocol (протокол управления передачей);

UDP - User Datagram protocol (протокол передачи дейтаграмм пользователя).

4 Общие положения

В IP-сетях, не обеспечивающих гарантированное качество обслуживания, пакеты могут теряться, может изменяться порядок их поступления; данные, передаваемые в пакетах, могут искажаться. Для обеспечения надежной доставки передаваемой информации в этих

O'ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, METROLOGIYA
NAZORATI MILLIY AGENTLIGI
AXBOROT TEXNOLOGIYALARI
JORIY ETISH BOSHQARMASI

условиях используются различные процедуры транспортного уровня. При передаче цифровых данных для этой цели применяется протокол TCP. Для приложений аудио- и видеоконференцсвязи задержки пакетов гораздо в большей степени влияют на качество сигнала, чем отдельные искажения данных. Различия в задержках могут приводить к появлению пауз. Для таких приложений применяется протокол реального времени RTP.

Протокол RTP регламентирует передачу мультимедийных данных в пакетах через информационно-вычислительные сети на транспортном уровне и дополняется протоколом управления передачей данных в реальном масштабе времени RTCP. Протокол RTCP обеспечивает контроль доставки мультимедийных данных, контроль качества обслуживания, передачу информации об участниках текущего сеанса связи, управление и идентификацию.

Действие протокола RTP сводится к присваиванию каждому исходящему пакету временных меток. На приемной стороне временные метки пакетов указывают на то, в какой последовательности и с какими задержками их необходимо воспроизводить. Поддержка RTP и RTCP позволяет принимающему узлу располагать принимаемые пакеты в надлежащем порядке, снижать влияние неравномерности времени задержки пакетов в сети на качество сигнала и восстанавливать синхронизацию между аудио и видео, чтобы поступающая информация могла правильно прослушиваться и просматриваться пользователями.

Характерные для IP-сетей временные задержки и джиттер могут серьезно исказить информацию, чувствительную к задержке, например, речь и видеоинформацию, сделав ее абсолютно непригодной для восприятия. Протокол RTP позволяет компенсировать негативное влияние джиттера на качество речевой и видеоинформации. В то же время, он не имеет собственных механизмов, гарантирующих своевременную доставку пакетов или другие параметры качества услуг, это осуществляют нижележащие протоколы. Протокол RTP не предотвращает нарушения порядка следования пакетов, но при этом и не предполагает, что основная сеть абсолютно надежна и передает пакеты в нужной последовательности. Порядковые номера, включенные в RTP, позволяют получателю восстанавливать последовательность пакетов отправителя.

Протокол RTP поддерживает как двустороннюю связь, так и передачу данных группе адресатов, если групповая передача поддерживается нижележащей сетью. Он предназначен для обеспечения информации, требуемой отдельным приложениям, и в большинстве случаев интегрируется в работу приложения.

Протокол RTP функционирует поверх протокола транспортного уровня UDP. Оба протокола вносят свои доли в функциональность

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATI, MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

транспортного уровня. Протоколы RTP и RTCP являются независимыми от нижележащих уровней - транспортного и сетевого, поэтому протоколы RTP/RTCP могут использоваться с другими подходящими транспортными протоколами.

Для того, чтобы протокол RTP был более гибким и мог применяться для различных приложений, некоторые его параметры сделаны преднамеренно неопределенными, но зато в нем предусмотрено понятие профиля. В профиле определяются 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. Каждое приложение обычно работает только с одним профилем, и задание типа профиля происходит путем выбора соответствующего приложения. Никакой явной индикации типа профиля номером порта, идентификатором протокола и т.п. не предусмотрено.

5 Протокол RTP

5.1 Поля фиксированного заголовка RTP

Пакет RTP должен включать в свой состав фиксированный заголовок, необязательное расширение заголовка с переменной длиной и поле данных. Фиксированный заголовок пакетов протокола RTP имеет формат, приведенный на рисунке 1.

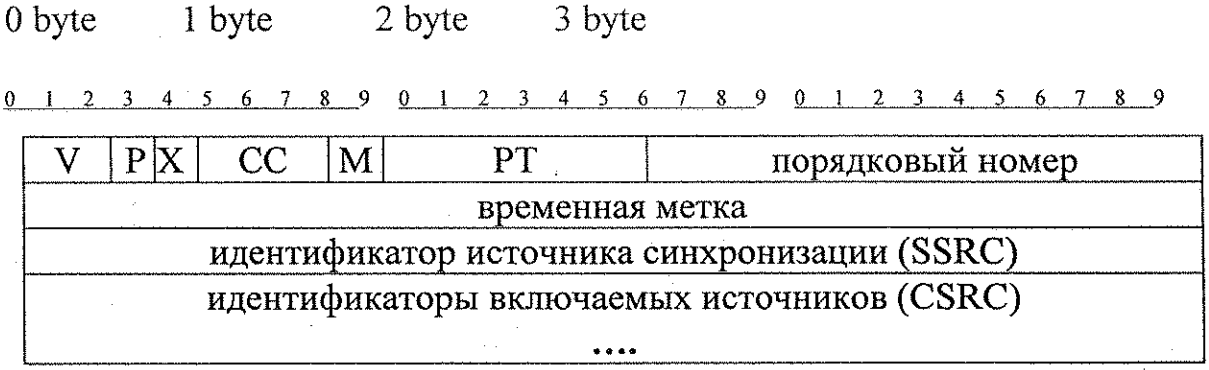


Рисунок 1 – Заголовок пакета RTP

Первые двенадцать октетов присутствуют в каждом пакете RTP, в то время как поле идентификаторов включаемых источников CSRC присутствует только тогда, когда оно вставлено микшером. Поля должны иметь следующие назначения:

– версия (V - version): 2 bit. Это поле идентифицирует версию RTP. Оборудование должно поддерживать версии формата заголовка пакета RTP до второй включительно;

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, PAYLAT
NAZORATINI MONOPOLIASHTIRISHNI
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

– дополнение (P - padding): 1 bit. 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 bit. Если бит расширения установлен, то за фиксированным заголовком следует расширение заголовка;

– счетчик CSRC (CC): 4 bit. Счетчик CSRC содержит число идентификаторов включаемых источников CSRC, которые следуют за фиксированным заголовком;

– маркер (M): 1 bit. Интерпретация маркера определяется профилем. Он предназначен для того, чтобы позволить маркировать в потоке пакетов значительные события (например, границы видеокадра). Профиль может вводить дополнительные биты маркера или определять, что никакого бита маркера не имеется, изменяя число битов в поле типа трафика;

– тип трафика (PT): 7 bit. Это поле идентифицирует формат трафика RTP и определяет его интерпретацию приложением. Профиль определяет заданное по умолчанию статическое соответствие значений PT и форматов трафика. Дополнительные коды типа трафика могут быть определены динамически через не-RTP средства. Отправитель пакета RTP в любой момент времени выдает единственное значение типа трафика RTP. Это поле не предназначено для мультиплексирования отдельных мультимедийных потоков;

– порядковый номер: 16 bit. Значение порядкового номера увеличивается на единицу с каждым посланным информационным пакетом RTP и может использоваться получателем для обнаружения потерь пакетов и восстановления их исходной последовательности. Начальная величина порядкового номера выбирается случайным образом, чтобы усложнить попытки взлома ключа с опорой на известные значения данного поля (даже если шифрование не используется источником, так как пакеты могут проходить через транслятор, который применяет шифрование);

– временная метка: 32 bit. Временная метка отражает момент дискретизации для первого октета в информационном пакете RTP. Момент дискретизации должен быть получен от таймера, который увеличивает свои значения монотонно и линейно во времени, для обеспечения синхронизации и определения джиттера. Разрешение таймера должно быть достаточным для желательной точности синхронизации и измерения джиттера поступления пакетов (одного отчета таймера на видеокадр обычно бывает недостаточно). Частота таймирования зависит

O‘ZSTANDART AGENTLIGA
STANDARTLASHTIRISH, DAVLAT
NAZORAT VA MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

от формата передаваемого трафика и задается статически в профиле или спецификации формата трафика или может задаваться динамически для форматов трафика, определенных через не-RTP средства. Если пакеты RTP генерируются периодически, то должны использоваться номинальные моменты дискретизации, определяемые таймером дискретизации, а не значения системного таймера. Например, для звукового сигнала с фиксированной скоростью желательно, чтобы датчик временной метки увеличивался на единицу для каждого периода дискретизации. Если звуковое приложение из устройства ввода читает блоки, содержащие 160 отсчетов, то временная метка при этом должна увеличиваться на 160 для каждого такого блока, независимо от того, передан ли блок в пакете или сброшен, как пауза. Начальное значение временной метки, так же, как и начальное значение порядкового номера, является случайной величиной. Несколько последовательных пакетов RTP могут иметь равные временные метки, если они логически генерируются одновременно, например, принадлежат одному и тому же видеокадру. Последовательные пакеты RTP могут содержать немонотонные временные метки, если данные не передаются в порядке дискретизации, как в случае интерполируемых видеокадров MPEG (однако порядковые номера пакетов при передаче все же будут монотонными);

– SSRC: 32 bit. Поле SSRC идентифицирует источник синхронизации. Этот идентификатор выбирается случайным образом так, чтобы никакие два источника синхронизации в рамках одного и того же сеанса связи RTP не имели одинаковых идентификаторов SSRC. Хотя вероятность того, что несколько источников выберут один и тот же идентификатор, низка, все же все реализации RTP должны быть готовы обнаруживать и разрешать подобные коллизии;

– список CSRC: от 0 до 15 пунктов, 32 bit каждый. Список CSRC идентифицирует включаемые источники трафика, содержащегося в пакете. Число идентификаторов задается полем CC. Если имеется более пятнадцати включаемых источников, то только 15 из них могут быть идентифицированы. Идентификаторы CSRC вставляются микшерами при использовании идентификаторов SSRC для включаемых источников. Например, для звуковых пакетов идентификаторы SSRC всех источников, которые были смешаны при создании пакета, перечисляются в списке CSRC, обеспечивая корректную индикацию источников сообщений для получателя.

5.2 Сеансы связи RTP

В соответствии с протоколом RTP трафик различных типов должен передаваться отдельно, в разных сеансах связи RTP. Сеанс определяется конкретной парой транспортных адресов назначения (один сетевой адрес

O'ZBEKISTON RESPUBLIKASI STANDARTLASHTIRISH, METR... MAHSULOT VA XIZMAT SIFATINI BOSHQARISH AXBOROT TEXNOLOGIYALARINI JORIY ETISH BOSHQARMASI

плюс пара портов для RTP и RTCP). Например, в телеконференции, составленной из звукового и видеосигнала, кодированных отдельно, трафик каждого типа нужно передавать в отдельном сеансе RTP со своим собственным транспортным адресом назначения. Не предполагается, что звуковой и видеосигнал будут передаваться в одном сеансе RTP и разделяться на основе типа трафика или полей SSRC. Перемежение пакетов, имеющих различные типы трафика, но использующих один и тот же SSRC, вызвало бы некоторые проблемы:

a) если в течение сеанса один из типов трафика изменится, то не будет никаких общих средств, чтобы определить, какая из старых величин была заменена новой;

b) SSRC идентифицирует единственное значение интервала таймирования и пространство порядкового номера. Перемежение множества типов трафика потребовало бы различных интервалов синхронизации, если тактовые частоты разных потоков различаются, и различных пространств порядковых номеров для индикации типа трафика, к которому относится потеря пакета;

c) сообщения отправителя и получателя протокола RTCP описывают только одно значение интервала таймирования и пространство порядковых номеров для SSRC и не передают поле типа трафика;

d) микшер RTP не способен объединять перемеженные потоки различных типов трафика в один поток;

e) передаче множества типов трафика в одном сеансе RTP препятствуют следующие факторы: использование различных сетевых путей или распределение сетевых ресурсов; прием подмножества мультимедийных данных, когда это требуется, например, только звука, если видеосигнал превысил доступную полосу пропускания; реализации приемника, которые используют отдельные процессы для различных типов трафика, в то время как использование отдельных сеансов RTP допускает реализации как с одним, так и со множеством процессов.

В соответствии с вышеизложенным для каждого типа трафика следует использовать свой сеанс RTP.

5.3 Определяемые профилем изменения заголовка RTP

Существующий заголовок информационного пакета RTP является полным для набора функций, требуемых в общем случае для всех классов приложений, которые могли бы поддерживать RTP. Однако, для лучшего приспособления к конкретным задачам заголовок может быть видоизменен посредством модификаций или дополнений, определенных в спецификации профиля.

Бит маркера и поле типа трафика несут информацию, зависящую от профиля, но они расположены в фиксированном заголовке, так как

O ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATI VA KUZATUVCHILIK ISHLARI
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BO‘LIMI

ожидается, что в них будут нуждаться много приложений. Октет, содержащий эти поля, может быть переопределен профилем для удовлетворения различным требованиям, например, с большим или меньшим количеством битов маркера. Если имеются какие-либо биты маркера, они должны размещаться в старших битах октета, так как независимые от профиля мониторы могут быть способны наблюдать корреляцию между характером потерь пакетов и битом маркера.

Дополнительная информация, которая требуется для конкретного формата трафика (например, тип кодирования видеосигнала), должна передаваться в поле данных пакета. Она может размещаться на определенном месте в начале или внутри массива данных.

Если конкретный класс приложений нуждается в дополнительных функциональных возможностях, не зависящих от формата трафика, то профиль, с которым функционируют эти приложения, должен определить дополнительные фиксированные поля, располагаемые сразу после поля SSRC существующего фиксированного заголовка. Эти приложения будут способны быстро напрямую обращаться к дополнительным полям, в то время как профиль-независимые мониторы или регистраторы все еще будут способны обрабатывать пакеты RTP, интерпретируя только первые двенадцать октетов.

5.4 Расширение заголовка RTP

Для обеспечения возможности отдельным реализациям экспериментировать с новыми функциями, независимыми от формата трафика, которые требуют, чтобы в заголовке информационного пакета передавалась дополнительная информация, протоколом 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 (вслед за списком CSRC, если он есть) присоединяется расширение заголовка с переменной длиной. Это расширение заголовка предназначено только для ограниченного использования. Расширение заголовка пакета RTP должно иметь формат, представленный на рисунке 2.

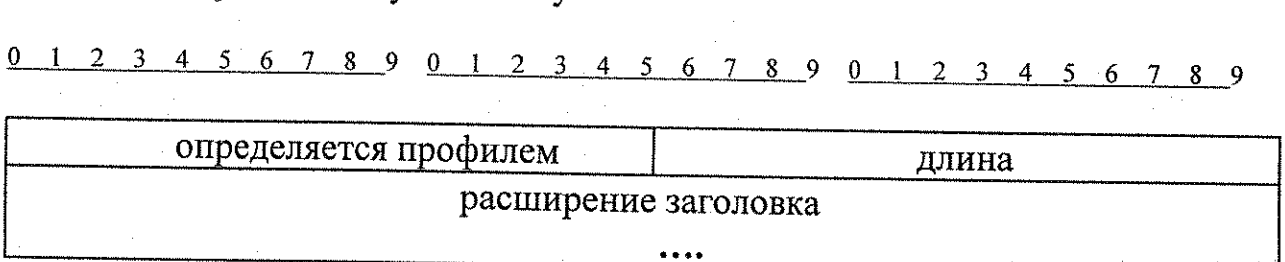


Рисунок 2 – Формат расширения заголовка

O'ZBEKISTON MILLIY STANDARTLASHTIRISH, BAHOLAT NAZORAT VA AXBOROT TEXNOLOGIYALARINI JORIY ETISH AGENTLIGI

Расширение содержит 16-разрядное поле длины, которое показывает количество 32-разрядных слов в нем, исключая четырехоктетный заголовок расширения (следовательно, длина может иметь нулевое значение). Только одно расширение может быть добавлено к фиксированному заголовку информационного пакета RTP. Чтобы позволить каждому из множества взаимодействующих реализаций экспериментировать независимо с различными расширениями заголовка или позволять конкретной реализации экспериментировать более чем с одним типом расширения заголовка, использование первых 16 bit расширения не определено, оставлено для различающих идентификаторов или параметров. Формат из этих 16 bit должен быть определен спецификацией профиля, с которым работают приложения.

6 Протокол управления реального времени RTCP

6.1 Основные функции RTCP

Протокол RTCP основан на периодической передаче пакетов управления всем участникам сеанса связи при использовании того же механизма распределения, что и протокол RTP. Протокол нижележащего уровня должен обеспечить мультиплексирование информационных и управляющих пакетов, например, с использованием различных номеров портов UDP. Протокол RTCP выполняет четыре основные функции:

a) главная функция - это обеспечение обратной связи для оценки качества распределения данных. Это неотъемлемая функция RTP, как транспортного протокола, она связана с функциями управления потоком и перегрузками других транспортных протоколов. Обратная связь может быть непосредственно полезна для управления адаптивным кодированием, но эксперименты с IPM показали, что обратную связь с получателями также важно иметь для диагностики дефектов при распространении информации. Посылка отчетов обратной связи о приеме данных всем участникам позволяет при наблюдении проблем, оценивать, являются они локальными или глобальными. С механизмом распределения IPM для таких объектов, как поставщики услуг сети, возможно также получать информацию обратной связи и действовать при диагностике проблем сети, как монитор третьей стороны. Эта функция обратной связи обеспечивается отчетами отправителя и приемника RTCP;

b) RTCP поддерживает устойчивый идентификатор источника данных RTP на транспортном уровне, называемый каноническим именем CNAME. Так как идентификатор SSRC может изменяться, если обнаружен конфликт или перезапущена программа, то получателям для отслеживания каждого участника требуется CNAME. Получатели также требуют CNAME для отображения множества потоков информации от данного

O‘ZSTANDART AGENTLIGA
STANDARTLASHTIRISH, DAVLAT
NAZORAT VA AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSH QARMASI

участника на множество связанных сеансов RTP, например, при синхронизации звукового и видеосигнала;

c) первые две функции требуют, чтобы все участники посылали пакеты RTCP, следовательно, для предоставления возможности масштабирования числа участников протоколом RTP должна регулироваться частота передачи таких пакетов. При посылке каждым участником телеконференции управляющих пакетов всем остальным участникам, каждый может независимо оценивать общее число участников. Это число используется при вычислении частоты отправления пакетов;

d) дополнительная функция RTCP, обеспечивающая информацию управления сеансом (например, идентификацию участника), которая будет отражена в интерфейсе пользователя. Наиболее вероятно, что это будет полезным в «свободно управляемых» сеансах, где участники вступают в группу и выходят из нее без контроля принадлежности или согласования параметров.

Функции с первой по третью являются обязательными, когда RTP используется в IPM, и рекомендуемыми во всех остальных случаях. Разработчикам приложений RTP рекомендуется избегать механизмов, работающих только в двустороннем режиме и не масштабируемых для увеличения числа пользователей.

6.2 Требования к пакетам RTCP

Для передачи различного рода информации управления определено несколько типов пакетов RTCP, в том числе:

– SR: отчет отправителя, для статистической информации о передаче и приеме участников, которые являются активными отправителями;

– RR: отчет получателя, для статистики приема от участников, которые не являются активными отправителями;

– SDES: пакет описания источника, включая CNAME;

– BYE: указатель пакета завершения связи;

– APP: функции, определяемые приложением.

Каждый пакет RTCP должен начинаться с фиксированной части (подобной фиксированной части информационных пакетов RTP). За ней должны следовать структурные элементы, которые могут иметь переменную длину согласно типу пакета, но всегда выравниваться 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

STANDARTLASHTIRISH, DAVLA
NAZORAT VA MUVOFIQLASHTIRISH
ANDOROT TEXNOLOGIYALARINI

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 существуют следующие требования:

a) статистика приема (в пакетах SR или RR) должна посылаться так часто, как позволяет полоса пропускания, чтобы максимизировать точность статистики: следовательно, в каждый составной пакет RTCP должен включаться пакет отчета;

b) новые участники телеконференции должны получить CNAME источника как можно скорее, чтобы опознать источник и начать согласовывать формат мультимедийных данных, так что каждый составной пакет RTCP должен также включать пакет описания источника SDES с пунктом CNAME;

c) число типов пакетов, которые могут появляться первыми в составном пакете, должно быть ограничено, чтобы увеличить число постоянных битов в первом слове и уменьшить вероятность ошибок при распознавании пакетов RTCP среди пакетов других протоколов.

Все пакеты RTCP должны передаваться в составном пакете, включающем, по крайней мере, два индивидуальных пакета (SR/RR и SDES), со следующим рекомендуемым форматом:

a) префикс шифрования. Если составной пакет должен быть зашифрован, то ему предшествует произвольная 32-разрядная величина, повторно передаваемая в каждом составном пакете;

b) SR или RR. 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 посланы, ни получены и если единственный пакет RTCP в составном пакете - это пакет BYE (тогда посылается пустой пакет RR);

c) дополнительные пакеты 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;

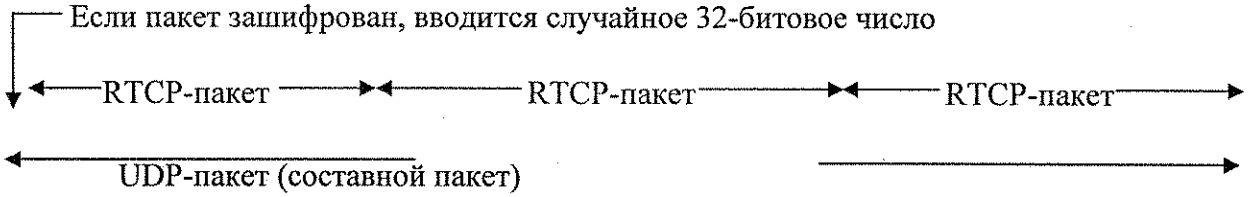
d) SDES. Пакет SDES, содержащий пункт CNAME, должен включаться в каждый составной пакет RTCP. Если требуется конкретным приложением, то дополнительно и другие пункты описания источника могут быть включены в пакет SDES в соответствии с ограничениями полосы пропускания;

e) BYE или APP. Другие типы пакетов RTCP могут следовать в любом порядке, за исключением того, что пакет BYE должен быть последним пакетом, посланным с данным SSRC/CSRC.

O‘ZSTANDART AGENTLIGA
STANDARTLASHTIRISH, DAVLAT
NAZORATI VA UYG‘UNLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BO‘LIMIDAN

Для трансляторов и микшеров рекомендуется объединять индивидуальные пакеты RTCP из множества источников, с которыми они работают, в один составной пакет всякий раз, когда это возможно, чтобы уменьшить избыточность и не передавать лишние заголовки пакета.

Пример составного RTCP-пакета, который может быть сформирован с микшером, представлен на рисунке 3.



R	SR #Доклад #Узел #Узел SDES	#CNAME PHONE #CNAME LOC #BYE##why
R	SR #отправителя # 1 # 2	# # # ##
R	SR # # #	# # # ##
R	SR # # #	# # # ##

(#: SSRC/CSRC)

Рисунок 3 – Пример составного пакета RTCP

Если полная длина составного пакета превышает величину максимального блока передачи сетевого пути, то составной пакет может быть сегментирован на множество более коротких составных пакетов, которые будут переданы в отдельных блоках данных протокола нижележащего уровня. В этом случае каждый из составных пакетов должен начинаться с пакета SR или RR.

Приложение может игнорировать входящие пакеты RTCP с неизвестными ему типами. Дополнительные типы пакетов RTCP могут быть зарегистрированы в IANA.

6.3 Интенсивность передачи пакетов RTCP

6.3.1 Полоса пропускания сеанса пакетов RTCP

Протокол RTP позволяет приложению автоматически масштабировать представительность сеанса связи в пределах от нескольких участников до нескольких тысяч. Например, в аудиоконференции трафик данных, по существу, является самоограничивающим, потому что только один или два человека могут говорить одновременно, и при групповом распределении скорость передачи данных на любой линии связи остается относительно постоянной, независящей от числа участников. Однако, трафик

STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH
AXBOROT

управления самоограничивающим не является. Если отчеты приема от каждого участника посылаются с постоянной интенсивностью, то трафик управления с ростом числа участников будет расти линейно. Следовательно, должен быть предусмотрен специальный механизм понижения частоты передачи управляющих пакетов.

Для каждого сеанса предполагается, что трафик данных соответствует агрегированному пределу, называемому полосой пропускания сеанса связи, которая совместно используется всеми участниками. Эта полоса пропускания может быть зарезервирована, и ее предел установлен сетью.

Полоса пропускания сеанса не зависит от типа кодирования мультимедийных данных, но выбор типа кодирования может быть ограничен полосой пропускания сеанса связи. Параметр полосы пропускания сеанса, как ожидается, будет обеспечен приложением управления сеанса, когда оно вызовет мультимедийное приложение, но мультимедийные приложения могут также устанавливать значение по умолчанию, основанное на полосе пропускания данных с единственным отправителем для типа кодирования, выбранного для данного сеанса.

Вычисления полосы пропускания для трафика управления и данных выполняются с учетом нижележащих протоколов транспортного и сетевого уровней (например, UDP и IP). Заголовки уровня звена передачи данных при вычислениях не учитываются, так как пакет по мере его передачи может инкапсулироваться с различными заголовками уровня звена передачи данных.

Трафик управления должен быть ограничен малой и известной частью полосы пропускания сеанса: малой настолько, чтобы не пострадала основная функция транспортного протокола - передача данных; известной так, чтобы трафик управления мог быть включен в спецификацию полосы пропускания, данную протоколу резервирования ресурсов, и так, чтобы каждый участник мог независимо вычислить свою долю. Предполагается, что часть полосы пропускания сеанса, выделяемая для RTCP, должна быть установлена равной 5 %. Все участники сеанса должны использовать одинаковую величину полосы пропускания RTCP, так чтобы вычисленные значения интервала передачи пакетов управления были одинаковыми. Поэтому эти константы должны быть установлены для каждого профиля.

Алгоритм вычисления интервала между посылками составных пакетов RTCP для разделения среди участников полосы пропускания, выделенной для трафика управления, имеет следующие основные характеристики.

Отправители коллективно используют по крайней мере 1/4 полосы пропускания трафика управления так, как в сеансах с большим количеством получателей, но с малым числом отправителей; едва

O‘ZSTANDART AGENTLIGA
STANDARTLASHTIRISH, DAVLAT
NAZORATINI, KUZATISHLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

установив соединение, участники в течение короткого интервала времени получают CNAME передающих сайтов.

Требуется, чтобы расчетный интервал между пакетами RTCP, как минимум, превышал 5 s, чтобы избежать пачек пакетов RTCP, превышающих позволенную полосу пропускания, когда число участников мало, и трафик не сглаживается согласно закону больших чисел.

Интервал между пакетами RTCP изменяется случайно в пределах от половины до полутора расчетных интервалов во избежание непреднамеренной синхронизации всех участников. Первый пакет RTCP, посланный после вступления в сеанс связи, также задерживается случайным образом (до половины минимума интервала RTCP) в случае, если приложение начато во множестве сайтов одновременно, например, при объявлении о начале сеанса связи.

Для автоматической адаптации к изменениям в объеме передаваемой информации управления вычисляется динамическая оценка среднего размера составного пакета RTCP с использованием всех полученных и посланных пакетов.

Этот алгоритм может использоваться для сеансов, в которых передача пакетов допустима для всех участников. В этом случае, параметр полосы пропускания сеанса - это произведение полосы пропускания индивидуального отправителя на число участников, и полоса пропускания RTCP составляет 5 % от этой величины.

6.3.2 Учет числа участников сеанса связи

Вычисление величин интервалов передачи пакетов RTCP зависит от оценки числа участников сеанса связи. Новые участники учитываются, когда они отмечаются в работе и когда для каждого в таблице создается запись с соответствующим идентификатором SSRC или CSRC. Новые записи не могут иметь силу, пока не будет получено множество пакетов, содержащих новый SSRC. При получении пакета BYE с соответствующим идентификатором SSRC записи из таблицы удаляются.

Участник может пометить другой сайт как неактивный или удалить соответствующую ему запись, если никаких пакетов RTP или RTCP не было получено для некоторого числа интервалов передачи отчетов RTCP (предлагается пять интервалов). Это обеспечивает некоторую устойчивость к потерям пакетов. Все сайты для того, чтобы работать правильно, должны вычислять приблизительно одну и ту же величину периода передачи отчетов RTCP в соответствии с заданным таймаутом.

Если сайт, признанный участником телеконференции, впоследствии отмечается, как неактивный, то состояние этого сайта еще какое-то время должно сохраняться неизменным, и сайт все еще должен учитываться в общем числе сайтов, совместно использующих полосу пропускания RTCP. Для данного таймаута предложено значение, равное 30 min.

O'ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH V
AXBOROT TEXNOLOGIYALARINI

6.3.3 Выделение полосы пропускания для пакетов описания источника SDES

Приложения должны учитывать возможность передачи дополнительных пунктов при распределении полосы пропускания RTCP, потому что это замедлит скорость, с которой будут передаваться отчеты о приеме и CNAME, ухудшая характеристики протокола. Рекомендуется, чтобы для передачи дополнительной информации использовалось не более 20 % полосы пропускания RTCP, выделенной одному участнику. Кроме того, не требуется, чтобы все пункты SDES использовались каждым приложением. За теми из них, которые включены в использование, должны быть закреплены некоторые части полосы пропускания.

Например, приложение может быть разработано так, чтобы включать в пакеты SDES только пункты CNAME, NAME, EMAIL и никаких других. Пункту NAME может быть назначен гораздо более высокий приоритет, чем пункту EMAIL, потому что NAME будет индицироваться непрерывно в интерфейсе пользователя данного приложения, в то время как пункт описания пользователя EMAIL будет показываться только по требованию. В каждом интервале RTCP посылается пакет RR и пакет SDES с пунктом CNAME. Для сеанса с малым числом пользователей, работающего с минимальным интервалом отчетности, это было бы в среднем каждые 5 s. Каждый третий интервал (15 s), один дополнительный пункт был бы включен в пакет SDES. Семь из восьми раз это будет пункт NAME, а каждый восьмой раз (2 min) – пункт EMAIL.

Если несколько приложений функционируют одновременно, взаимодействуя между собой через общий для всех пункт CNAME (например, в мультимедийной конференции, составленной из сеансов RTP для каждого типа трафика), то дополнительная информация SDES может представляться только в одном сеансе RTP. Во всех остальных сеансах передается только пункт CNAME.

6.4 Пакеты отчетов отправителя и получателя (SR и RR)

6.4.1 Форма отчета SR и RR

Получатели RTP обеспечивают обратную связь - оценку качества приема, используя пакеты отчета RTCP, которые могут принимать одну из двух форм в зависимости от того, является получатель также и отправителем или нет. Единственная разность между формами отчетов SR и RR, помимо кода типа пакета, - это то, что отчет отправителя включает 20-байтовый раздел информации отправителя для использования активными отправителями. SR передается, если сайт посылал любые

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATI VA SERTIFIKATLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

пакеты данных в течение интервала, начиная с передачи последнего или предыдущего отчета, в противном случае передается RR.

Формы SR и RR включают нуль или более блоков отчета приема, один для каждого из источников синхронизации, от которых получатель принял пакеты данных RTP, начиная с последнего отчета. Для включаемых источников, перечисленных в списке CSRC, отчеты не выпускаются. Каждый блок отчета приема обеспечивает статистику относительно данных, полученных от конкретного источника, обозначенного в этом блоке. Так как максимум 31 блок приемных отчетов возможен в пакетах SR или RR, то дополнительные пакеты RR могут быть помещены в стек после начальных пакетов SR или RR. Это необходимо, чтобы содержать отчеты приема для всех источников, отмечаемых в течение интервала отчетности, начиная с последнего отчета.

6.4.2 Формат пакета SR

Пакет SR должен содержать три основных секции и может содержать дополнительную четвертую, определяемую профилем, секцию расширения. На рисунке 4 приведен формат пакета SR.

Первая секция. Заголовок имеет длину 8 октетов. Ее поля имеют следующие значения:

– версия (V - version): 2 bit. Идентифицирует версию RTP, которая является одинаковой в пакетах RTCP и информационных пакетах RTP;

– дополнение (P - padding): 1 bit. 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;

– счетчик отчетов приема (RC - reception report count): 5 bit. Число блоков отчетов приема, содержащихся в данном пакете. Нуль - возможное значение RC;

– тип пакета (PT - packet type): 8 bit. Содержит константу 200 для идентификации пакета, как пакета SR протокола RTCP;

– длина: 16 bit. 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 bit. Идентификатор источника синхронизации для источника данного пакета SR.

STANDARTLASHTIRISH, DATALAT
MAZORATINI RIVOJLANTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

0 byte 1 byte 2 byte 3 byte

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9

V	P	RC	PT=SR=200	длина
SSRC отправителя				
временная метка NTP, наиболее значащее слово				
временная метка NTP, наименее значащее слово				
временная метка RTP				
счетчик пакетов отправителя				
счетчик октетов отправителя				
SSRC первого источника (SSRC_1)				
доля потерь		общее число потерянных пакетов		
расширенный наибольший полученный порядковый номер				
джиттер прибытия				
временная метка последнего SR (LSR)				
задержка с момента последнего SR (DLSR)				
SSRC второго источника (SSRC_2)				
. . .				
расширение, зависящее от профиля				

Рисунок 4 – Формат пакета SR

Вторая секция, информация отправителя, имеет длину 20 октетов и присутствует в каждом пакете SR. Она подытоживает факты передачи данных от этого отправителя. Поля второй секции имеют следующие значения:

– временная метка NTP: 64 bit. 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. Неопределенность измерения для временной метки не обозначается, поскольку она не может быть известна. Отправитель, который может следить за прошедшим временем, но не имеет данных об абсолютном времени, вместо этого может использовать время, прошедшее с начала соединения сеанса. Оно должно быть меньше, чем 68 лет, - тогда старший разряд будет иметь нулевое значение. Для оценки прошедшего абсолютного времени допустимо использование

O‘ZSTANDART AGENTLIGA
STANDARTLASHTIRISH, DAVLAT
NAZORATI VA KUZATISHLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

таймера дискретизации. Отправитель, который не имеет никаких данных об абсолютном или прошедшем времени, может устанавливать временную метку NTP в нуль;

– временная метка RTP: 32 bit. Соответствует тому же самому времени, что и временная метка NTP (см. выше), 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. В большинстве случаев эта временная метка не будет равна временной метке RTP в любом соседнем информационном пакете. Она вычисляется из соответствующей временной метки NTP с использованием связи между счетчиком временной метки RTP и реальным временем, которое поддерживается периодически контролем абсолютного времени в моменты дискретизации;

– счетчик пакетов отправителя: 32 bit. 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: 32 bit . Общее число октетов трафика (то есть 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.

Третья секция пакета SR 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 передает статистическую информацию о приеме пакетов RTP из одного источника синхронизации. Получатели не переносят статистику, когда источник изменяет свой идентификатор SSRC вследствие коллизий. Эта статистика включает следующую информацию:

– SSRC_n : 32 bit. Идентификатор SSRC источника, к которому относится информация в этом блоке отчета приема;

– доля потерь: 8 bit. 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;

O'ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, PATENT
NAZORATI VA MUVOFIQLASHTIRISH
AXBOROT TEXNOLOGIYALARI
JORIY ETILGAN

– общее число потерянных пакетов: 24 bit, 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. 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: 32 bit. Младшие 16 bit содержат наибольший порядковый номер, полученный в информационном пакете RTP из источника SSRC_n, а старшие 16 bit расширяют этот порядковый номер соответствующим счетчиком циклов порядкового номера. Различные получатели в рамках одного и того же сеанса генерируют различные расширения порядкового номера, если время начала для них значительно различается;

– джиттер прибытия: 32 bit. 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 (LSR): 32 bit. Средние 32 bit из 64 bit 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 (DLSR): 32 bit. Задержка в приемнике пакетов, выраженная в единицах, равных 1/65536 s, 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.

С помощью значений временной метки последнего SR (LSR) и задержки в приемнике с момента последнего SR (DLSR) источник SSRC_n может вычислять задержку распространения пакетов на пути к получателю SSRC_r и обратно (круговую задержку). При поступлении отчета приема источник SSRC_n фиксирует время этого события T. Затем он вычисляет общее время двойного прохода T-LSR с использованием поля временной метки последнего SR (LSR) и вычитает задержку DLSR, в результате получая время распространения пакета туда и обратно (T-LSR-DLSR). Это может использоваться как приблизительная мера расстояния до кластера получателей.

O'ZSTANDART AGENTLIGA
STANDARTLASHTIRISH, DAVLAT
NAZORATINI KUCHAYTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

6.4.3 Формат пакета отчета получателя (RR)

Формат пакета RR, приведенный на рисунке 5, такой же, как и формат пакета SR, за исключением того, что поле типа пакета содержит константу, равную 201, а пять слов информации отправителя отсутствуют (временные метки NTP и RTP и счетчики пакетов и октетов отправителя). Оставшиеся поля имеют то же самое значение, что и для пакета SR.

0 byte 1 byte 2 byte 3 byte

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9

V	P	RC	PT=SR=201	длина
SSRC отправителя				
SSRC первого источника (SSRC_1)				
доля потерь		общее число потерянных пакетов		
расширенный наибольший полученный порядковый номер				
джиттер прибытия				
временная метка последнего SR (LSR)				
задержка с момента последнего SR (DLSR)				
SSRC второго источника (SSRC_2)				
...				
расширения, зависящие от профиля				

Рисунок 5 – Формат пакета RR

Когда нет никакой передачи данных или приема, о которых можно было бы сообщить, во главу составного пакета RTCP помещается пустой пакет RR (RC = 0).

6.4.4 Расширение отчетов отправителя и получателя

Если имеется дополнительная информация об отправителе или получателе, которая должна регулярно сообщаться, то профиль должен определять расширения к отчету отправителя и получателя. Использовать этот метод предпочтительнее, чем определять другой тип пакета RTCP, потому что он требует меньше избыточности:

– меньше октетов в пакете (не требуется ни заголовка RTCP, ни поля SSRC);

– более простой и быстрый анализ, потому, что приложения, выполняющиеся в соответствии с данным профилем, могут программироваться так, чтобы всегда рассматривать поля расширения в непосредственно доступном месте после отчетов приема.

Если требуется дополнительная информация отправителя, то она должна быть включена в первую очередь в расширение отчетов

отправителя, но не должна присутствовать в отчетах приема. Если должна быть включена информация о получателях, то данные могут быть структурированы, как массив блоков, параллельный существующему массиву блоков отчета приема. Число блоков должно быть обозначено полем RC.

6.4.5 Анализ отчетов отправителя и получателя

Обратная связь качества приема полезна не только для отправителя, но также для получателей и мониторов третьей стороны. Отправитель может модифицировать свои передачи на основе обратной связи. Получатели могут определять, являются ли проблемы локальными, региональными или глобальными. Диспетчеры сети могут использовать независимые от профиля мониторы, которые получают пакеты RTCP, чтобы оценить характеристику сетей для группового распределения.

В информации отправителя и в блоках отчета приема используются кумулятивные счетчики потерянных пакетов. Разность значений счетчиков в двух полученных отчетах может использоваться для оценки текущего качества передачи пакетов на протяжении коротких и длинных интервалов времени с обеспечением устойчивости к потере отчетов. Данные временной метки NTP позволяют вычислять интенсивность потерь из разницы на интервале между двумя отчетами. Так как эта временная метка не зависит от тактовой частоты кодирования данных, можно использовать независимые от кодирования и профиля мониторы.

Из информации отправителя монитор третьей стороны без получения данных может вычислять среднюю на интервале скорость передачи трафика и среднюю частоту передачи пакетов. Отношение этих двух величин дает средний размер поля данных. Если вероятность потери пакета не зависит от его размера, то число пакетов, принятых конкретным получателем, умноженное на средний размер поля данных (или соответствующий размер пакета) дает производительность этого получателя.

В дополнение к кумулятивным счетчикам, которые обеспечивают определение потерь пакетов на протяжении длительных интервалов времени на основе разницы в отчетах, поле доли потерь обеспечивает краткосрочное измерение на базе одного отчета. Это становится более важным по мере роста числа участников телеконференции, поскольку информация о состоянии приема может не обеспечиваться для всех получателей, а интервал между отчетами становится достаточно длительным.

Поле джиттера прибытия обеспечивает второй краткосрочный критерий оценки перегрузки сети. Потери пакета отслеживают устойчивую перегрузку, в то время как на основе джиттера может прослеживаться кратковременная перегрузка. Критерий джиттера может

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATI VA SERTIFIKATLASHTIRISHNI
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

указывать на перегрузку прежде, чем это приведет к потерям пакетов. Так как поле джиттера прибытия содержит только мгновенный срез джиттера в момент формирования отчета, может быть необходим анализ нескольких отчетов, поступивших от одного получателя через какое-то время или от множества получателей, например, внутри одной сети.

6.5 Пакет описания источника (SDES)

6.5.1 Формат пакета SDES

Пакет SDES состоит из заголовка и нуля или более частей, каждая из которых включает пункты, описывающие источник, идентифицированный в этой части. Формат пакета SDES представлен ниже на рисунке 6.

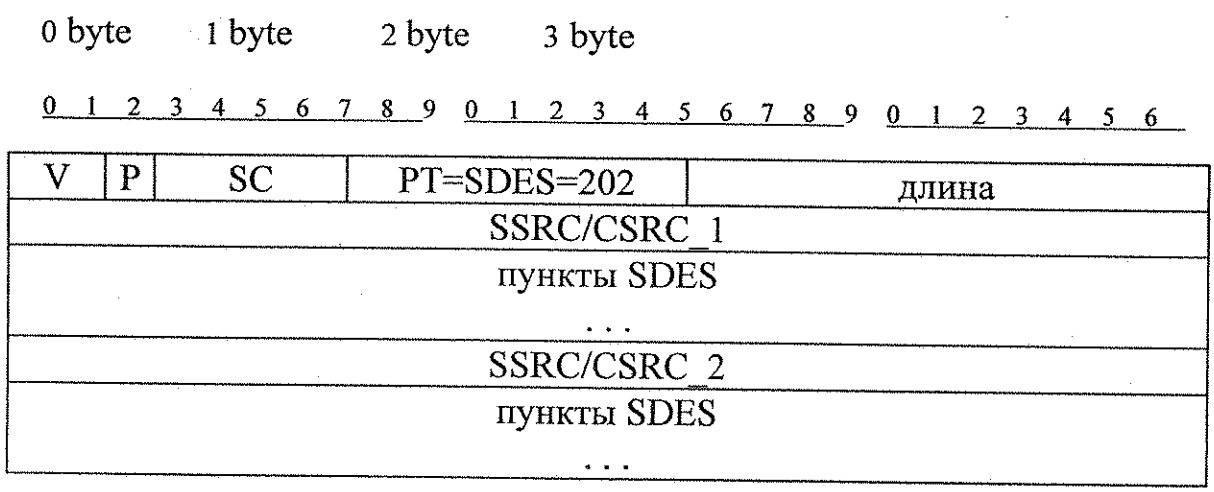


Рисунок 6 – Формат пакета SDES

Заголовок пакета включает следующие поля:

– поля версии (V), дополнения (P) и длины – такие же, как и для пакета SR;

– тип трафика (PT - packet type): 8 bit. Содержит константу 202 для идентификации пакета, как пакета SDES протокола RTCP;

– счетчик источника (SC - source count): 5 bit. Число частей SSRC/CSRC, содержащихся в пакете SDES. Нулевая величина является допустимой, но неиспользуемой;

Каждая часть RTCP-пакета SDES состоит из идентификатора SSRC/CSRC, за которым следует список из нуля или более пунктов с информацией о SSRC/CSRC. Каждая часть выровнена по 32-разрядной границе. Каждый пункт состоит из восьмиразрядного поля типа, восьмиразрядного счетчика октетов, указывающего на длину текста (не включая этот двухоктетный заголовок), и непосредственно текста. Размер текста не должен превышать 255 октетов. Это обусловливается необходимостью ограничения затрат полосы пропускания для RTCP.

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AYSCHET TEXNOLOGIYALARINI
[illegible] DARMASI

Пункты передаются непрерывно, то есть они индивидуально не дополняются до 32-разрядной границы. Текст не должен заканчиваться нулем. Список пунктов в каждой части заканчивается одним или более нулевых октетов, первый из которых интерпретируется как нулевой тип пункта для обозначения конца списка, а остальные необходимы для дополнения до 32-разрядной границы. Часть с нулевыми пунктами (четыре нулевых октета) допустима, но не используема.

Оконечные системы посылают один пакет SDES, содержащий их собственный идентификатор источника (такой же, как идентификатор SSRC в фиксированном заголовке протокола RTP). Микшер посылает один пакет SDES, содержащий часть для каждого включаемого источника, от которого он получает информацию SDES, или множество полных пакетов SDES в формате, приведенном выше, если имеются более чем 31 такой источник.

6.5.2 Пункт канонического имени (CNAME)

Формат пункта CNAME должен иметь вид, приведенный на рисунке 7.

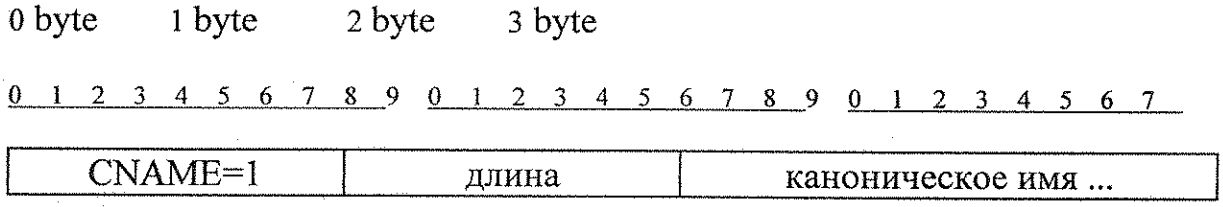


Рисунок 7 – Формат пункта CNAME

Идентификатор CNAME имеет следующие свойства:

– 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 сведения 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.

Когда это возможно, CNAME следует получать алгоритмически, а не вводить вручную. Пункт CNAME должен иметь следующий формат (если только профиль не определяет альтернативный синтаксис или семантику): «пользователь@хост» или «хост» (если имя пользователя отсутствует, как для систем с единственным пользователем). Для обоих форматов «хост» -

ELEKTRON RAQAMLI STANDARTLASHTIRISH, DAVLAT NAZORAT VA MUVOFIQLASHTIRISH VA AXBOROT TEXNOLOGIYALARINI JORIY ETISH BOSHQARMASI

это полное доменное имя хоста, являющегося источником данных реального времени или стандартное представление в коде ASCII числового адреса хоста.

Примеры идентификатора CNAME для многопользовательской системы: «idoe@sleepy.megacorp.com» или «doe@192.0.2.89». Примеры для системы без имени пользователя: «sleepy.megacorp.com» или «192.0.2.89». Имя пользователя должно быть именем входа в систему, а не персональным именем человека. Имя хоста не обязательно должно быть идентично имени в адресе электронной почты участника.

Этот синтаксис не обеспечивает уникальность идентификаторов для каждого источника, если приложение разрешает пользователю генерировать множество источников в пределах одного хоста. Такое приложение для дальнейшей идентификации источника должно полагаться на SSRC или на профиль, для которого приложение должно определить дополнительный синтаксис идентификатора CNAME.

Если каждое приложение создает свое CNAME независимо, то эти имена могут не быть идентичными, как требуется для обеспечения взаимодействия множества мультимедийных программных средств, принадлежащих одному участнику во множестве взаимосвязанных сеансов RTP. При этом для назначения единого имени CNAME могут потребоваться некоторые внешние средства координации.

Конкретные назначения сетевых адресов могут создавать сетевые адреса, не являющиеся глобально уникальными. Это приводит к не уникальности CNAMES, если хосты с частными адресами и без прямой IP-связи с сетью Интернет направляют пакеты RTP в Интернет через транслятор RTP-уровня. Чтобы отрабатывать этот случай, приложения могут обеспечивать средства конфигурации уникального CNAME.

6.5.3 Пункт имени пользователя (NAME)

Пункт 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. Формат пункта NAME представлен на рисунке 8.

O'ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORAT VA AXBOROTLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

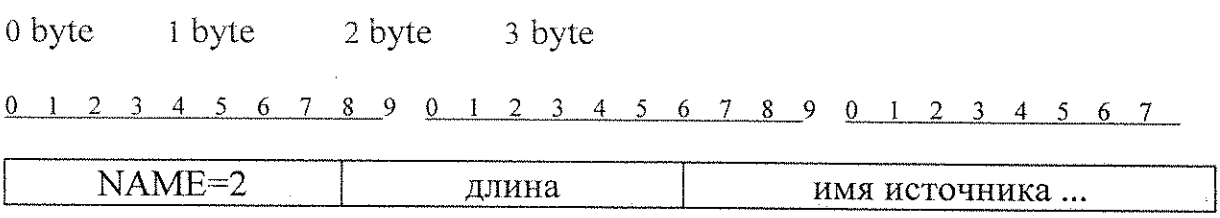


Рисунок 8 – Формат пункта NAME

6.5.4 Пункт адреса пользователя EMAIL

EMAIL должен иметь следующий вид: «John.Doe@megacorp.com». Величина пункта EMAIL в течение сеанса связи остается постоянной. Формат пункта EMAIL приведен ниже на рисунке 9.

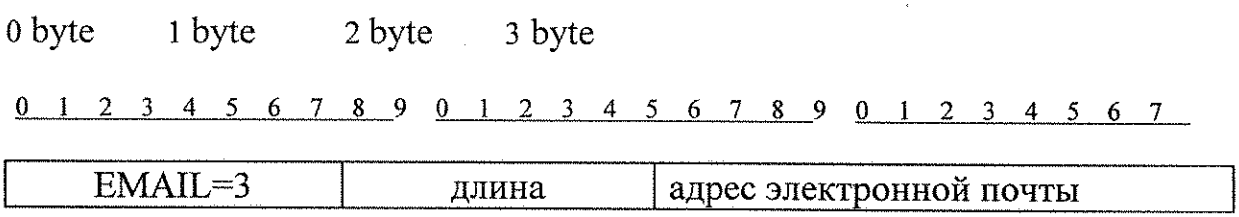


Рисунок 9 - Формат пункта EMAIL

6.5.5 Пункт пользователя телефонного номера (PHONE)

Номер телефона должен формироваться со знаком «плюс», заменяющим код международного префикса. Например, «+998 71 2551212» для номера в Узбекистане. Формат пункта PHONE показан на рисунке 10.

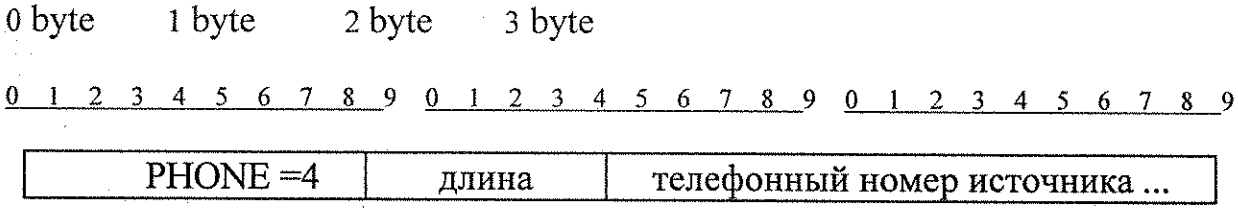


Рисунок 10 - Формат пункта PHONE

6.5.6 Пункт географического местоположения пользователя (LOC)

В зависимости от приложения пункту LOC 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&T BL MH». Степень детализации оставлена приложению или пользователю, но формат и содержание могут предписываться в

STANDARTLASHTIRISH, DAVLAT
NAZORATI VA SERTIFIKATLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

соответствии с профилем. Значение пункта LOC для всех хостов, кроме мобильных, остается постоянным на протяжении всего сеанса связи.

Формат пункта LOC представлен на рисунке 11.

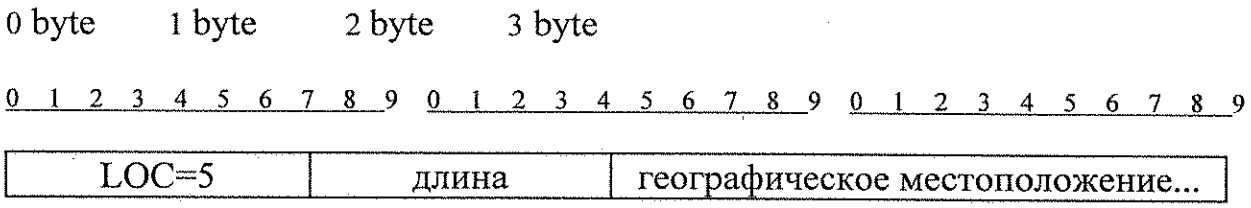


Рисунок 11 – Формат пункта LOC

6.5.7 Пункт имени приложения или средства (TOOL)

Пункт TOOL пакета SDES включает строку, содержащую имя и 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. Формат пункта TOOL приведен ниже на рисунке 12.

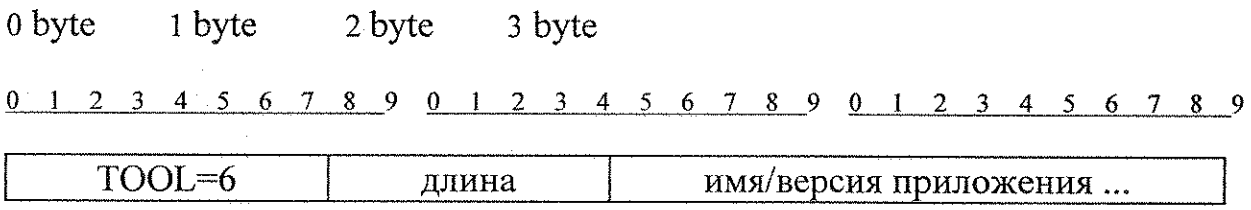
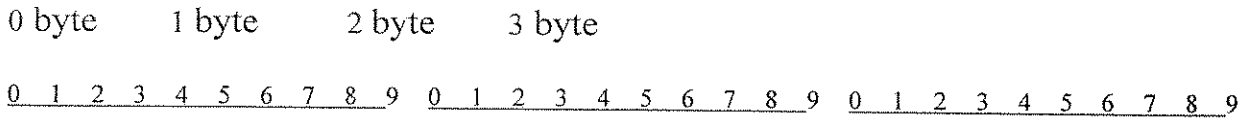


Рисунок 12 – Формат пункта TOOL

6.5.8 Пункт заметок/статуса (NOTE)

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. На рисунке 13 представлен формат пункта NOTE.

MAXSUS TEXNIK OSTIVALIGI



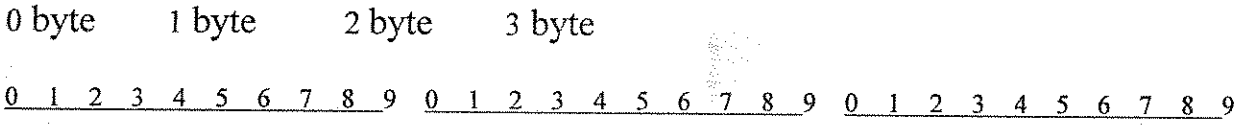
NOTE =7	длина	заметки об источнике . . .

Рисунок 13 – Формат пункта NOTE

Так как пункт NOTE может быть важен для показа, то в случае необходимости интенсивность, с который передаются другие (не CNAME) пункты (такие как NAME), может быть снижена так, чтобы пункт NOTE мог использовать соответствующую часть полосы пропускания RTCP. Когда кратковременное сообщение становится неактивным, пункт NOTE должен передаваться несколько раз с той же самой скоростью повторения, но со строкой нулевой длины, чтобы информировать получателей. Если пункт NOTE не был получен в течение некоторого количества интервалов повторения или, возможно, 20-30 интервалов RTCP, то получатели должны считать его неактивным.

6.5.9 Пункт частных расширений (PRIV)

Этот пункт используется для определяемых приложением расширений SDES. Формат пункта PRIV приведен ниже на рисунке 14.



PRIV =8	длина	длина префикса	строка префикса...
. . .	строка величин . . .		

Рисунок 14 – Формат пункта PRIV

Пункт содержит префикс, состоящий из пары: поле длины и поле строки, за которым следует строка величин, заполняющая остаток пункта и содержащая интересующую информацию. Размер поля длины префикса - 8 bit. 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. В качестве альтернативы рекомендуется задавать строку префикса так, чтобы она отражала сущность приложения и величин пункта PRIV.

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, METROLOGIYA
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

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.

6.6 Пакет завершения связи (BYE)

Пакет BYE указывает, что один или более источников становятся не активными. BYE имеет формат, представленный на рисунке 15.

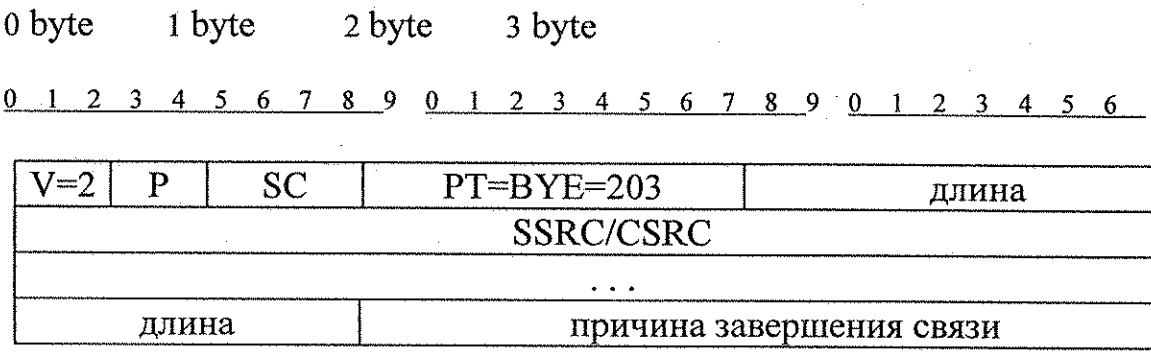


Рисунок 15 – Формат пакета BYE

В составе пакета имеются следующие поля:

– поля версии (V), дополнения (P) и длины – такие же, как и для пакета SR;

– тип пакета (PT): 8 bit. Содержит константу 203 для распознавания этого пакета, как пакета BYE протокола RTCP;

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

Если пакет BYE получен микшером, то он передает пакет BYE с неизменным идентификатором (идентификаторами) SSRC/CSRC. Если микшер выключается, он посылает пакет BYE, содержащий все включаемые источники, с которыми он работает, а также свой собственный идентификатор SSRC. Пакет BYE может также включать (необязательно) восьмиразрядный 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.

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, AKKREDITATSIYALASHTIRISH VA
METROLOGIYA TEXNOLOGIYALARI
JORIY ETISH BOSHQARMASI

6.7 Пакет, определяемый приложением (APP)

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. После испытания, если оправдано более широкое использование, рекомендуется, чтобы каждый пакет APP был переопределен без полей подтипа и имени и зарегистрирован в IANA с выделением для него нового типа пакета RTCP. Формат пакета APP приведен на рисунке 16.

0 byte 1 byte 2 byte 3 byte

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9

V=2	P	подтип	PT=APP=204	длина
SSRC/CSRC				
имя (ASCII)				
данные, определяемые приложением				

Рисунок 16 – Формат пакета APP

Пакет APP включает следующие поля:

– поля версии (V), дополнения (P) и длины соответствуют описаниям данных полей для пакета SR;

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

– тип пакета (PT): 8 bit. Содержит константу 204 для распознавания данного пакета, как пакета APP протокола RTCP;

– 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 bit.

O‘ZSTANDART AGENTLIGA
STANDARTLASHTIRISH DAVLAT
NAZORAT M. MOSLIGI LASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

7 Трансляторы и микшеры

7.1 Общее описание транслятора и микшера

В дополнение к оконечным системам протокол RTP поддерживает такие понятия как трансляторы и микшеры, которые могут рассматриваться, как промежуточные системы уровня RTP.

Транслятор/микшер RTP соединяет два или более сегментов сети (сайтов) на транспортном уровне. Обычно, при этом каждый сайт определяется единым протоколом сетевого и транспортного уровня (например, IP/UDP), групповым адресом или парой индивидуальных адресов и портом назначения транспортного уровня (трансляторы протоколов сетевого уровня типа IP версии 4 в IP версии 6, могут присутствовать в сегменте сети незаметно для RTP). Одна система может служить в качестве транслятора или микшера для различных сеансов RTP, но при этом транслятор и микшер рассматриваются, как логически отдельные сущности.

Чтобы избежать зацикливания при использовании транслятора или микшера, должны соблюдаться следующие правила:

– каждый из сегментов, соединенных транслятором и микшером, участвующий в одном сеансе RTP, должен отличаться от всех других, по крайней мере, одним из параметров (протокол, адрес, порт) или должен быть изолирован от других сегментов на сетевом уровне;

– не должно быть множества трансляторов или микшеров, соединенных параллельно, если в соответствии с некоторой структурой они не разделяют между собой множество источников.

Все оконечные системы RTP, которые могут передавать мультимедийные данные через один или более трансляторов или микшеров RTP, совместно используют одно и то же пространство SSRC, то есть идентификаторы SSRC должны быть уникальными среди всех этих оконечных систем.

Может иметься большое многообразие трансляторов и микшеров, разработанных для различных целей и приложений. Некоторые типы данных систем должны шифровать/дешифровать данные, изменять тип кодирования данных или нижележащие протоколы или передавать данные между групповым адресом и одним или более индивидуальных адресов. Принципиальное различие между трансляторами и микшерами состоит в том, что транслятор передает потоки данных от различных источников отдельно, в то время как микшер объединяет их, формируя один новый поток.

Транслятор передает пакеты RTP с неизмененными идентификаторами SSRC. Это дает получателям возможность распознавать отдельные источники, даже если пакеты от всех источников прошли через один и тот же транслятор и содержат в качестве источника

STANDARTLASHTIRISH, METRAT
MILLIY AGENTLIGI
AXBOROT TEXNOLOGIYALARINI

сетевой адрес транслятора. Некоторые виды трансляторов передают данные без изменений, а другие могут изменять тип кодирования данных и, таким образом, тип трафика RTP, а также временную метку. Если множество информационных пакетов преобразуется в один или, наоборот, один - во множество, то транслятор должен назначить исходящим пакетам новые порядковые номера. Потери во входящем потоке пакетов могут вызывать появление соответствующих промежутков в исходящих порядковых номерах. Получатели не смогут обнаружить присутствие транслятора, если каким-либо другим образом, не узнают какой тип трафика или транспортный адрес используется первоисточником данных.

Микшер получает потоки информационных пакетов RTP из одного или более источников, возможно, изменяет формат данных, объединяет потоки и затем передает комбинированный поток. Так как время формирования пакетов для множества различных источников в общем случае не синхронизировано, то микшер будет выполнять корректировку синхронизации потоков и генерировать собственную синхронизацию для комбинированного потока, являясь источником синхронизации. Следовательно, все информационные пакеты, посланные микшером, будут содержать в поле источника синхронизации идентификатор SSRC микшера. Чтобы сохранять идентичность первоначальных источников, участвующих в формировании комбинированного пакета, микшер должен вставить их идентификаторы источников синхронизации SSRC в список идентификаторов включаемых источников CSRC, следующий за фиксированным заголовком пакета RTP. Микшер, который также сам по себе является включаемым источником для некоторого пакета, должен явно включить свой собственный идентификатор SSRC в список CSRC для этого пакета.

Для некоторых приложений микшер может не опознавать источники в списке CSRC. Это может привести к тому, что зацикливания этих источников не смогут быть обнаружены.

Для звуковых приложений микшер имеет преимущество перед транслятором, состоящее в том, что выходная полоса пропускания микшера ограничивается полосой пропускания одного источника даже в том случае, когда на входной стороне активными являются несколько источников. Это может быть важно для узкополосных линий связи. Недостатком использования микшера является то, что получатели на выходной стороне не имеют данных о том, сообщения каких источников передаются или приглушаются, если для дистанционного управления микшером не предусмотрен некоторый механизм контроля.

Пример RTP-сети с оконечными системами, микшерами и трансляторами представлен на рисунке 17.

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATI VA MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

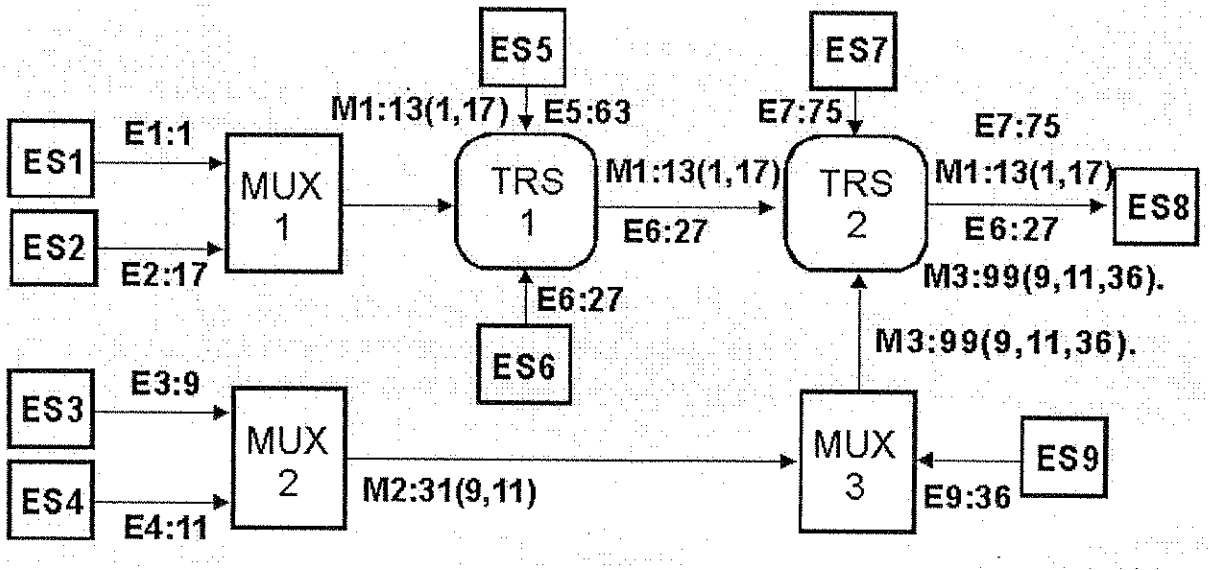


Рисунок 17 – Пример RTP-сети с оконечными системами, микшерами и трансляторами

Здесь показано их влияние на SSRC и CSRC-идентификаторы. Оконечные системы обозначены символами ES. Трансляторы обозначены буквами TRS (на рисунке овалы) и микшеры обозначены как MUX (прямоугольники). Запись «M1:13(1,17)» обозначает пакет отправленный микшером MUX1, который идентифицируется случайным значением SSRC 13 и двумя CSRC-идентификаторами 1 и 17, скопированными с SSRC-идентификаторов пакетов оконечных систем ES1 и ES2.

7.2 Передача пакетов протокола RTCP трансляторами

В дополнение к передаче информационных пакетов (возможно, при модификации) трансляторы и микшеры должны также обрабатывать пакеты RTCP. Во многих случаях, они демонтируют составные пакеты RTCP, полученные от оконечных систем, объединяют информацию SDES и модифицируют пакеты SR или RR.

Транслятор, не модифицирующий информационные пакеты (например, тот, который только передает мультимедийные данные между групповым и индивидуальным адресом), может передавать пакеты RTCP, также их не модифицируя. Транслятор, который некоторым способом преобразует трафик, должен делать соответствующие преобразования в информации пакетов SR и RR так, чтобы она корректно отражала характеристики данных и качество приема. В общем случае, транслятор не должен объединять пакеты SR и RR из различных источников в один пакет, так как это уменьшило бы точность определения задержки распространения на основе полей заголовков LSR и DLSR.

Информация отправителя пакета SR. Транслятор не генерирует свою собственную информацию отправителя, но передает пакеты SR,

O'ZSTANDART AGENTLIGI
STANDARTLASHTIRISH BO'YICHA
NAZORAT BO'LINMASINING
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

полученные от одного сегмента, другим. Идентификатор SSRC при этом не изменяется, но информация отправителя должна быть изменена, если это требуется трансляцией. Если транслятор изменяет тип кодирования данных, то одновременно должно изменяться поле счетчика байтов отправителя. Если транслятор также объединяет отдельные пакеты данных в один выходной пакет, то он должен изменить поле счетчика пакетов отправителя. Если он изменяет период формирования временной метки, он должен изменить поле временной метки RTP в пакете SR.

Блоки отчетов приема пакетов SR/RR. Транслятор передает отчеты приема, полученные от одного сегмента. Заметим, что этот поток имеет направление, противоположное направлению передачи данных. SSRC остается неизменным. Если транслятор объединяет отдельные информационные пакеты в один выходной пакет и, следовательно, изменяет порядковые номера, то он должен делать соответствующее преобразование для поля потерь пакетов и поля расширенного последнего порядкового номера. Это может быть сложным. В крайнем случае, может вообще не быть никакого действенного способа транслировать отчеты приема. Тогда транслятор может не передавать никаких отчетов о приеме вообще или синтезировать свой отчет, основанный на собственном приеме. Общее правило - необходимо делать то, что имеет смысл в конкретной ситуации.

SDES. Трансляторы обычно передают без изменения информацию SDES от одного сегмента другим, но могут, например, если полоса пропускания ограничена, фильтровать информацию SDES не-CNAME. Канонические имена CNAME должны передаваться для обнаружения коллизий идентификатора SSRC. Транслятор, который генерирует свои собственные пакеты RR, должен посылать информацию SDES CNAME о себе тем же сегментам, которым он посылает пакеты RR.

BYE. Трансляторы передают пакеты BYE неизмененными. Если трансляторы собираются прекращать передачу пакетов, то они должны генерировать пакеты BYE со своими собственными идентификаторами SSRC.

APP. Трансляторы передают пакеты APP без изменения.

7.3 Передача пакетов протокола RTCP микшерами

Поскольку микшер генерирует новый собственный поток данных, он не транслирует пакеты SR или RR, а вместо этого генерирует новую информацию для обеих сторон.

Информация отправителя пакета SR. Микшер не передает информацию отправителя из источников, с которыми он работает, потому, что характеристики исходных потоков теряются при смешивании. Как источник синхронизации, микшер генерирует свои собственные пакеты

AXBOROT TEXNOLOGIYALARI AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATI VA MUVOFIQLASHTIRISH
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

SR с информацией отправителя относительно смешанного потока данных и посылает их в том же самом направлении, что и смешанный поток.

Блоки отчетов о приеме пакетов SR/RR. Микшер генерирует свои собственные отчеты приема для источников в каждом сегменте и посылает их наружу только в те же самые сегменты. Он не посылает этих отчетов приема другим сегментам и не передает отчеты о приеме из одного сегмента в другие, потому что эти источники не являются источниками синхронизации SSRC (являются только включаемыми источниками CSRC).

SDES. Микшеры обычно передают без изменения информацию SDES от одного сегмента другим, но могут, например, если полоса пропускания ограничена, фильтровать информацию SDES не-CNAME. CNAME должны передаваться, чтобы обеспечить обнаружение коллизий идентификатором SSRC (идентификатор в списке CSRC, сгенерированным микшером, может конфликтовать с идентификатором SSRC, сгенерированным оконечной системой). Микшер должен послать информацию SDES CNAME о себе тем сегментам, которым он посылает пакеты SR или RR.

Так как микшеры не передают пакеты SR или RR, то они обычно извлекают пакеты SDES из составного пакета RTCP. Чтобы минимизировать избыточность, части пакетов SDES могут объединяться в один пакет SDES, который затем помещается в пакет SR или RR, генерируемый микшером. Интенсивность генерации пакетов RTCP на разных сторонах микшера может быть различной.

Микшер, который не вставляет идентификаторы CSRC, может также воздержаться от пересылки CNAME SDES. В этом случае, пространства идентификатора SSRC в двух сегментах являются независимыми. Этот режим работы создает опасность того, что зацикливания не смогут быть обнаружены.

BYE. Микшеры должны передавать пакеты BYE. Если микшеры собираются прекратить пересылку пакетов, то они должны генерировать пакеты BYE с их собственными идентификаторами SSRC.

APP. Передача микшерами пакетов APP определяется приложением.

7.4 Последовательное включение микшеров

В сеансе RTP могут быть задействованы несколько микшеров и трансляторов, как это показано на рисунке 17. Если два микшера включены последовательно, так как MUX2 и MUX3 – пакеты, полученные микшером могут быть уже объединены и включать CSRC-список со многими идентификаторами. Микшер (MUX3) должен формировать CSRC-список для исходящих пакетов, используя CSRC-идентификаторы уже смешанных входных пакетов (выход MUX2) и SSRC-идентификаторы

O‘ZSTANDART MILLIY STANDARTLASHTIRISH, DAVLAT NAZORAT VA AXBOROT TEXNOLOGIYALARINI JORIY ETISH DEPARTAMENTI

несмешанных входных пакетов, поступивших от ES9 (E:36). Это отмечено на рисунке для выходных пакетов микшера MUX3 как M3:99(9,11,36). Если число идентификаторов в списке CSRC превышает 15, остальные не могут быть туда включены.

8 Назначение и использование SSRC-идентификатора

8.1 Идентификатор SSRC

Идентификатор SSRC, содержащийся в заголовке RTP и в различных полях пакетов RTCP, - это произвольное 32-битовое число, которое должно быть глобально уникальным в пределах сеанса RTP. Необходимо выбирать этот идентификатор так, чтобы участники в одной и той же сети или начавшие работу в одно и то же время с малой вероятностью выбрали одно и то же число.

Использовать в качестве идентификатора локальный сетевой адрес (такой, как адрес IPv4) не следует. Такой адрес может не быть уникальным, так как трансляторы и микшеры RTP позволяют взаимодействовать множеству сетей с различными адресными пространствами. Множество источников данных, выполняющихся на одном и том же хосте, также могут конфликтовать.

8.2 Разрешение коллизий и обнаружение зацикливаний

Хотя вероятность коллизии идентификаторов SSRC низка, все реализации RTP должны быть готовы обнаруживать коллизии и выполнять соответствующие действия, чтобы разрешать их. Если источник обнаруживает, что другой источник использует такой же идентификатор SSRC, то он должен послать пакет BYE протокола RTCP со старым идентификатором и выбирать произвольный новый. Если получатель обнаруживает, что два других источника конфликтуют, он может принимать пакеты от одного и отбрасывать пакеты другого, когда это может быть обнаружено по различию транспортных адресов источников или CNAME. Два источника должны исчерпать конфликт так, чтобы такое состояние не продолжалось.

Так как произвольные идентификаторы должны быть глобально уникальными для каждого сеанса RTP, то они могут использоваться для обнаружения зацикливаний, появляющихся при использовании микшеров или трансляторов. Зацикливание вызывает дублирование данных и информации управления.

Транслятор может ошибочно передавать пакет той же многопользовательской группе, от которой он получил пакет, или непосредственно, или через цепь трансляторов. В этом случае один и тот

O‘ZSTANDART AGENTLIGA
STANDARTLASHTIRISH, DAVLAT
NAZORATI VA MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

же пакет появляется несколько раз, возникая из различных источников сети.

Два транслятора, неправильно установленные параллельно (с одними и теми же многопользовательскими группами с обеих сторон), передают пакеты от одной многопользовательской группы другой. Однонаправленные трансляторы производят две копии; двунаправленные трансляторы создают зацикливание.

Микшер может замыкать петлю зацикливания, посылая пакеты тому же самому транспортному адресу, от которого он их получает, или непосредственно, или через другой микшер (транслятор). В этом случае источник может идентифицироваться и как SSRC в пакете данных, и как CSRC в смешанном пакете данных.

Источник может обнаружить, что зациклены его собственные пакеты, или пакеты из другого источника (зацикливание третьей стороны).

Зацикливания и коллизии при случайном выборе идентификатора источника приводят к тому, что пакеты прибывают с одним и тем же идентификатором SSRC, но различными транспортными адресами источника, которые могут быть адресами оконечной системы, сформировавшей пакет, или промежуточной системы. Следовательно, если источник изменяет транспортный адрес источника, он должен также выбрать новый идентификатор SSRC, чтобы его не интерпретировали, как зацикленный источник. Зацикливания или коллизии, имеющиеся на удаленной стороне транслятора или микшера, не могут быть обнаружены с помощью транспортного адреса источника, если все копии пакетов проходят через транслятор или микшер, однако коллизии все еще могут обнаруживаться, когда части от двух пакетов SDES протокола RTCP содержат один и тот же идентификатор SSRC, но различные CNAME.

Чтобы обнаружить и разрешить эти конфликты, реализация RTP должна включать специальный алгоритм. Такой алгоритм состоит в разрешении коллизии на основе использования собственного идентификатора SSRC участника, посылке пакета BYE протокола RTCP для старого идентификатора и выборе нового. Алгоритм может использоваться, когда транспортный адрес источника является общим для пакетов RTP и RTCP этого источника. Для поддержки приложений, которые не удовлетворяют этому ограничению, алгоритм нужно изменить.

Алгоритм требует ведения таблицы соответствия идентификатора источника и транспортного адреса источника, от которого идентификатор был (вначале) получен. Каждый идентификатор SSRC или CSRC, полученный в информационном или управляющем пакете, разыскивается в этой таблице для обработки содержащихся в пакете данных или управляющей информации. Для управляющих пакетов каждый элемент с собственным идентификатором SSRC (например, часть пакета SDES) требует отдельного поиска (исключением является SSRC в блоке отчета

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

приема). Если SSRC или CSRC не найден, то создается новая запись таблицы. Записи таблицы уничтожаются, если поступает пакет BYE протокола RTCP с соответствующим SSRC или если в течение длительного интервала времени никакие пакеты не поступали.

Чтобы отследить зацикливания собственных информационных пакетов участника, также необходимо хранить отдельный список транспортных адресов (не идентификаторов) конфликтующих источников. Этот список должен быть коротким. Обычно он является пустым. Каждый элемент в этом списке содержит транспортный адрес источника и время получения последнего конфликтующего пакета. Элемент может удаляться из списка, когда из данного источника в течение порядка десяти интервалов отчетности RTCP не поступило никаких конфликтующих пакетов.

Когда из-за коллизии выбирается новый идентификатор SSRC, то его предполагаемое значение сначала разыскивается в исходной таблице идентификаторов, чтобы видеть, не находится ли оно уже в использовании некоторым другим источником. Если это так, то генерируется другое значение, и процесс повторяется.

Зацикливание пакетов данных с групповым адресом может вызывать лавинообразный рост числа пакетов в сети. Требуется, чтобы все микшеры и трансляторы выполняли обнаружение и разрушение зацикливаний. Это должно ограничить излишний рост трафика не более, чем одной двойной копией, пока причина зацикливания не будет найдена. В чрезвычайных ситуациях, когда микшер или транслятор не разрушает зацикливание, что приводит к значительному росту трафика, для оконечных систем может быть необходимо полное прекращение передачи информационных или управляющих пакетов. Это решение может зависеть от приложения. Состояние ошибки при этом должно быть соответствующим образом обозначено. Вновь передача может быть предпринята после длительного (со случайным значением длительности) интервала времени (порядка нескольких минут).

9 Обеспечение безопасности

9.1 Конфиденциальность

Услуги обеспечения безопасности связи, которые требуются приложениям RTP, включая аутентификацию, целостность и конфиденциальность, могут обеспечиваться протоколами нижележащих уровней. Так как протокол RTP может использоваться с различными протоколами нижележащих уровней, в том числе и не предоставляющими подобного рода услуг, а потребность в конфиденциальности связи присутствует в звуковых и видеоприложениях, то в протоколе RTP

O'ZSTANDART AGENTLIGA
STANDARTLASHTIRISH, DAVLAT
NAZORATINI AMALGA OSHIRISHNI
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

предусмотрена услуга обеспечения конфиденциальности, когда услуги нижележащего уровня недоступны. Избыточность протокола для обеспечения этой услуги низка.

Обеспечение конфиденциальности означает, что декодировать данные из полученного пакета может только адресат. Для других пакет не содержит никакой полезной информации. Конфиденциальность обеспечивается шифрованием.

Когда требуется шифрование пакетов RTP или RTCP, все октеты, которые инкапсулируются для передачи в одном пакете протокола нижележащего уровня, шифруются как единый блок. До шифрования пакетов протокола RTCP перед блоком размещается 32-битовое случайное число, чтобы препятствовать вскрытию шифра по известному началу текста. Для протокола RTP префикс не требуется, потому что поля порядкового номера и временной метки инициализируются с произвольными значениями.

Для протокола RTCP позволено декомпозировать составной пакет RTCP на два пакета нижележащего уровня, один из которых шифруется, а другой передается в открытом виде. Например, информация SDES может шифроваться, в то время как отчеты о приеме - передаваться в открытом виде для обеспечения мониторинга третьей стороной, которая не владеет ключом шифрования.

Присутствие шифрования и использование корректного ключа подтверждается получателем через заголовок или результаты проверки корректности передаваемых данных.

Заданный по умолчанию алгоритм шифрования - это DES в режиме цепочки шифруемых блоков CBC. Вектор инициализации является нулевым, потому что случайное начало блока данных обеспечивается заголовком пакета RTP или произвольным префиксом для составных пакетов RTCP. Реализации, которые поддерживают шифрование, должны всегда по умолчанию поддерживать алгоритм DES в режиме CBC, чтобы максимизировать способность к взаимодействию. Другие алгоритмы шифрования могут определяться динамически средствами не-RTP для конкретного сеанса связи.

Как альтернатива шифрованию на уровне RTP профили могут определять дополнительные типы трафика для шифрованных данных. Этот метод позволяет шифровать только передаваемые данные, а заголовки оставлять открытыми для приложений там, где это желательно.

O'ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, BANDLIK
BAZORAT VA AXBOROT
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

9.2 Аутентификация и обеспечение целостности сообщения

Аутентификация и целостность сообщения не определены, так как эти услуги непосредственно не возможны без инфраструктуры управления ключом. Предполагается, что услуги аутентификации и обеспечения целостности будут обеспечиваться протоколами нижележащих уровней.

9.3 Безопасный транспортный протокол реального времени (SRTP)

SRTP определяет профиль RTP и предназначен для шифрования, установления подлинности сообщения, целостности, защиту от замены данных RTP в однонаправленных и широковещательных передачах медиа и приложения. SRTP служит основой для шифрования и идентификации сообщении RTP и потоков RTCP. SRTP может достигать высокой пропускной способности и низкого расширения пакета, а также оказывает подходящую защиту для разнородной окружающей среды (сочетание проводных и беспроводных сетей).

9.4 Цели и особенности SRTP

Цели безопасности для SRTP состоят в том, чтобы гарантировать:

a) конфиденциальность RTP и полезной нагрузки RTCP;

b) целостность всего RTP и пакетов RTCP, вместе с защитой от воспроизводимых пакетов.

Эти службы безопасности дополнительные и независимые друг от друга, за исключением того, что защита целостности SRTCP обязательна (злонамеренное или ошибочное изменение сообщений RTCP может разрушить обработку потока RTP).

Другие функциональные цели для протокола:

– структура, которая позволяет модернизировать с новыми криптографическими преобразованиями;

– низкая стоимость пропускной способности;

– низкие вычислительные затраты;

– небольшие размеры (т.е., небольшой размер кода и памяти данных);

– ограниченное расширение пакета для экономии полосы пропускания;

– высокая устойчивость к потере пакетов.

Ниже перечисленные свойства - гарантируют, что SRTP - подходящая схема защиты RTP/RTCP и в как проводных, так и в беспроводных сетях передачи данных.

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI KUCHAYTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

Так как RTP тесно связан с RTCP, в протоколе SRTP также есть родственный протокол, названный Secure RTCP (или SRTCP). SRTCP обеспечивает те же самые функции, связанные с безопасностью в RTCP, для той же функциональности SRTP в RTP.

Использование SRTP или SRTCP является необязательным при использовании RTP или RTCP, но даже если SRTP/SRTCP используются, все дополнительные возможности (такие как шифрование и установление подлинности) опциональны и могут быть включены или выключены. Единственное исключение – функция аутентификации сообщений, которая обязательна при использовании SRTCP.

Для шифрования медиа потока (в целях конфиденциальности голосового соединения), SRTP (вместе с SRTCP) стандартизирует использование только единственного шифра AES, который может использоваться в двух режимах, превращающих изначально блочный шифр AES в потоковый шифр:

– сегментированный целочисленный счётчик - типичный режим, который осуществляет произвольный доступ к любым блокам, что является существенным для трафика RTP, передающегося в публичных сетях с непредсказуемым уровнем надежности и возможной потерей пакетов. В общем случае почти любая функция может использоваться в роли «счётчика», предполагая, что эта функция не повторяется для большого числа итераций. Но стандарт для шифрования данных RTP - только обычное целочисленное значение счётчика. AES, работающий в этом режиме, является алгоритмом шифрования по умолчанию, с длиной шифровального ключа по умолчанию в 128 bit и ключом сессии длиной в 112 bit;

– f8-режим - вариант режима способа обратной связи, расширенного, чтобы быть доступным с изменённой функцией инициализации. Значения по умолчанию для шифровального ключа и ключа сессии - то же, что и в AES в режиме, описано выше. (AES, работающий в этом режиме, был выбран для использования в мобильных сетях 3G UMTS).

Помимо шифра AES, SRTP позволяет прямое шифрование, используя так называемый «пустой шифр», который может быть принят как второй поддерживаемый шифр (или третий режим шифрования в дополнение к описанным двум выше). Фактически, пустой шифр не выполняет шифрования (то есть функции алгоритма шифрования, как если бы ключевой поток содержал только нули, и копирует входной поток в выходной без изменений). Это обязательно для этого способа шифрования, который должен быть обеспечен в любой SRTP-совместимой системе. Также это может использоваться, когда конфиденциальность, которую гарантирует SRTP, не требуется, однако другие возможности SRTP - аутентификация и целостность сообщения - могут использоваться.

O ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, QAYDLAT
NAZORAT
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

10 Перечень констант протокола

Константы типа трафика RTP (PT) определяются в профилях. Однако, октет заголовка RTP, который содержит бит(ы) маркера и поле типа трафика, не должен содержать зарезервированные величины 200 и 201 (десятичный вид), чтобы пакеты RTP отличались от пакетов RTCP SR и RR. Для стандартного формата с одним битом маркера и семибитовым полем типа трафика, это ограничение означает, что типы трафика 72 и 73 использоваться не должны.

Типы пакетов RTCP представлены в таблице 1. Значения типов пакетов RTCP выбраны в диапазоне от 200 до 204 для лучшего контроля корректности заголовка пакетов RTCP при сравнении с пакетами RTP. Когда поле типа пакета RTCP сравнивается с соответствующим октетом заголовка RTP, этот диапазон соответствует биту маркера, равному единице (чего обычно не бывает в информационных пакетах) и старшему разряду поля стандартного типа трафика, равному единице (в то время как статически заданные типы трафика обычно имеют значения PT с нулем в старшем разряде). Этот диапазон был также выбран для большего дистанцирования от значений 0 и 255, так как поля, целиком состоящие из нулей или единиц, в основном характерны для данных.

Таблица 1 – Типы пакетов RTCP

Обозначение	Наименование	Величина
SR	отчет отправителя	200
RR	отчет получателя	201
SDES	описание источника	202
BYE	завершение связи	203
APP	пакет, определяемый приложением	204

Другие типы пакетов RTCP определяются Сообществом IANA. Разработчики имеют возможность регистрировать значения, которые им требуются для проведения экспериментальных исследований, а затем аннулировать регистрацию по мере исчезновения потребности в этих значениях.

Допустимые типы пунктов пакета SDES приведены в таблице 2.

O‘ZSTANDART AGENTLIGA
STANDARTLASHTIRISH, DAVLAT
NAZORAT VA MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

Таблица 2 – Типы пунктов пакета SDES

Обозначение	Наименование	Величина
END	конец списка SDES	0
CNAME	каноническое имя	1
NAME	имя пользователя	2
EMAIL	адрес электронной почты пользователя	3
PHONE	телефонный номер пользователя	4
LOC	географическое местоположение пользователя	5
TOOL	имя приложения или средства	6
NOTE	заметки об источнике	7
PRIV	частные расширения	8

11 Описание профиля и формата трафика

Для полного описания RTP для конкретного приложения требуются дополнительные документы двух типов: описание профиля и формата трафика.

RTP может использоваться для многих классов приложений со значительно различающимися требованиями. Гибкость адаптации к этим требованиям обеспечивается использованием различных профилей. Обычно приложение использует только один профиль и нет никакой явной индикации того, какой профиль находится в данный момент в использовании.

Дополнительный документ второго типа - спецификация формата трафика определяет, как конкретный вид трафика должен передаваться в соответствии с RTP. Один и тот же формат трафика может использоваться для множества профилей и может быть определен независимо от профиля. Документы профиля отвечают лишь за соответствие этого формата и значения PT.

В описании профиля могут определяться следующие пункты.

Заголовок пакета данных RTP. Октет в заголовке пакета данных RTP, который содержит бит маркера и поле типа трафика, может быть переопределен в соответствии с профилем для удовлетворения различным требованиям, например, для обеспечения большего или меньшего количества битов маркера.

Типы трафика. Профиль обычно определяет множество форматов трафика (например, алгоритмов кодирования мультимедийных данных) и заданное по умолчанию статическое соответствие этих форматов и значений PT. Некоторые из форматов трафика могут быть определены ссылкой на отдельные описания формата трафика. Для каждого

O‘ZBEKISTON RESPUBLIKASI STANDARTLARI BILAN O‘ZGARTIRISH VA MAZKUR MILLIY STANDARTLARNI AXBOROT TEXNOLOGIYALARINI JORIY ETISH BOSHQARMASI

определенного типа трафика профиль должен задать необходимую для использования тактовую частоту временной метки RTP.

Дополнения заголовка пакета данных RTP. Если требуются некоторые дополнительные функциональные возможности в рамках класса приложений профиля, не зависящих от типа трафика, то к фиксированному заголовку пакета данных RTP могут быть присоединены дополнительные поля.

Расширения заголовка пакета данных RTP. Должно быть определено содержимое первых 16 bit структуры расширения заголовка пакета данных RTP, если использование этого механизма позволено профилем.

Типы пакетов RTCP. Могут быть определены (и зарегистрированы IANA) новые, зависящие от класса приложения, типы пакетов RTCP.

Интервал отчетности RTCP. Профиль должен определить величины, используемые при вычислении интервала отчетности RTCP: часть полосы пропускания сеанса RTCP, минимальный интервал отчетности и разделение полосы пропускания между отправителями и получателями.

Расширение пакета SR/RR. Если имеется дополнительная информация об отправителе или получателе, которая должна регулярно передаваться, то для пакетов SR и RR протокола RTCP может быть определен раздел расширения.

Использование SDES. Профиль может определять относительные приоритеты для пунктов SDES протокола RTCP, которые будут переданы или исключены, альтернативный синтаксис или семантику для пункта CNAME, формат пункта LOC, семантику и использование пункта NOTE и новые пункты SDES, которые должны регистрироваться в IANA.

Безопасность. Профиль может определять, какие услуги по обеспечению безопасности и алгоритмы нужно использовать приложениям, и может обеспечивать управление их использованием.

Соответствие пароль-ключ. Профиль может определять, как введенный пользователем пароль преобразуется в ключ шифрования.

Протокол нижележащего уровня. Для передачи пакетов RTP может требоваться использование конкретной нижележащей сети или протокола транспортного уровня.

Для каждого разрабатываемого приложения не должен требоваться новый профиль. Целесообразнее в рамках одного класса приложений расширять существующий профиль, а не создавать новый. Это облегчит взаимодействие приложений, так как каждое приложение обычно выполняется под управлением только одного профиля. Простые расширения, такие как определения дополнительных значений PT или типов пакетов RTCP, могут быть выполнены путем регистрации их в IANA и публикации их описаний в спецификации профиля или в спецификации формата трафика.

O‘ZSTANDART AGENTLIGA
STANDARTLASHTIRISH, DAVLAT
NAZORATI VA KUZATISH TIZIMIDA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

12 Профиль RTP для аудио- и видеоконференций с минимальным управлением

12.1 Форматы пакетов RTP и RTCP и параметры протокола

В данном подразделе приведено описание профиля для использования протокола реального времени RTP и связанного с ним протокола управления RTCP в рамках групповой аудио- или видеоконференции, так называемого профиля RTP для аудио- и видеоконференций с минимальным управлением (RTP Profile for Audio and Video Conferences with Minimal Control). Минимум управления означает, что не требуется никакая поддержка согласования параметров или управления принадлежностью (например, при использовании статических соответствий типов трафика и индикаций принадлежности, обеспечиваемых RTCP). Ниже приведены описание ряда пунктов, которые могут быть определены или изменены в профиле.

Заголовок информационного пакета RTP. Используется стандартный формат фиксированного заголовка информационных пакетов RTP (один бит маркера).

Типы трафика. Статические значения типов трафика определены в подразделах 12.3 и 12.4.

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. То есть, 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 bit таким образом, чтобы можно было идентифицировать множество различных расширений.

Типы пакетов RTCP. Никаких дополнительных типов пакетов RTCP в этой спецификации профиля не определено.

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 CNAME посылается в каждом отчетном интервале, другие пункты должны передаваться только в каждом пятом интервале отчетности.

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH VA METROLOGIYA
AGENTLIGI TOMONIDAN TASDIQLANGAN
ASLIDAN KO‘CHIRILDI
JORIY ETISH UCHUN BOSHQARMASI

Безопасность. Заданные по умолчанию службы безопасности RTP также определяются по умолчанию этим профилем.

Соответствие пароль-ключ. Вводимый пользователем пароль преобразуется с использованием алгоритма MD5 в 16-октетный дайджест. N-битовый ключ получается из дайджеста путем использования его первых N битов. Предполагается, что пароль может включать только буквы в коде ASCII, цифры, дефисы и пробелы, чтобы уменьшить вероятность искажений при передаче паролей по телефону, факсу, телексу или электронной почте. Паролю может предшествовать спецификация алгоритма шифрования. Любые символы вплоть до первой наклонной черты вправо (код ASCII 0x2f) воспринимаются как название алгоритма шифрования. Если наклонная черта вправо отсутствует, то по умолчанию считается, что используется алгоритм шифрования DES-CBC.

Нижележащий протокол. Профиль определяет использование RTP над протоколом UDP в двухстороннем и групповом режиме.

Транспортное соответствие. Используется стандартное соответствие RTP и RTCP адресам транспортного уровня.

Инкапсуляция. Инкапсуляция пакетов RTP не определена.

12.2 Регистрация типов трафика

Данный профиль определяет стандартные типы кодирования, используемые с RTP. Другие типы кодирования перед использованием должны быть зарегистрированы IANA. При регистрации нового типа кодирования должна быть обеспечена следующая информация:

– условное наименование типа кодирования и тактовая частота временной метки RTP (условные наименования должны иметь длину в три или четыре символа для обеспечения компактного представления, если это необходимо);

– указание того, кто имеет право изменять тип кодирования (международные организации по стандартизации, консорциум, конкретная компания или группа компаний);

– любые рабочие параметры;

– ссылки на доступные описания алгоритма кодирования, (например в порядке предпочтения), изданная статья, регистрация патента, технический отчет, исходный текст кодека или справочник;

– для частных типов кодирований, контактная информация (почтовый адрес и адрес электронной почты);

– величина для обозначения типа трафика этого профиля в случае необходимости.

Не все типы кодирования, которые нужно использовать с протоколом RTP, должны быть назначены статически. Для установления динамического соответствия между значением типа трафика (PT) в

STANDARTLASHTIRISH, DAVLAT
NAZORATI VA SERTIFIKATLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

диапазоне от 96 до 127 и типом кодирования могут использоваться не-RTP средства.

Доступное пространство значений типов трафика достаточно мало. Новые типы трафика назначаются статически (постоянно) только, если выполнены следующие условия:

– кодирование в большой степени интересует сообщество сети Интернет;

– 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.

12.3 Кодирование звукового сигнала

Для приложений, которые не посылают пакеты во время пауз, первый пакет активного участка речи (первый пакет после паузы) отличается установленным в единицу битом маркера в заголовке информационного пакета RTP. Приложения без подавления пауз устанавливают этот бит в нуль.

Тактовая частота RTP, используемая при генерации временной метки RTP, не зависит от числа каналов и типа кодирования и равна числу периодов дискретизации в секунду. Для N-канального кодирования (стерео, квадро и т.п.) каждый период дискретизации (1/8000 s) генерирует N отсчетов. Общее число отсчетов, сгенерированных за секунду, равно произведению частоты дискретизации на число каналов.

При использовании нескольких звуковых каналов они нумеруются слева направо, начиная с первого. В звуковых пакетах RTP данные из каналов с меньшими номерами предшествуют данным из каналов с большими номерами.

Отсчеты всех каналов, принадлежащие одному моменту дискретизации, должны быть внутри одного и того же пакета. Перемежение отсчетов из различных каналов зависит от типа кодирования.

Частота дискретизации должна быть выбрана из множества: 8000, 11025, 16000, 22050, 24000, 32000, 44100 и 48000 Hz (компьютеры Macintosh Apple имеют собственные значения частоты дискретизации 22254,54 и 11127,27, которые могут быть преобразованы в 22050 и 11025 с допустимым качеством путем пропуска четырех или двух отсчетов в 20-миллисекундном кадре). Однако большинство алгоритмов кодирования звука определено для более ограниченного множества частот дискретизации. Получатели должны быть готовы принимать многоканальный звук, но могут выбирать и монофонический режим.

O'ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI, MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
... ETISH BOSHQARMASI

Для пакетизации звукового сигнала заданный по умолчанию интервал пакетизации должен иметь продолжительность 20 ms, если при описании кодирования не указано иное значение. Интервал пакетизации определяет минимальную задержку из конца в конец. В более длинных пакетах под заголовок отводится относительно меньшая часть байтов, но они вызывают большую задержку и делают потери пакетов более значимыми. Для неинтерактивных приложений, таких как лекции, или каналов со значительными ограничениями полосы пропускания может быть допустима более высокая задержка пакетизации. Получатель должен принимать пакеты со звуковым сигналом с задержкой от 0 до 200 ms. Это ограничение обеспечивает приемлемый размер буфера для получателя.

В основанных на отсчетах кодированиях каждый отсчет сигнала представлен фиксированным числом битов. Внутри сжатых звуковых данных коды отдельных отсчетов могут пересекать границы октета. Длительность сигнала, передаваемого в звуковом пакете, определяется числом отсчетов в пакете.

Для типов кодирования, основанных на отсчетах и производящих для каждого отсчета один или более октетов, отсчеты из различных каналов, дискретизированные одновременно, упаковываются в соседние октеты. Например, для кодирования стереозвука последовательность октетов такова: левый канал, первый отсчет; правый канал, первый отсчет; левый канал, второй отсчет; правый канал, второй отсчет и т.д. При многооктетном кодировании первым передается старший октет. Упаковка основанных на отсчетах кодирований, производящих менее одного октета для каждого отсчета, определяется алгоритмом кодирования.

Алгоритм основанного на кадре кодирования преобразует блок звукового сигнала фиксированной длины в другой блок сжатых данных, обычно также фиксированной длины. Для основанных на кадрах кодирований отправитель может объединять несколько таких кадров в одно сообщение.

Для основанных на кадрах кодеков, порядок следования каналов определен для целого блока. То есть, для стереозвука отсчеты для левого и правого каналов кодируются независимо; при этом кадр кодирования для левого канала предшествует кадру для правого канала.

Все ориентированные на кадры звуковые кодеки должны быть способны кодировать и декодировать несколько последовательных кадров, передаваемых внутри одного пакета. Так как размер кадра для ориентированных на кадры кодеков задан, то нет никакой потребности использовать отдельное обозначение для одного и того же кодирования, но с различным числом кадров в пакете.

В таблице 3 представлены значения типов кодирования PT, условные обозначения алгоритмов кодирования и тактовая частота,

O‘ZSTANDART AGENTLIGA
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISHVA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

определяемая данным профилем, а также не назначенные, зарезервированные и динамически задаваемые значения PT.

Таблица 3 – Значения типов кодирования PT

Значение типа трафика	Условное обозначение алгоритма кодирования	Тактовая частота, Hz
24	не назначено	-
25	CelB	90000
26	JPEG	90000
27	не назначено	-
28	nv	90000
29	не назначено	-
30	не назначено	-
31	H261	90000
32	MP2T	90000
33-71	не назначено	-
72-76	зарезервировано	-
77-95	не назначено	-
96-127	динамически задаваемые значения	-

Значения типа трафика в диапазоне от 96 до 127 могут быть определены динамически через протокол управления конференции, который не рассматривается в данной статье. Например, каталог сеанса может определять, что для данного сеанса связи, тип трафика 96 обозначает кодирование PCMU, двухканальное с частотой дискретизации 8000 Hz. Диапазон значений типа трафика, отмеченный, как «зарезервировано», не используется, чтобы пакеты RTCP и RTP могли надежно различаться.

Источник RTP в любой заданный момент времени выдает трафик только одного типа; перемежение трафика различных типов в одном сеансе связи RTP недопустимо. Для передачи различных типов трафика могут использоваться параллельно несколько сеансов RTP. Типы трафика, определенные в данном профиле, относятся или к звуковому, или к видеосигналу, но не к обоим сразу. Однако позволяется определять комбинированные типы трафика, которые объединяют, например, звук и видео с соответствующим разделением в формате трафика.

Звуковые приложения, использующие данный профиль, должны, как минимум, быть способны посылать и получать трафик типа 0 (PCMU) и 5 (DVI4). Это позволяет взаимодействовать без согласования формата.

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, METROLOGIYA
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

12.4 Назначение портов

Данные протокола RTP должны передаваться через порт UDP с четным номером, а соответствующие пакеты RTCP должны передаваться через порт с номером, на единицу большим (нечетным номером).

Приложения, работающие с этим профилем, могут использовать любую такую пару портов UDP. Например, пара портов может назначаться программой управления сеансом связи случайным образом. Единственная фиксированная пара номеров портов не может быть задана потому, что в ряде случаев несколько приложений, использующих этот профиль, должны корректно исполняться на одном и том же хосте, а некоторые операционные системы не позволяют множеству процессов использовать один и тот же порт UDP с различными групповыми адресами.

Однако по умолчанию могут быть заданы номера портов 5004 и 5005. Приложения, которые используют множество профилей, могут выбирать эту пару портов, как индикатор данного профиля. Но приложения могут также требовать, чтобы пара портов была задана в явном виде.

O'ZSTANDART AGENTLIGA
STANDARTLASHTIRISH, DAVLAT
NAZORATI VA AXBOROT-KUTUBXONA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH KOSHQARMASI

УДК ОКС 33.040.40 Э 54

Ключевые слова: идентификатор, пакетная передача данных, протокол, профиль, режим реального времени, сеанс

O‘ZSTANDART AGENTLIGI
STA... ...TSH. QAYLAT
NAZO... ...LASHTIRISH VA
AXBO... ...TIVLARINI
JORIY ET... ...QARMASI

Заместитель директора
ГУП «UNICON.UZ» А.Кадиров

Заместитель начальника
научно-исследовательского
департамента развития
телекоммуникационной
инфраструктуры А.Мирхабибов

Инженер научно-
исследовательского
отдела телекоммуникационных
технологий и услуг З.Салахутдинов

Нормоконтроль 02.11.2014 Л.Шаймарданова

СОГЛАСОВАНО

Начальник отдела
телекоммуникационных
технологий и услуг
Государственного комитета
связи, информатизации
и телекоммуникационных
технологий Республики Узбекистан

З.Зияев
письмо от 29.07.2014
№ 09-8/4521

СОГЛАСОВАНО

Заместитель генерального
директора АК «Узбектелеком»

Ж.Максудов
письмо от 22.07.2014
№ 27-03-44/3067

O‘ZSTANDART AGENTLIGA
STANDARTLASHTIRISH, DAVLAT
NAZORAT VA SERTIFIKATLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
IBRIY ETISH BOSHQARMASI