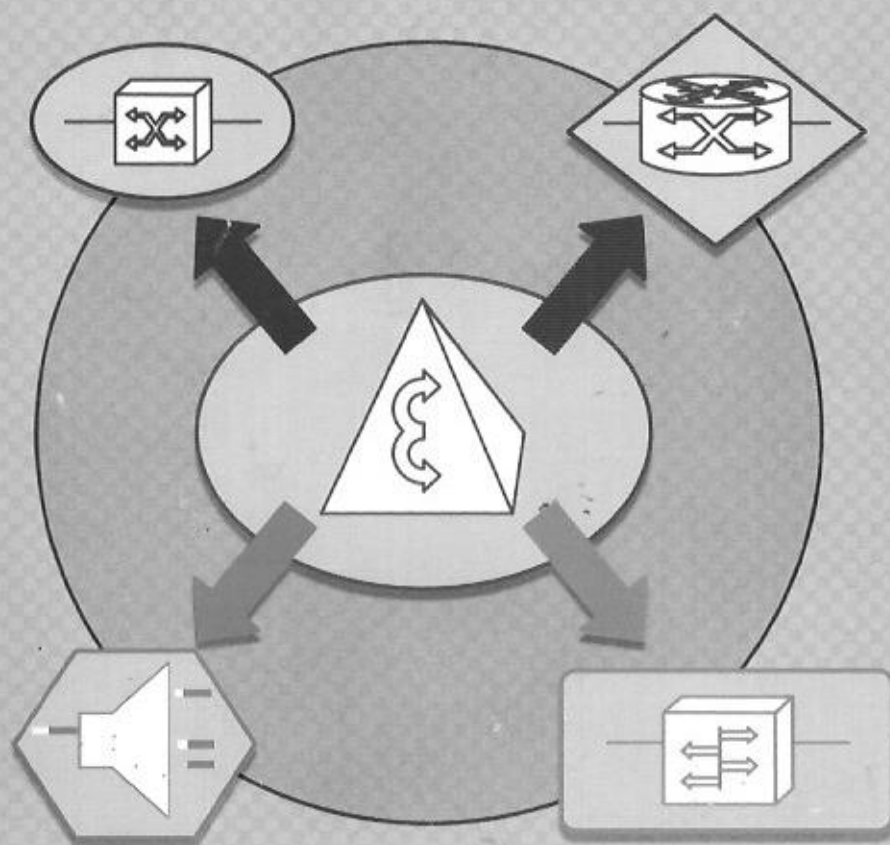


В.Ю.Деарт

МУЛЬТИСЕРВИСНЫЕ СЕТИ СВЯЗИ

Протоколы и системы управления сеансами
(Softswitch/IMS)



ГО 16.05.15 4527
ГО 24.10.15 7969

**МИНИСТЕРСТВО СВЯЗИ
И МАССОВЫХ КОММУНИКАЦИЙ
РОССИЙСКОЙ ФЕДЕРАЦИИ**

Государственное образовательное учреждение
высшего профессионального образования

Московский технический университет связи и информатики

В.Ю. Деарт

Рекомендовано УМО по образованию в области телекоммуникаций в качестве учебного пособия для студентов высших учебных заведений, обучающихся по направлению подготовки дипломированных специалистов 210400 – Телекоммуникации. Протокол № 55 от 24 февраля 2011 г.

Мультисервисные сети связи

**Протоколы и системы управления сеансами
(Softswitch/IMS)**

Учебное пособие

Москва 2011

Библиотека
МТУСИ

28.4.15 a

Деарт В.Ю.

Мультисервисные сети связи. Протоколы и системы управления сеансами (Softswitch/IMS). – М.: Брис-М, 2011 – 198 с., 79 илл.

Развитие современных телекоммуникационных сетей неразрывно связано с созданием сетей нового поколения (NGN), основу которых составляют мультисервисные сети. Построение единой транспортной сети на базе протокола IP, представляющей пользователю максимальный набор услуг, невозможно без специалистов владеющих всеми современными технологиями. Цель данного пособия сформировать целостное представление о мультисервисных сетях у выпускников телекоммуникационных вузов.

Книга написана по материалам курса лекций «Мультисервисные сети связи», многократно прочитанного автором в период 2008-2010 годов студентам по специальности 210400 (Сети связи и системы коммутации), магистрам по направлению 231200 (Информатика и вычислительная техника) и аспирантам МТУСИ.

Первая часть пособия, в которую вошли лекции по транспортным сетям и сетям доступа, была издана в 2007-2008 гг. В данной книге рассматривается уровень управления сеансами сетей NGN. Здесь уделяется большое внимание протоколам управления и сигнализации, которые реализуются в программных коммутаторах (Softswitch) и подсистемах мультимедийной связи (IMS).

Материал изложен таким образом, что его можно читать без изучения первой части. Однако в любом случае от читателя потребуются знания основ IP-технологии и базовых знаний по современным сетям связи (особенно в части ОКСи7).

Рецензенты: доктор технических наук, профессор Самуйлов К.Е.
кандидат технических наук Бакланов И.Г.

ISBN 978-5-905376-01-6

© В.Ю. Деарт, МТУСИ – 2011г.

СОДЕРЖАНИЕ

Введение	6
Глава 1. Технология передачи голоса через IP-сети.....	8
1.1 Терминалы VoIP	8
1.2 Кодеки.....	11
1.3 Протокол передачи в реальном времени (RTP)	16
1.4 Протокол управления RTCP (RTP Control Protocol)	25
Глава 2. Протокол H.323	36
2.1 Архитектура сети H.323	36
2.2 Адресация в H.323	37
2.3 Структура Рекомендации H.323	38
2.4 Комментарий по чтению трассировок.....	46
Глава 3. Протокол инициации сессий SIP	48
3.1 Структура протокола SIP	48
3.2 Сообщения SIP	49
3.3 Сценарий установления соединения.....	51
3.4 Формат сообщений SIP	53
3.5 Временная диаграмма процесса установления соединения	57
Глава 4. Сети NGN с программными коммутаторами (Softswitch)	63
4.1 Построение сетей NGN на базе программных коммутаторов.....	63
4.2 Взаимодействие сигнализаций в NGN	66
4.3 Сценарии перехода от ТФОП к NGN.....	70
4.4 Функциональная схема программного коммутатора SX	73
Глава 5. Протоколы транзита сигнализации SIGTRAN.....	76
5.1 Архитектура протоколов SIGTRAN	76
5.2 Транспортный протокол с управлением потоками SCTP.....	78
5.3 Протоколы адаптации SIGTRAN	92
5.3.1 Протокол M3UA	92
5.3.2 Протокол SUA	96
5.3.3 Протокол M2UA	98
5.3.4 Протокол M2PA	101
5.3.5 Протокол IUA	104

Глава 6. Протокол управления транспортными шлюзами MEGACO/H.248.....	105
6.1 Развитие протоколов управления шлюзами.....	105
6.2 Концепция и основные определения.....	106
6.3 Порядок установления соединения через сеть NGN, управляемую программным коммутатором SX.....	118
Глава 7. Принципы построения защищенных сетей NGN....	125
7.1 Необходимость защиты информации в NGN	125
7.1.1 Технологические изменения.....	125
7.1.2 Законодательные изменения.....	126
7.1.3 Организационные изменения	127
7.1.4 Причины необходимости защиты информации в NGN.....	127
7.2 Анализ уязвимостей и факторов риска в NGN	129
7.2.1 Основные понятия и определения.....	129
7.2.2 Наиболее вероятные риски в NGN	131
7.2.3 Анализ мультимедийной архитектуры NGN.....	132
7.2.4 Необходимость приоритезации задач защиты сети.....	134
7.3 Виртуальные частные сети (VPN) – основа защищенного решения.....	135
7.4 Защищенное решение для сети NGN класса 5	139
7.4.1 Защищенные зоны.....	140
7.4.2 Защита на границах зон и доменов	142
7.4.3 Технологии защиты	143
7.4.4 Обнаружение и предотвращение атак.....	145
7.4.5 Проблемы прохождения потоков через межсетевые экраны и NAT.....	146
Глава 8. Подсистема мультимедийной связи IMS	149
8.1 Концепция IMS (IP Multimedia Subsystem)	149
8.2 Архитектура IMS	150
8.3 Сценарии установления сессий.....	157
8.4 Реализация IMS.....	162
Литература.....	165
Список сокращений	166

Приложение 1. Сокращенная трассировка процесса установления соединения, передачи речи и разъединения соединения между двумя терминалами H.323 под управлением привратника	169
Приложение 2. Сокращенная трассировка процесса установления соединения, передачи речи и разъединения соединения между двумя терминалами SIP через Proxy сервер	179
Приложение 3. Сокращенная трассировка процесса установления соединения, передачи речи и разъединения соединения между исходящим шлюзом A7505 MG и входящим шлюзом A7515 MG под управлением контроллера шлюзов A5020 MGC.....	184

ВВЕДЕНИЕ

На сегодняшний день сети следующего поколения NGN превратились из неточно определенной концепции в ряд реальных проектов, разработка, внедрение и опытная эксплуатация, которых дали инженерам ценный опыт освоения новой технологии и выявили достоинства и скрытые недостатки новых сетей. Именно практический опыт показал как недостаточную проработанность некоторых технических решений, так и неготовность эксплуатировавшего персонала решать насущные задачи по настройке и мониторингу сетей NGN, а самое главное по обеспечению требований по качеству обслуживания QoS и защите информации. Усовершенствование технологии NGN в наибольшей степени коснулось уровня управления сеансами, где на смену программным коммутаторам Softswitch пришли новые распределенные платформы IMS. Переход к сервисно-ориентированным платформам, имеющим единую абонентскую базу HSS и предоставляющим пользователям любые услуги, включая передачу голоса VoIP, высокоскоростной доступ в Интернет (HSI), передачу телевидения IPTV, видео по запросу VOD, мультимедийную конференцсвязь и др. ознаменовал фактически новый этап в развитии сетей следующего поколения.

Быстрое развитие и совершенствование технологий NGN обострило вопрос о подготовке специалистов, способных глубоко понимать технологию и уметь решать задачи построения, мониторинга, эксплуатации и техобслуживания оборудования NGN второго этапа их развития.

Формирование цельного представления о современных сетях NGN, основанное на глубоком понимании и знании протоколов взаимодействия сетевых элементов и является основной задачей, которую автор поставил перед собой в процессе написания данной книги. Для достижения поставленной цели автор использовал оригинальную концепцию построения как учебного курса в целом, так и настоящего пособия. Концепция предполагает изучение протоколов NGN на примерах реальных трассировок процессов установления и разъединения сеансов, снятых на функционирующих сетях программой-сниффером WireShark. При этом в основных разделах соблюдается следующая последовательность: сначала

излагаются функции протокола, его синтаксис и примеры основных команд, затем приводится временная диаграмма процесса с пояснениями и, наконец, в приложении приводится текст реальной трассировки, точно соответствующий рассмотренному сценарию. Таким образом, читателю предоставляется возможность изучить функциональность и команды протокола, исследовать временную диаграмму и закрепить и расширить свои познания в процессе расшифровки и чтения трассировки. Получение практических навыков чтения трассировок сигнальных сообщений является необходимой частью формирования современного специалиста в области сетей NGN, поскольку этот процесс необходим при построении, наладке и эксплуатации современных мультисервисных сетей связи.

Читатель, успевший ознакомиться с оглавлением, знает, что книга начинается с рассмотрения технологии передачи голоса VoIP и включает подробное описание протоколов передачи мультимедийной информации – RTP/RTCP. В следующих главах рассматриваются протоколы H.323 и SIP в соответствии с изложенной концепцией (см. трассировки в приложениях 1 и 2). В 4-ой главе достаточно кратко рассматриваются принципы построения программных коммутаторов Softswitch (SX). Однако главы 5 и 6 можно считать продолжением рассмотрения функционирования SX, поскольку представленные в этих главах протоколы SIGTRAN и H.248/MEGACO определяют работу SX в режиме контроллера шлюзов (MGC). Особое место в пособии занимает глава 7, в которой излагаются принципы построения защищенных сетей NGN и приводятся примеры защищенных сетевых решений. Переход от программных коммутаторов SX к распределенным подсистемам мультимедийной связи IMS никак не изменил общую концепцию сетей NGN и набор применяемых протоколов взаимодействия. Более того, многие компании-производители оборудования в своих реализациях IMS продолжают использовать SX, в качестве составных элементов IMS. Таким образом, весь материал пособия составляет единое описание существующего уровня сетей NGN.

Автор выражает свою благодарность редактору Аладину В.М., аспиранту МТУСИ Пилюгину А.В. и преподавателю учебного центра Алкатель-Лусент Федотову Д.А., которые оказали автору существенную помощь в подготовке настоящего пособия.

Глава 1. ТЕХНОЛОГИЯ ПЕРЕДАЧИ ГОЛОСА ЧЕРЕЗ IP-СЕТИ

1.1 Терминалы VoIP

Технология передачи голоса через IP-сети уже прочно вошла в жизнь современного человека. Кто-то не задумывается, что его голос добирается в виде непрерывного аналогового сигнала по ТфОП только до ближайшего шлюза, а далее продолжает свой путь в виде потока голосовых пакетов. Некоторые используют для международного разговора дешевые карты провайдера VoIP. Другие сознательно покупают гарнитуру и устанавливают у себя на ПК специальные программы (Skype, Google Talk...) для того, чтобы осуществлять телефонную связь с использованием технологии VoIP по всему миру, снижая свои затраты. Крупные и средние корпорации устанавливают у себя офисные VoIP АТС, которые позволяют использовать IP-телефонию для внутренних переговоров, а исходящий телефонный трафик может быть направлен, как в обычную телефонную сеть, так и провайдеру VoIP.

Попробуем разобраться, какие общие технологические особенности VoIP объединяют этих пользователей и в чем проявляются отличия, присущие только определенным группам пользователей.

Начнем с классификации терминалов. Все терминалы VoIP делятся на программные реализации для ПК и отдельные полнофункциональные устройства. Естественно, что для ПК тоже потребуется дополнение в виде гарнитуры (телефон + микрофон). Однако основную работу будет выполнять аппаратный комплекс ПК под управлением специализированной программы, поэтому часто такие терминалы VoIP называют *программными*. Существует большое количество программных реализаций VoIP-терминалов, которые следует разделять на *стандартные* и *специализированные*. Стандартные программные пакеты ориентированы на реализацию стандартизованных протоколов сигнализации VoIP: H.323 или SIP (например, SJPhone или eyeBeam), тогда как специализированные используют нестандартную сигнализацию и часто нестандартные протоколы передачи речи (например, Skype или Cisco IP Communicator). Каждая программа эмулирует на эк-

ране компьютера образ некоего телефонного устройства IP-телефона (eyeBeam, SJPhone, Skype), на котором обычно отражаются клавиши набора номера, функциональные кнопки, телефонный справочник, меню сервисов и пр. (рис. 1.1).



Рисунок 1.1 Пример интерфейсов программных VoIP-терминалов

Как правило, экран управления программного IP-телефона (IP-Phone) содержит общепонятные обозначения стандартных функций телефонного аппарата: поднятую и положенную телефонную трубку, клавиши набора цифр телефонного номера, изображение микрофона и панели управления уровнем громкости. При этом, даже программы известных производителей могут иметь определенные отличия в реализации сигнальных протоколов H.323 или SIP, что, как правило, не приводит к нарушениям в процессе установления обычного соединения, но может приводить к некорректной реализации дополнительных видов обслуживания (ДВО).

Необходимо отметить, что сигнализационные протоколы H.323 не совместимы с протоколами SIP, поэтому взаимодействие соответствующих терминалов обычно организуется на уровне программного коммутатора SX (Interworking Function).

Аппаратные терминалы VoIP можно подразделить на так называемые USB-Phone и аппаратные IP-Phone. **USB-Phone** – это отдельное функциональное устройство (рис. 1.2), которое подключается к разьему USB стандартного ПК. Как видно из рис. 1.2, по форме оно напоминает телефонный аппарат и содержит все необ-

ходимые клавиши управления. Однако для своего функционирования этому устройству требуется ПК, подключенный к IP-сети с установленными драйверами. То есть USB-Phone, по своей сути, является упрощенным интерфейсом программного IP-телефона.



Рисунок 1.2 Аппаратный USB-Phone

Аппаратный IP-Phone представляет из себя отдельное полнофункциональное устройство, которое имеет встроенный Ethernet интерфейс, и выполняет все функции по установлению и разъединению телефонных соединений и передачи голоса (рис. 1.3).



Рисунок 1.3 Аппаратный IP-телефон Alcatel-Lucent

Существует большое количество разнообразных моделей аппаратных IP-Phone различных компаний производителей, например, IP-телефоны компании Cisco или Alcatel-Lucent.

Шлюзы VoIP обеспечивают возможность подключения обычных аналоговых телефонных аппаратов или цифровых телефонов ISDN к пакетным сетям. Для подключения к IP-сети используется IP-интерфейс, а все функции по установлению и разъединению соединений в пакетной сети выполняются самим шлюзом. Шлюз также может поддерживать аналоговую сигнализацию и ЦАС№1 (DSS1) на абонентских портах.

Офисные АТС (УПАТС) выполняют все функции по поддержке сигнализации и передачи голосового трафика в пакетной сети посредством встроенных шлюзов VoIP и отличаются от последних обязательной возможностью внутренних соединений между локальными абонентами и наличием большого набора ДВО.

Таким образом, все перечисленные терминалы VoIP должны обязательно выполнять следующие функции:

- обеспечивать кодирование голоса для преобразования в цифровой вид (кодеки);
- выполнять упаковку фрагментов речи в пакеты по стеку протоколов RTP/UDP/IP;
- поддерживать непрерывный поток голосовых пакетов (RTP-сессию);
- сглаживать неравномерность поступления пакетов (антиджиттерный буфер);
- обеспечивать установление и разъединение голосовых соединений (сигнализационные протоколы H.323 или SIP);
- поддерживать ДВО.

Последовательно рассмотрим реализацию всех перечисленных функций.

1.2 Кодеки

Задача преобразования аналогового телефонного сигнала в цифровой поток и его восстановление из непрерывного цифрового потока в аналоговый сигнал, воспроизводимый в телефоне, была решена еще на заре создания первых цифровых систем передачи с

помощью кодеков, построенных по Рекомендации МСЭ-Т G.711. Для кодирования использовался метод импульсно-кодовой модуляции (ИКМ), который предполагал, что поступающий аналоговый голосовой сигнал сначала дискретизируется с частотой 8 кГц, а затем амплитуда полученных отсчетов проходит процедуру нелинейного квантования по уровню в соответствии с квазилогарифмическим законом (А-закон для Европы). В результате этих действий каждый отсчет представляется одной 8-битной двоичной комбинацией. Таким образом, скорость передачи на выходе кодека составляет 64 кбит/с (8 кГц × 8 бит). Этот кодек отличается простотой реализации и достаточно высоким качеством передачи речи, что обуславливает его широкое применение и в технологии VoIP. К недостаткам кодеков G.711 следует отнести относительно высокую скорость передачи, необходимую для одного голосового вызова.

Рекомендация G.726 описывает технологию кодирования с применением адаптивной дифференциальной импульсно-кодовой модуляции (АДИКМ). Метод основан на кодировании не абсолютных значений аналогового сигнала, а на передаче информации об изменении сигнала по сравнению с его предыдущим значением, что позволяет снизить требуемую скорость передачи до 32 кбит/с (24 кбит/с, 16 кбит/с). Такие кодеки часто используются в системах видеоконференции. В приложениях VoIP кодеки такого типа практически не нашли применения из-за недостаточной устойчивости к потерям пакетов.

В кодеках, основанных на Рекомендации G.728, используется технология LD-CELP (Low Delay – Code Excited Linear Prediction). Данная технология предполагает, что передается информация не об одном отсчете, а о группе из 5 отсчетов. Таким образом, длительность кадра составляет 0,625 мс, а задержка кодирования не превышает 2,5 мс. Недостатками кодека G.728 являются высокие требования к производительности процессора обработки (40 MIPS) и относительно высокая чувствительность к потерям кадров. Данный тип кодеков предназначен для использования в терминалах видеоконференцсвязи и в терминалах VoIP применяется достаточно редко.

Семейство кодеков G.729 реализовано с применением технологии CS-ACELP (Conjugate Structure – Algebraic Code Excited Li-

near Prediction). Алгоритм сопряженной структуры с управляемым алгебраическим кодом и линейным предсказанием достаточно сложен (подробнее см. в [13]). Кодек формирует кадры голосового сигнала длительностью 10 мс, при стандартной частоте дискретизации 8 кГц. Скорость передачи на выходе кодека составляет 8 кбит/с. В терминалах VoIP данный кодек применяется очень часто, поскольку обеспечивает достаточно высокое качество передачи речи и устойчив к потерям кадров.

Рекомендация G.723 описывает технологию MP-MLQ (Multi-Pulse – Multi Level Quantization). Алгоритм множественной импульсной многоуровневой квантизации предполагает, что сначала речь кодируется кодом G.711, а затем применяется вокодер. Процесс обработки речи предполагает формирование кадров длительностью 30 мс. Данный алгоритм позволяет снизить скорость передачи на выходе кодера до 5,6-6,3 кбит/с. Кодек имеет два варианта кодирования: с алгоритмом MP-MLQ, работающем на скорости 6,3 кбит/с, и с алгоритмом CELP, обеспечивающем скорость 5,6 кбит/с. Такой кодек обеспечивает наименьшую скорость на своем выходе, однако чувствителен к потерям пакетов. Применение кодеков этого типа в терминалах VoIP ограничено относительно невысоким качеством кодирования речи.

Наилучшее качество передаваемой речи обеспечивают широкополосные кодеки, которые позволяют кодировать весь диапазон частот человеческой речи 0,05 – 7 кГц. Одним из таких кодеков является кодек G.722, использующий технологию субдиапазонной адаптивной дифференциальной импульсно-кодовой модуляции (sub-band ADPCM). Для кодирования речи в семействе кодеков G.722 дискретизация происходит на частоте 16 кГц (иногда на 8 кГц для обеспечения обратной совместимости) и каждый отсчет кодируется при помощи 14 бит. Далее поток бит проходит вторичное кодирование на SB-ADPCM кодере, который снижает скорость передачи до 64 кбит/с. Таким образом, кодеки семейства G.722 обеспечивают передачу речи в высоком качестве (в некоторых источниках используется термин «HD quality») при требованиях к полосе пропускания не выше 64 кбит/с (не выше, чем у кодека G.711).

Последней версией семейства кодеков G.722 является кодек с функционалом AMR-WB (Adaptive Multirate Wideband), позво-

ляющему производить адаптивное изменение скорости передачи в зависимости от условий сетевого окружения. В случае обнаружения насыщения сети пакетами, кодек автоматически снижает скорость передачи. За счёт механизма адаптации происходит снижение требования к занимаемой полосе пропускания. Скорость передачи составляет 6,6-23,85 кбит/с. Преимуществами данного кодека является высокое качество передаваемой речи. Недостатками – сложный механизм кодирования речи, который поддерживается не всеми терминалами и системами.

Наряду с перечисленными кодеками [13], традиционно применяемыми в сетях фиксированной связи, стремительное развитие технологий кодирования речи нашло свое отражение в сетях связи с подвижными объектами. Типичным кодеком, используемым до недавнего времени во всех мобильных телефонах, является кодек по Рекомендации GSM 06.02, который обеспечивает скорость на выходе 13 кбит/с. В последнее время в мобильных терминалах устанавливаются кодеки с алгоритмом AMR (Adaptive MultiRate). У которых скорость передачи на выходе составляет 4,7-11 кбит/с при достаточно высоком качестве передачи речи.

Кроме стандартизованных кодеков некоторые компании разрабатывают собственные корпоративные кодеки (например, известный кодек NetCoder компании AudioCodes). Однако, применение таких кодеков резко ограничено их несовместимостью со стандартными кодеками. Это является существенным недостатком, кроме тех случаев, когда такое ограничение является стратегической целью компании (например, Skype).

Многие из перечисленных кодеков используют дополнительные механизмы повышения эффективности передачи речи, например, алгоритм обнаружения активных фрагментов речи и пауз VAD (Voice Activity Detector). Он позволяет уменьшить требуемую скорость передачи в 4-9 раз.

Однако, в связи с быстрым развитием транспортных сетей, приводящих к многократному уменьшению стоимости передачи данных, многие критерии, по которым ранее проводился отбор и классификация кодеков, теряют свою значимость. Так в современных сетях NGN на первое место выдвигаются показатели качества передачи речи, а способы уменьшения требуемой полосы пропускания становятся менее востребованными. Развитие микропроцес-

сорной техники в области построения все более мощных цифровых сигнальных процессоров (DSP) снижает значимость требований по быстродействию, необходимому для обработки речевых сигналов. Оно еще недавно было очень существенным фактором.

Применение различных кодеков в сетях VoIP выдвигает следующие критерии, расположенные по степени значимости:

1. Качество передачи речи, определяемое как характеристиками кодера, так и показателями пакетной сети (задержки пакетов, джиттер, потери пакетов).
2. Требуемая полоса пропускания в пакетных сетях с учетом заголовков.

Качество передачи речи, обеспечиваемое свойствами конкретного кодека, обычно оценивается по характеристике MOS (Mean Opinion Score). Усредненное экспертное мнение оценивается по пятибалльной шкале, в которой значения в пределах 4-5 баллов соответствуют высокому качеству, 3-4 баллов – хорошему качеству, менее 3 баллов – неудовлетворительному качеству.

В пакетных сетях важными характеристиками, влияющими на качество передачи речи являются:

- а) задержка, вносимая кодером (поскольку общая задержка передачи не должна превышать 150 мс);
- б) типовой размер полезной (голосовой) части пакета;
- в) требуемая скорость передачи в пакетной сети с учетом заголовков.

В кодеках время задержки, вносимой кодированием, и размер кадра определяются применяемой технологией. Типовой размер полезной части голосового пакета не может быть меньше, чем размер кадра, но в одном пакете могут размещаться несколько кадров речи. Выбор оптимальной длины полезной части голосового пакета также зависит от свойства кодека по минимизации влияния потерянных пакетов на качество воспроизводимой речи. Чем больше отрезок речи передавался в одном пакете, тем труднее сглаживать эффект от его потери в сети. Таким образом, сведем все характеристики кодеков в общую сравнительную таблицу 1.1.

Таблица 1.1

Сравнительные характеристики кодеков

Кодек	G.711	G.726	G.728	G.729	G.723.1	G.722.2
Скорость кодирования, кбит/с	64	24/32	16	8	5,3/6,3	6,6-23,85
Размер аудио кадра, байт	160	15/20	10	10	20/25	60
Размер переносимой аудиоинформации в одном аудио кадре, мс	20	5	5	10	30	20
Стандартное количество аудио кадров на пакет	1	5	6	2	1	1
Задержка при кодировании, мс	0,75	0,125	0,625	15	37,5	20-25
Скорость передачи в пакетной IP-сети, кбит/с	80	40/48	32	24	16/17	23-40
Оценка качества по MOS	4,4	4/4,3	3,6	4	3,62/3,9	4,3-4,5

1.3 Протокол передачи в реальном времени (RTP)

Для того, чтобы обеспечить передачу непрерывного потока через пакетную сеть, необходимо использовать такой протокол, который мог бы решать следующие проблемы:

- контроль и восстановление порядка поступления пакетов;
- устранение неравномерности задержки поступления пакетов;
- сглаживание эффекта потери пакетов.

Следовательно, протокол, обеспечивающий решение этих проблем должен:

- вести последовательность пакетов (нумеровать и перенумеровывать);
- обнаруживать потерю пакетов и синхронизировать во времени.

Основой для такого протокола может служить как стек TCP/IP, так и стек UDP/IP.

Вариант с TCP/IP практически невозможен, так как протокол

TCP, хоть и обеспечивает нумерацию пакетов, но абсолютно не подходит к передаче трафика в реальном масштабе времени. Протокол TCP (глава 3 в [6]) распознаёт потерю пакетов и осуществляет переспрос, что значительно увеличивает время поступления необходимых данных и исключает возможность работы в реальном масштабе времени. Протокол TCP обеспечивает сложный механизм контроля скорости передачи потока данных, что негативно сказывается на работе приложений реального времени.

Более подходящим для таких приложений является протокол UDP. Он действует по упрощённой схеме без установления и поддержания логического соединения, что позволяет ему работать быстрее. Протокол UDP осуществляет только доставку пакета в нужный порт и сверку контрольной суммы. Функции обработки последовательности пакетов и их синхронизации по временным отметкам добавляются уже в протоколе RTP (Real-time Transport Protocol – транспортный протокол в реальном времени).

Протокол RTP, описанный в RFC 1889, работает вместе с протоколом управления RTCP (Real-Time Transfer Control Protocol – протокол контроля передачи в реальном времени). RTP осуществляет передачу закодированного аудио- и видеосигнала, а RTCP обеспечивает мониторинг доставки пакетов и сбор статистических данных.

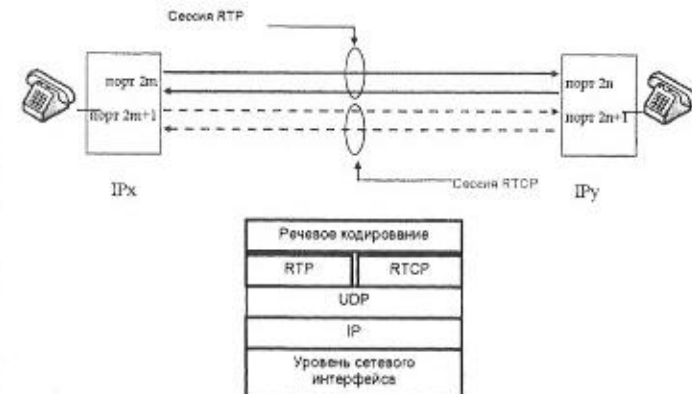


Рисунок 1.4 Сессии RTP и RTCP

За счет буферизации на приеме RTP позволяет:

- устранить отклонение задержек передачи пакетов (джиттер);

- восстановить порядок следования пакетов.

Каждая RTP-сессия (рис. 1.5) идентифицируется следующими параметрами: IP-адресами участников ($IP_src=x$, $IP_dst=y$) и четными номерами UDP-портов ($Port_src=2m$, $Port_dst=2n$). Для контроля и управления RTP-сессией организуется сессия протокола RTCP. Идентификация RTCP-сессии включает те же IP-адреса участников и нечетные номера портов ($Port_src=2m+1$, $Port_dst=2n+1$).

RTP-сессия допускает большое число участников, соединение между которыми возможно в одном из трех режимов (рис. 1.5).

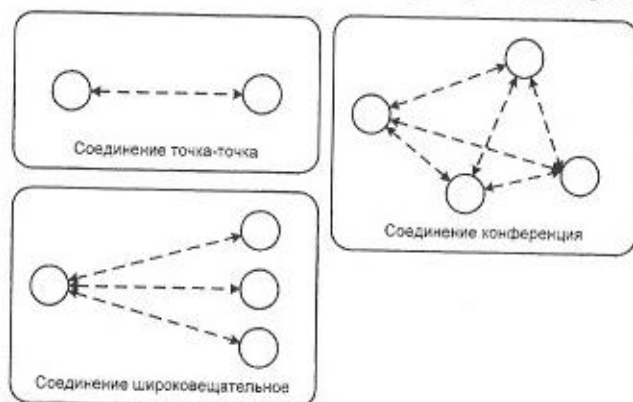


Рисунок 1.5 Конфигурации RTP сессий

При соединении точка-точка обеспечивается двусторонний обмен между двумя участниками. При широковещательной передаче несколько участников получают RTP-поток от одного участника. В конференции обеспечивается равноправный обмен между всеми участниками.

Для описания участников RTP-сессии используются следующие понятия:

- **SSRC** (Synchronization SouRCe – источник синхронизации) – это уникальный 32-битный идентификатор единый для всех пакетов в одном направлении в рамках одной RTP-сессии. Следовательно, назначение пакета однозначно определяется IP-адресом назначения (IP_dst), портом назначения ($Port_dst$) и идентификатором SSRC;

- **Mixer** (Микшер, смеситель) – это промежуточная система, которая получает RTP-пакеты от одного или нескольких источников, комбинирует пакеты по-своему, возможно, меняет формат данных и передает как новый RTP-пакет со своим SSRC;
- **CSRC** (Contributing SouRCe – содействующий источник) – это источник потока RTP-пакетов, который участвует в общей сессии, формируемой смесителем.
- **Транслятор** (translator) – это промежуточная система, которая пропускает RTP пакеты без изменения SSRC, но изменяя каким-либо образом содержание пакета (например, изменяет аудио/видео кодек).

Функционирование трансляторов и смесителей представлено на рис. 1.6.

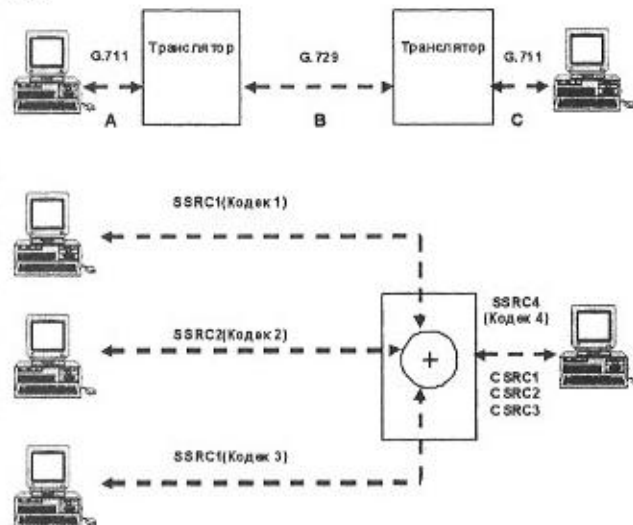


Рисунок 1.6 Функционирование трансляторов и смесителей

Каждый источник передает RTP-пакеты с идентификатором SSRC, который является случайным числом, устанавливаемым в начале сессии. Трансляторы обеспечивают преобразование речевых сигналов с изменением типа кодека.

Пусть участки сети A и C обеспечивают достаточную скорость

передачи данных, и на этих участках возможно применение кодеков G.711, при этом участок В не обеспечивает необходимой скорости передачи данных, там применяется кодек G.729.

При получении пользователем данных из нескольких источников необходимо объединение нескольких RTP-потоков в один. Эта функция выполняется микшерами. При этом возможна также трансляция, так как различные источники информации могут использовать различные кодеки.

В примере, представленном на рис. 1.6, RTP-пакеты передаются от трех источников (SSRC1, SSRC2, SSRC3) в микшер, который собирает принятые пакеты и отправляет их к получателю в объединенном пакете. При этом, пакет имеет SSRC4, а включенные в него пакеты сохраняют свои идентификаторы как содействующих источников (CSRC1, CSRC2, CSRC3).

Заголовок RTP

Заголовок RTP-пакета формируется из нескольких 32-битных строк как показано на рисунке рис. 1.7.

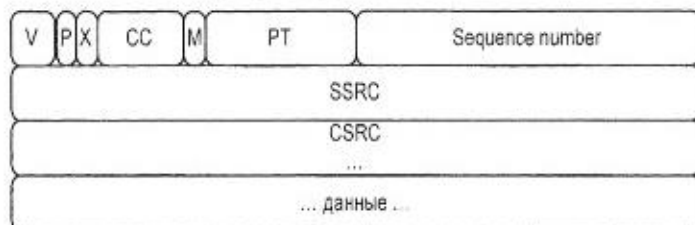


Рисунок 1.7 Формат заголовка RTP-пакета

Рассмотрим назначение полей заголовка:

- *V* (Version) – 2 бита поля зарезервированы для указания версии RTP. На данный момент используется версия 2;
- *P-бит* (Padding) – указывает на, то что пакет содержит один или несколько октетов заполняющих бит для выравнивания. Последний октет точно указывает, сколько заполняющих октетов было добавлено к первоначальной нагрузке. Это необходимо, поскольку нет поля для указания длины нагрузки;
- *X-бит* (eXtension) – указывает на наличие расширения заго-

ловка пакета после поля CSRC в фиксированном заголовке. Цель этих расширений – ввести дополнительные возможности, которых нет в стандартном заголовке;

- *CC* (CSRC Count) – 4 бита указывают на число CSRC, следующих дальше в заголовке;
- *M-бит* (Marked) – обозначает определенные события, например, границу кадра. Этот бит используется опционально. Он может быть использован для обозначения всплеска разговорной речи при использовании механизма подавления пауз, как, например, в кодеке G.723.1;
- *PT* (Payload Type) – 7 бит используются для идентификации формата поля полезной нагрузки. Эти биты могут принимать значения, указанные в табл. 1.2.

Таблица 1.2

Коды протоколов в поле «Тип нагрузки» (PT)

0	G.711 mu-law PCM audio	18	G.729 audio
1	1016 audio	19-22	unassigned audio
2	G.721	23	unassigned audio
3	GSM 6.10 audio	24	unassigned audio
4	G.723.1 audio	25	Ce I B video
5	DV15 audio (8kHz)	26	JPEG video
6	DV15 audio (1kHz)	27	unassigned audio
7	LPC audio	28	nv video
8	G.711 A-law PCM audio	29-30	unassigned audio
9	G.722 audio (16kHz)	31	H.261 video
10	L16 audio (stereo)	32	MPV video
11	L16 audio (mono)	33	MP2T video
12	G.723	34	H.263 video
13	CN (comfort noise level)	35-71	unassigned
14	MPA audio	72-76	reserved
15	G.728 audio	77	RED audio
16	DV15 audio (11.025 kHz)	78-95	unassigned
17	DV15audio (22.050 kHz)	96-127	dynamic

- *Sequence number* (16 бит) – определяет последовательный номер

пакета и увеличивается на один с каждым посланным пакетом RTP. Используется получателем для определения порядка отправки пакетов и обнаружения потери пакетов. Начальный номер последовательности выбирается случайным образом;

- **Timestamp** (32 бита) – указывает относительную временную отметку. Например, при передаче видеоданных первая отметка вставляется (и далее отсчитывается) при кодировании первого кадра в полезную нагрузку пакета, а при передаче аудиоданных первая отметка вставляется, когда первый аудио отрезок помещается в поле полезной нагрузки. Начальное значение этой отметки выбирается случайным образом;
- **SSRC** (32 бита) – определяет источник синхронизации, который подробно уже был описан ранее. Идентификатор выбирается случайно;
- **CSRC** (32 бита) – определяет идентификатор содействующего источника. Всего может быть идентифицировано до 15 распределенных источников. Большее количество CSRC может быть использовано, но их невозможно указать в заголовке пакета. (Если не используется технология смешивания (mixer), то биты CS устанавливаются в 0 и отсутствуют биты CSRC).

Таким образом, в заголовке RTP пакета размещается информация о типе протокола, при помощи которого выполнялось кодирование, о метке относительного времени (времени кодирования), об идентификаторе источника синхронизации и о числе и идентификаторах содействующих источников (участников конференции), если таковые имеются. Для того, чтобы нагляднее представить процесс передачи RTP пакетов во время сессии, рассмотрим временную диаграмму (рис. 1.8), которая была снята программой – sniffером Wireshark во время телефонного разговора.

Как видно из рис. 1.8, пакет №61 передается от терминала с IP-адресом 192.168.0.183 к терминалу назначения с IP-адресом 192.168.0.187. и в качестве полезной нагрузки переносит отсчеты речи, полученные при помощи кодека G.711 с А-законом компандирования. Идентификатор источника синхронизации равен 33071136, а порядковый номер пакета – 22054. Метка относительного времени равна 0, что соответствует началу сессии. Пакет №62

направлен тому же адресату с меткой относительного времени равной 160, что означает передачу 160 отсчетов кодека G.711 в предыдущем пакете. Каждый отсчет кодека G.711 берется через интервал 0,125 мс, что позволяет определить продолжительность передаваемого отрезка речи в 20 мс.

№ пакета	Время	Источник	Назначение	Протокол кодирования пакета	Доп. данные
61	1.11128	192.168.0.183	192.168.0.187	RTP Payload Type=ITU-T G.711PCMA	SSRC=33071136, Seq=22054, Time=0, Mark
62	1.111372	192.168.0.183	192.168.0.187	RTP Payload Type=ITU-T G.711PCMA	SSRC=33071136, Seq=22055, Time=160, Mark
63	1.12588	192.168.0.187	192.168.0.183	RTP Payload Type=ITU-T G.711PCMA	SSRC=435983184, Seq=7840, Time=0, Mark
64	1.126117	192.168.0.187	192.168.0.183	RTP Payload Type=ITU-T G.711PCMA	SSRC=435983184, Seq=7841, Time=160, Mark

Рисунок 1.8 Временная диаграмма передачи RTP пакетов

Пакет №63 передается в обратном направлении и содержит идентификатор источника синхронизации равный 435983184. Порядковый номер этого пакета 7840, а метка относительного времени равна 0, что указывает на начало сессии в этом направлении.

Продолжая рассмотрение приведенной временной диаграммы, нетрудно убедиться, что в ходе сессии происходит обмен RTP пакетами, каждый из которых переносит отрезок речи продолжительностью в 20 мс.

В зависимости от типа используемого кодека меняется соотношение между полезным содержимым (Payload) пакета VoIP и заголовками. На рис. 1.9 наглядно представлено сравнение для трех типов кодеков.

Как видно из приведенного примера, суммарная длина заголовков составляет $IP + UDP + RTP = 20 + 8 + 12 = 40$ байт. Это составляет существенное значение даже для кодеков G.711, а для кодеков G.729 превышает полезную часть. Поэтому в современных сетях применяются меры по уменьшению размера заголовков

в RTP сессиях (сRTP – compressed RTP). С помощью механизма сRTP полный стек IP/UDP/RTP сжимается до 2-4 байт. Количество байт зависит от наличия контрольной суммы.

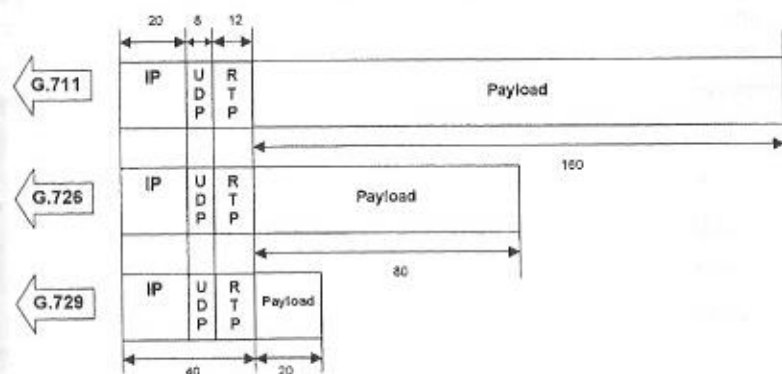


Рисунок 1.9 Соотношение длины заголовков и полезной части в пакетах VoIP

Протокол RTP не имеет механизмов выстраивания пакетов в правильном порядке. При этом, заголовки RTP-пакетов несут всю необходимую информацию (порядковый номер пакета и метку относительного времени). Для реализации данной функции используется анти-джиттерный буфер. Пакеты от источника всегда передаются последовательно и через равные отрезки времени. Однако, проходя через IP-сеть, пакеты могут продвигаться по разным путям и задерживаться на маршрутизаторах на различное время. Это означает, что некоторые пакеты будут приходить раньше предыдущих, а некоторые – позже, чем их ожидают на приеме. Анти-джиттерный буфер позволяет накапливать пакеты и восстанавливать их порядок следования по параметрам заголовков RTP-пакетов.

Кроме задержек в IP-сети возможны потери пакетов, которые приводят к необходимости заполнения пауз, образованных отсутствием голосового пакета. Обычно такие паузы заполняются комфортным шумом, поскольку на человеческом восприятии отрицательно сказывается внезапная полная тишина. Аналогичная ситуация возникает и в том случае, когда пакет задерживается на столько, что вместо его содержания уже начата передача комфортного

шума. Такие слишком задержавшиеся пакеты стираются в анти-джиттерном буфере. Разные типы кодеков обладают различной чувствительностью к потерям пакетов. В среднем, считается, что потери пакетов в IP-сети не должны превышать 1%.

1.4 Протокол управления RTCP (RTP Control Protocol)

Протокол RTCP используется для текущего контроля RTP-сессии и сбора статистической информации по качеству передачи информации (quality of transmission) в сети. Это осуществляется за счет организации обратной связи между источником и получателями информации. Также протокол RTCP поддерживает устойчивый идентификатор источника данных RTP на транспортном уровне, называемый «каноническим именем» (CNAME – canonical name). Так как идентификатор SSRC может изменяться, если обнаружен конфликт или перезапущена программа, то получателям для отслеживания каждого участника требуется каноническое имя CNAME. Получатели также требуют CNAME для отображения множества потоков информации от данного участника на множество связанных сеансов RTP. Например, для синхронизации звукового и видеосигнала. Каждый участник телеконференции при посылке управляющих пакетов всем остальным участникам, может независимо от других оценивать общее число участников. Это число используется при вычислении частоты отправления пакетов RTCP.

Пакеты RTCP передаются вместе с потоком данных RTP только на значительно меньшей скорости. Обычно под RTCP трафик отводится до 5% всего диапазона для передачи потоковых данных. Даже в самых быстрых сессиях пакеты RTCP передаются не чаще, чем раз в пять секунд.

Существует различные типы пакетов RTCP несущие разную информацию:

- SR (Sender Reports – рапорт источника) – содержит статистическую информацию отправителя и информацию получателей;
- RR (Receiver Reports – рапорт приемника) – содержит статистическую информацию получателей;
- SDES (Source DEscription) – содержит описание различных

параметров источника, включая CNAME (имя пользователя);

- *BYE* (запрос разъединения) – это последний пакет, который посылает участник конференции, когда хочет её покинуть;
- *APP* (application – приложение) – содержание приложения, которое определяется самим приложением.

В один пакет транспортного уровня укладывается, как правило, несколько пакетов RTCP. При этом общий заголовок отсутствует. Например, типичный пакет транспортного уровня, посылаемый активным участником сессии, содержит следующие пакеты RTCP: пакет SR (содержит информацию об отправленных пакетах), пакет RR (содержит информацию о принятых пакетах), пакет SDES (содержит описание источника).

На рис. 1.10 представлен формат рапорта приемника RR. В поле V (2 бит) указывается версия протокола RTCP, в поле P (1 бит) помещается признак наличия заполнения (Padding), в поле RC (5 бит) записывается число блоков источников, представленных в данном рапорте. В поле тип нагрузки (8 бит) записан PT=201, что показывает тип пакета RR. В поле длина (16 бит) записывается длина пакета (Length) в 32-битных словах за исключением заголовка и заполнителя. В поле, следующим за заголовком указывается идентификатор источника синхронизации, сформировавшего данное сообщение.

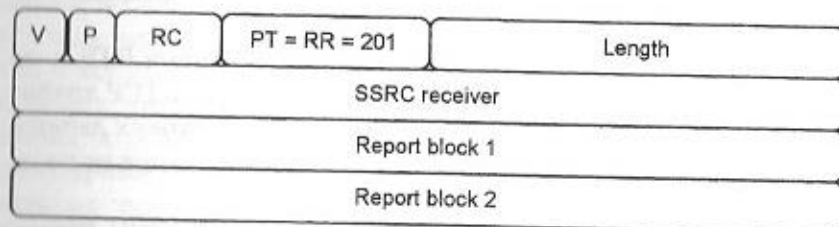


Рисунок 1.10 Формат пакета рапорта приемника

На рис. 1.11 представлен формат блока отчетных данных (Report block).

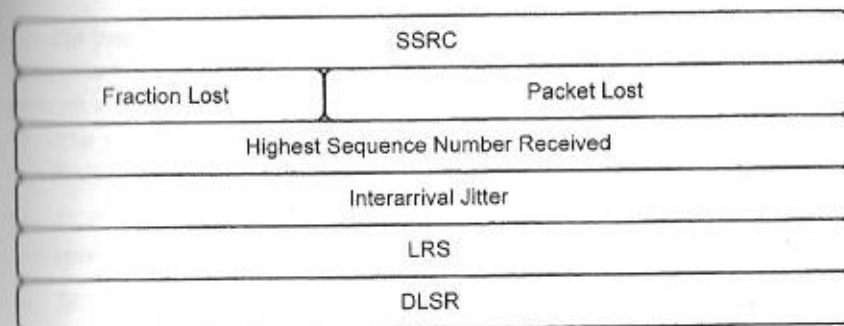


Рисунок 1.11 Формат блока отчетных данных по источнику (Report Block)

В сообщениях SR и RR каждый источник описывается блоком (рис. 1.11), содержащим следующие данные:

- *SSRC* – идентификатор источника синхронизации (идентификатор источника);
- *Fraction Lost* (8 бит) – доля потерянных пакетов данного источника относительно общего числа пакетов;
- *Packet Lost* (24 бит) – общее число потерянных пакетов данного источника;
- *Highest Sequence Number* – максимальный номер пакета, полученного от данного источника;
- *LSR* – старшая часть последнего значения метки времени NTP (Network Time Protocol) TimeStamp, полученного от данного источника;
- *DLSR* – задержка времени от получения последнего сообщения от данного источника до формирования данного блока.

Если SR (Sender Report) посылается источником, который работает, как микшер (т.е. сам получает информацию из нескольких источников и объединяет ее в один поток), то пакет SR содержит следующие части (рис. 1.12):

- *Header* (заголовок) его структура показана более подробно на рис. 1.13.

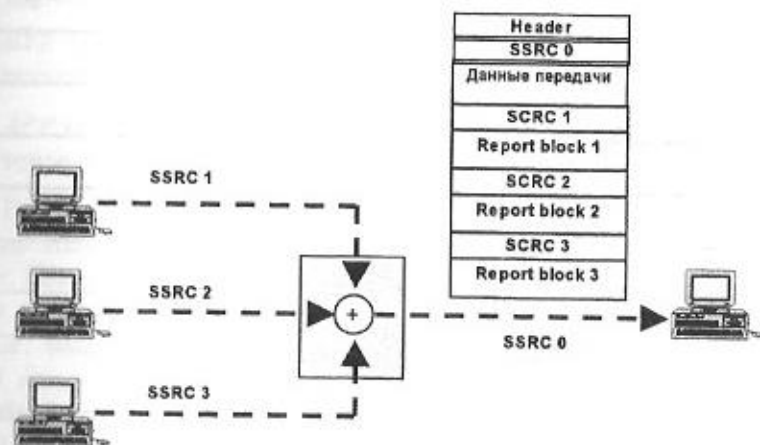


Рисунок 1.12 Формирование общего рапорта отправителя для микшера

Далее следует информация о приеме данных от источников и данные, которые используются для формирования передаваемого потока. Каждый такой источник описывается блоком данных. Каждый блок начинается с SCRC источника.

V	P	RC	PT = RR = 200	Length
SSRC of sender				
NTP timestamp (most significant)				
NTP timestamp (least significant)				
RTP timestamp				
Sender packet count				
Sender octet count				
SSRC 1				
Report block 1				
SSRC 2				
Report block 2				

Рисунок 1.13 Формат пакета отчетных данных отправителя (Sender Report)

На рис. 1.13 представлен формат пакета SR (Sender Report). Он содержит заголовок пакета, статистическую информацию отправителя и собранную статистическую информацию получателя (или группы получателей, если это конференция).

Рассмотрим назначение полей этого пакета:

- *V, P, M* – имеют тоже значение, что и в пакетах протокола RTP (рис. 1.10);
- *RC* (Report Count) – указывает на число рапортов получателей, которые включены в данный пакет;
- *PT* – для пакета рапорта отправителя равно *SR = 200*;
- *Length* – определяет общую длину данного пакета SR, не включая заголовок и заполнение;
- *NTP timestamp* (64 бита) – значение абсолютной метки времени в формате протокола NTP. Значение этого поля вместе с временной меткой в пакете отправителя может быть использовано для расчета RTT;
- *RTP timestamp* – содержит метку относительного времени, сгенерированную протоколом RTP;
- *Sender packet count* – содержит число отправленных пакетов с начала текущей сессии;
- *Sender octet count* – содержит общее число октетов, отправленных с начала сессии;
- *SSRC 1* – содержит идентификатор 1-го источника синхронизации;
- *Report block 1* – информация блока данных по 1-му источнику;
- *SSRC 2* – содержит идентификатор 2-го источника синхронизации;
- *Report block 2* – информация блока данных по 2-му источнику.

За счет пересылки рапортов RR и SR осуществляется обратная связь между получателем и источником. На основе статистических данных этих рапортов отправитель (источник) может принимать решение об изменении текущих параметров сессии. Например,

запросить большую полосу пропускания.

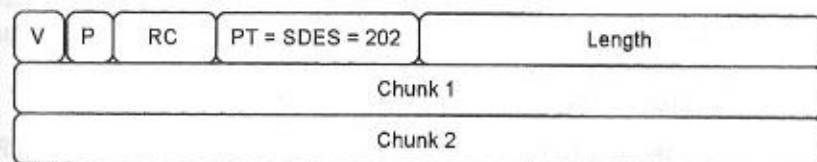


Рисунок 1.14 Формат пакета SDES (Source Description)

Пакет описание источника SDES (рис. 1.14) начинается с заголовка, в котором представлена версия протокола V=2, биты заполнения P, значение числа блоков источников (chunk) RC в данном рапорте, идентификатор типа пакета SDES = 202, общая длина пакета. Далее следуют блоки описания источников.

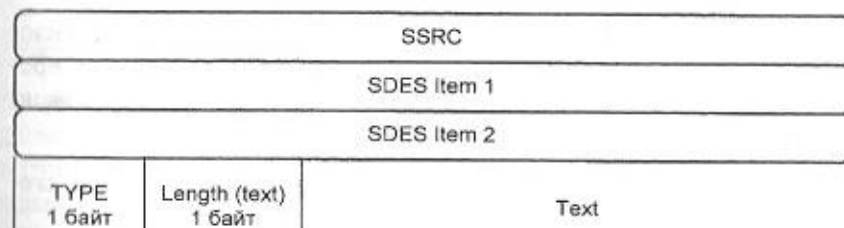


Рисунок 1.15 Формат блока описания источника

Блок описания источника Source Descriptor Block (рис. 1.15) начинается с SSRC источника. Далее следуют элементы описания источников (SDES Item). Каждый блок находится на границе двойного слова. Каждый элемент описания источника начинается с заголовка, состоящего из типа TYPE (1байт) (см. табл. 1.3), длины в байтах Length (1 байт), далее следует текст элемента. Длина относится к тексту.

Обычно CNAME имеет следующий формат: user@host, где user – имя пользователя, host – идентификатор хоста (доменное имя или IP-адрес в стандартном ASCII-представлении). Если по каким-либо причинам имя пользователя оказывается недоступным, то используется CNAME в формате host. Пример: dwarf@sleepy.beauty.com или dwarf@192.166.148.9. CNAME является единственным обязательным элементом описания источника.

Таблица 1.3

Типы кодов описаний источника

Аббревиатура	Тип	Описание
END	0	признак конца последовательности элементов описания источника
CNAME	1	каноническое имя источника
NAME	2	общее имя источника, задается в произвольной форме
EMAIL	3	E-mail источника
PHONE	4	телефонный номер источника
LOC (location)	5	информация о географическом положении источника
TOOL	6	информация о программных средствах, используемых источником
NOTE	7	дополнительная информация, связанная с источником
PRIV (private)	8	дополнительный элемент, использование которого имеет предварительный характер

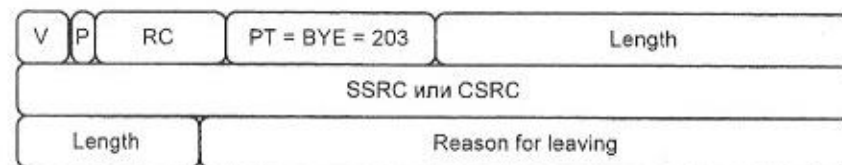


Рисунок 1.16 Формат пакета завершения сессии BYE

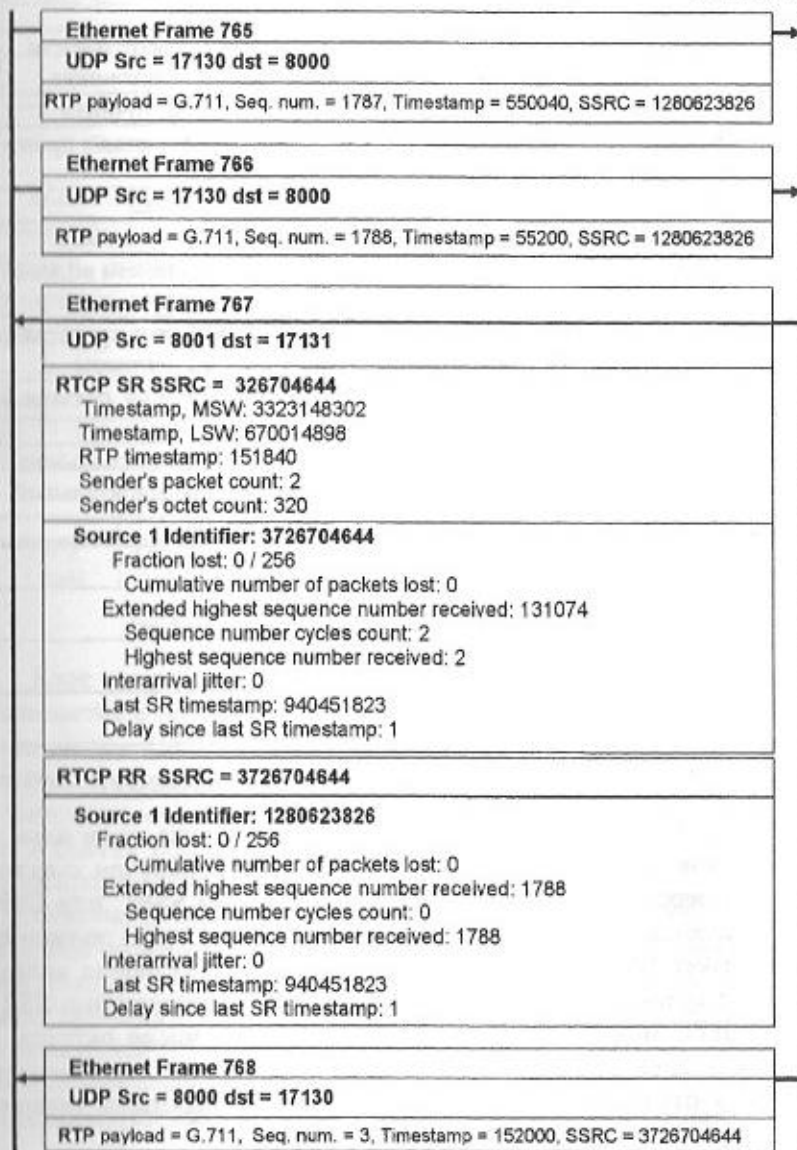
Пакет BYE (рис. 1.16) передается в том случае, если один из участников покидает сессию. Если пакет BYE получен смесителем, он передает этот пакет с идентификатором SSRC или CSRC без изменений. Если смеситель отключается сам, то он должен послать пакет BYE, перечислив все источники, вносящие вклад в поток, с которым он работал, а также свой идентификатор SSRC. Пакет BYE может также содержать 8-битовое число октетов, за которым следует текст соответствующей длины, поясняющий причину отключения. Например, «камера не работает» («camera malfunction»).

На временной диаграмме (рис. 1.17) показано, что обмен RTP

и RTCP пакетами производится между двумя терминалами с IP-адресами 217.10.67.6 и 192.168.1.42.

217.10.67.6

192.168.1.42



217.10.67.6

192.168.1.42

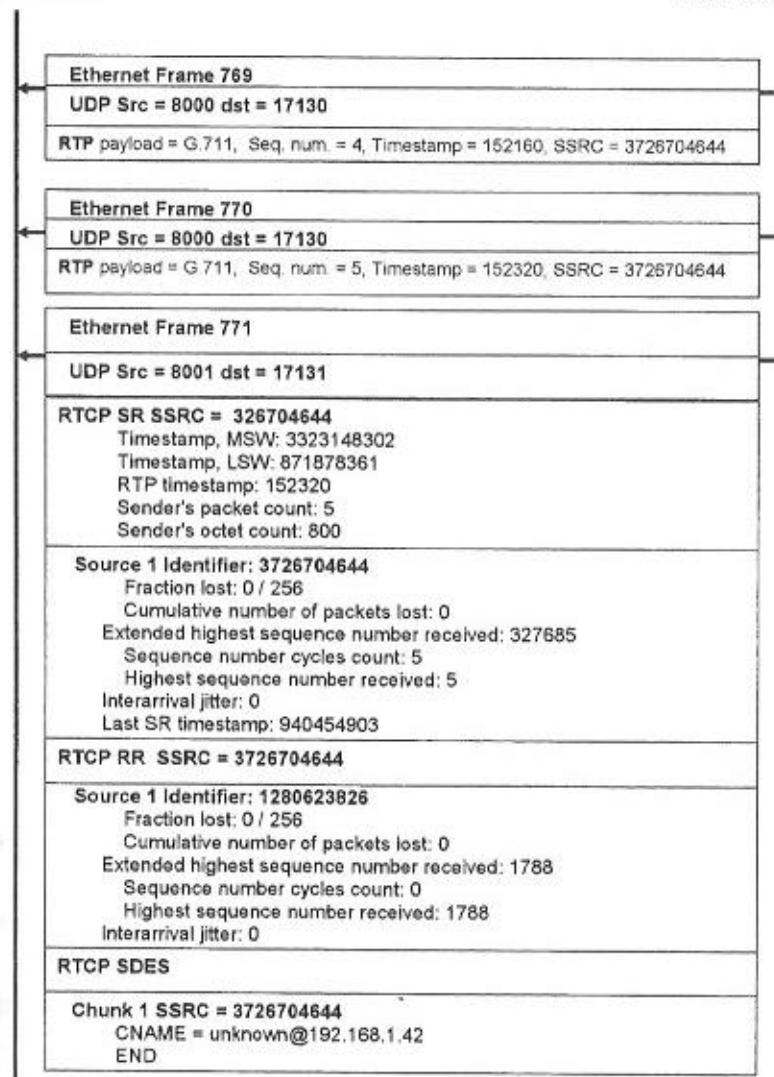


Рисунок 1.17 Трасса обмена пакетами RTP и RTCP

Для протокола RTP используются порты 17130 и 8000 соответственно, для протокола RTCP порты с номерами 17131 и 8001. После обмена очередными пакетами RTP (кадры 765 и 766) передаст-

ся кадр 767, который содержит 2 пакета RTCP: рапорт SR от источника SSRC = 326704644 и рапорт RR о приеме от источника SSRC = 1280623826. Рапорты содержат статистические данные по итогам обмена пакетами за период от начала сессии до момента формирования рапорта. Содержание рапортов предлагается изучить читателям самостоятельно, используя описание форматов рапортов, приведенное выше. После передачи следующих 3 пакетов RTP (кадры 769-770) происходит передача пакетов SR и RR, а также пакета описания источника SDP.

В настоящее время разработана расширенная версия протокола RTCP XR, описанная в RFC 3611. В ней увеличено число параметров, по которым собираются статистические данные. Наиболее значимыми дополнительными параметрами являются:

- доля сброшенных пакетов из-за переполнения буфера (Discard Rate);
- интенсивность и длительность вспышки трафика (Burst density/duration);
- интенсивность и продолжительность пауз (низкого уровня поступления пакетов Gap density/duration);
- задержка передачи пакета «туда и обратно» (Round Trip Delay);
- уровень сигнала (Signal Level) и уровень шума (Noise Level);
- экспертная оценка качества слушающим MOS-LQ (Estimated Mean Opinion Score for Listening Quality);
- экспертная оценка качества тракта MOS-CQ (Estimated Mean Opinion Score for Conversational Quality);
- номинальная задержка в анти-джиттерном буфере (Jitter Buffer Nominal Delay);
- максимальная задержка в анти-джиттерном буфере (зафиксированная) (Jitter Buffer Maximum).

Таким образом, расширенная версия протокола RTCP позволяет получить значительно больший перечень характеристик качест-

ва передачи в текущей сессии.

Протоколы RTP/RTCP являются универсальным механизмом передачи аудио- и видеоинформации через IP-сети. Для установления RTP-сессий используются протоколы сигнализации H.323 и SIP, которые будут подробно рассмотрены в следующих главах.

Контрольные вопросы и задания

1. Сравните типы терминалов VoIP по функциональным возможностям.
2. Рассчитайте размер IP-пакетов, используемых для передачи речи кодеками G.711 G.729, G.723.1 с учетом размеров заголовков RTP/UDP/IP/Eth.
3. Рассчитайте число переданных пакетов с момента начала сессии (рис. 1.8), если в последнем пакете параметр Time= 43040.
4. Перечислите параметры, которые могут быть определены по данным пакета RR протокола RTCP.
5. По трассе на рис. 1.17 определите идентификаторы SSRC для каждого терминала, определите число пакетов, переданных с каждой стороны, число потерянных пакетов, значение джиттера.

Глава 2. ПРОТОКОЛ H.323

2.1 Архитектура сети H.323

Первым протоколом, регламентирующим построение сетей VoIP, была Рекомендация H.323, которая разрабатывалась как средство поддержки мультимедийных конференций в пакетных сетях. Сети по Рекомендации H.323 ориентировались на интеграцию с ТфОП. Поэтому не удивительно, что в основу сигнализации был положен протокол Q.931, обеспечивающий передачу сигнальных сообщений в сетях ЦСИС. Рекомендация H.323 является зонтичной, то есть включает группу протоколов, которые можно разделить на:

- протокол регистрации и запроса разрешения на установление соединения RAS;
- протокол установления и разъединения соединений (H.225.0);
- протокол управления логическими каналами (H.245).

В Рекомендации H.323 также описана сетевая архитектура (рис. 2.1) и перечень сетевых элементов.

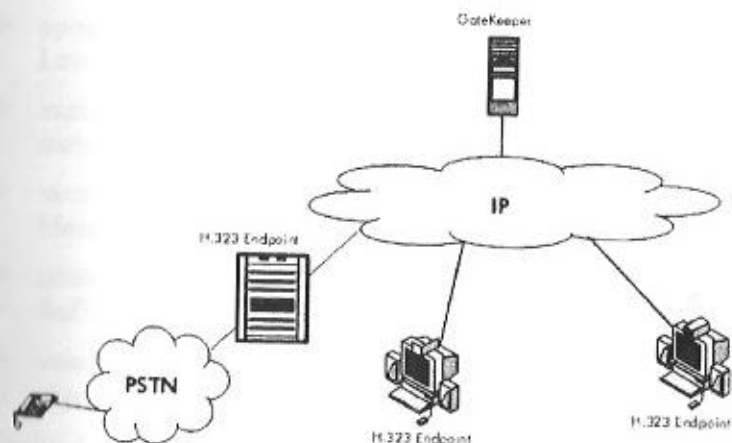


Рисунок 2.1 Архитектура сети по Рекомендации H.323

Терминалом H.323 называется оконечное оборудование пользователя, которое обеспечивает передачу аудио и видео потоков и тестовых сообщений и полностью соответствует Рекомендации H.323. В тех случаях, когда абоненту не требуется передача видеоизображений, используется упрощенный аудио терминал, который реализует функции передачи голоса через IP-сеть и совместим с другими элементами сети H.323.

Шлюз H.323 (Gateway) предназначен для сопряжения сети VoIP с ТфОП. Для этого, шлюз обеспечивает преобразование поступающего из телефонной сети непрерывного голосового потока в поток пакетов по стеку RTP/UDP/IP. Шлюз также обеспечивает прием сигнальных сообщений из телефонной сети (ЦАС№1, ОКС №7) и осуществляет установление соединений в пакетной сети по протоколу H.225.0.

Устройство управления конференциями MCU (Multipoint Control Unit) предназначено для осуществления централизованной конференцсвязи. При этом устройство управления контролирует процесс создания конференции, подключение новых участников, микширование аудио и видео потоков, а также процесс разрушения конференции.

Призрачник (Gatekeeper) – это основное устройство управления сети H.323, которое выполняет следующие функции:

- преобразует альтернативный (alias) адрес в транспортный адрес вызываемого (IP-адрес назначения + UDP порт);
- контролирует права доступа вызывающего;
- обеспечивает маршрутизацию сигнальных сообщений между терминалами в своей зоне.

Три первых перечисленных устройства играют роль оконечных точек (Endpoint) соединения в протоколе H.323.

2.2 Адресация в H.323

Каждое сетевое устройство сети H.323 должно иметь, по крайней мере, один IP-адрес. Для организации каналов сигнализации, управления и передачи медиапотоков используются транспортные адреса TSAP (Transport Service Application Point). Все

оконечные устройства имеют фиксированные адреса TSAP для канала сигнализации. Привратники (контроллеры зоны) имеют известные транспортные адреса режима регистрации (RAS) и для режима поиска привратника.

Оконечное оборудование H.323 может иметь один или несколько альтернативных (alias) адресов. По формату эти адреса соответствуют адресу E-mail. Обычно в первой части адреса указывается идентификатор пользователя, а во второй – имя домена, в котором расположен терминал. Соответствие между альтернативными и сетевыми адресами выполняется при помощи трансляционной таблицы, которая создается и хранится в привратнике.

2.3 Структура Рекомендации H.323

Рекомендация H.323 включает целую группу протоколов, объединенных общей задачей поддержки аудио- и видеоконференции через пакетную сеть.

Аудио		Видео		Управление терминалом и установление сессий		Передача данных
G.711 G.722 G.728 G.729	H.261 H.262 H.263	RTCP	RAS H.225	H.225.0 Q.931(Call Signaling - сигнализация)	H.245 (Call Control - Управл. вызовом)	T.125
RTP				X.225 (Class 0)		T.125
UDP				TCP		T.123
IP						
Канальный уровень						
Физический уровень						

Рисунок 2.2 Стеки протоколов по Рекомендации H.323

Как видно из рис. 2.2, передача аудио и видео потоков производится по уже известному стеку G.xxx/RTP/UDP/IP, H/xxx/RTP/UDP/IP. Естественно контроль текущих параметров сессии и сбор статистики выполняется протоколом RTCP.

Процесс взаимодействия оконечных устройств с привратником определяется протоколом H.225 RAS (Registration, Admission, Status).

Процесс установления и разъединения речевых соединений через IP-сеть регламентируется протоколом H.225.0, который использует сокращенный набор сигнальных сообщений протокола Q.931.

Процесс управления информационными (медиа) каналами регулируется протоколом H.245, который определяет ведущего и ведомого в сессии, обеспечивает согласование функциональных возможностей терминалов, управляет работой логических каналов.

Протокол RAS предусматривает два режима работы терминала с привратником: *ручной* и *автоматический*.

При ручном режиме адрес привратника задается в процессе конфигурации терминала.

При автоматическом режиме терминал передает запрос GRQ (Gatekeeper Request) на поиск привратника в режиме многоадресной рассылки (IP-адрес 224.0.1.14 и номер UDP-порта 1718 – подробнее в [1]). В ответ на этот запрос привратник посылает сообщение GCF (Gatekeeper Confirmation), в котором сообщает терминалу свой адрес и номер UDP-порта (обычно 1719). Получив эту информацию, терминал проводит процедуру регистрации, посылая запрос RRQ (Registration Request) к привратнику. Если процедура регистрации проходит успешно, в ответ терминал получает сообщение RCF (Registration Confirmation).

Перед началом соединения терминал посылает привратнику запрос ARQ (Admission Request), в котором указывает идентификатор вызываемого терминала (alias) и требование по скорости приема и передачи информации в будущем соединении. Если привратник может обеспечить заявленные требования, то отвечает терминалу сообщением ACF (Admission Confirm), в котором указывает номер TCP-порта для установления сигнального канала (Q.931) с привратником. Терминал устанавливает TCP-соединение с привратником (SYN-ACK-SYN/ACK), по которому будет передаваться сигнальная информация протокола H.225.0 (Q.931).

Процедура управлением соединения регламентирована Рекомендацией H.225.0, которая базируется на использовании усеченной версии протокола сигнализации ЦСИС – Q.931.

Из всего списка сигнальных сообщений Q.931 разрешено использовать только следующие сообщения:

- *SETUP* (Установить);
- *CALL PROCEEDING* (Соединение устанавливается);
- *ALERTING* (Контроль посылки вызова),
- *CONNECT* (Соединить);
- *RELEASE COMPLETE* (Освобождение завершено);
- *FACILITY* (Дополнительная услуга).

В соответствии с Рекомендацией Q.931, каждое сигнальное сообщение содержит заголовок и набор информационных элементов, значения которых определяют параметры будущего голосового соединения. В заголовке сигнального сообщения указывается, что сообщение составлено по протоколу Q.931, от кого оно поступило (от инициатора соединения или в ответ), порядковый номер вызова и тип сообщения.

Например, сигнальное сообщение *SETUP* (рис. 2.3) содержит следующие информационные элементы:

- возможности передачи BC (Bearer Capability);
- номер вызываемой стороны CdPN (Called Party Number);
- номер вызывающей стороны ClPN (Calling Party Number);
- информацию между пользователями UUI (User-user Information).

В заголовке рассматриваемого сигнального сообщения указано, что:

- оно составлено в соответствии с протоколом Q.931;
- длина поля указателя вызова равна двум октетам;
- сообщение передано от инициатора соединения;
- порядковый номер вызова 1000;
- тип сигнального сообщения *SETUP*.

```
Internet Protocol, Src: 10.16.64.6, Dst: 10.16.64.1
Transmission Control Protocol, Src Port: 1117, Dst Port: 1721 (Seq: 1,
Ack: 1)
Q.931
Protocol discriminator: Q.931
Call reference value length: 2
Call reference flag: Message sent from originating side
Call reference value: 1000
Message type: SETUP
Bearer capability: Coding standard: ITU-T
Information transfer capability: Unrestricted digital information
Transfer mode: Packet mode
User info layer 1 protocol: H.221 and H.242
Calling party number: '6'
Called party number: '5'
User-User
Protocol discriminator: X.208 and X.209 coded user information
H.225.0 CS
H.323_UserInformation
H323-message-body: setup
H245Tunneling: true
H245Control: request: terminalCapabilitySet
capabilityTable: 3 items
Item 0
receiveAudioCapability: g711Ulaw64k
Item 1
receiveAudioCapability: g711Alaw64k
Item 2
receiveAudioCapability: gsmFullRate
H245 request: masterSlaveDetermination
statusDeterminationNumber: 22981
```

Рисунок 2.3 Содержание сигнального сообщения *SETUP*

Информационный элемент «Возможности передачи» (BC) содержит информацию о возможностях передачи для данного вызова:

- стандарт кодирования – МСЭ-T;
- возможности передачи – неограниченная цифровая;

- режим – коммутация пакетов;
- информация пользователя на 1-ом уровне – по Рекомендациям H.221 и H.242.

Информационные элементы CdPN («5») и CIPN («6») содержат информацию об используемом плане нумерации и цифры передаваемого номера. Информационный элемент UUI содержит данные, которыми обмениваются непосредственно терминалы. В данном случае этот информационный элемент сформирован в соответствии с требованиями Рекомендации H.323, включен в состав сигнального сообщения SETUP, и содержит информацию протокола H.245. Эта информация является запросом на выбор типа кодека (terminal Capability Set) TCS и содержит список из поддерживаемых терминалом 3-х кодексов (capability Table): 0 – G.711 μ -закон, 1 – G.711 A-закон, 2 – GSM full rate (кодек, используемый в сетях GSM).

Рассматриваемый информационный элемент также содержит запрос на определение «Ведущий – ведомый» (master Slave Determination - MSD), в котором указано случайное число обозначения (status Determination Number) – 22981. Оно будет использовано в процедуре MSD.

Общий алгоритм установления соединения по протоколу H.225.0 предполагает обмен следующими сигнальными сообщениями:

1. Терминал посылает сообщение SETUP (BC, CdPN, CIPN, UUI), которое содержит необходимую информацию для установления соединения.
2. Привратник может ответить на это сообщением CALL PROCEEDING, указывающим, что вся необходимая информация им получена.
3. Привратник пересылает SETUP к вызываемому терминалу.
4. Вызываемый терминал принимает вызов и отвечает сообщением ALERTING, пересылаемым вызывающему терминалу, который генерирует сигнал КГВ.
5. После того, как пользователь принимает вызов, его терминал посылает сообщение CONNECT.

6. Вызов переходит в разговорную фазу и завершается любым из терминалов после отправки сообщения Release Complete.

Процедура управления информационными (логическими) каналами выполняется в соответствии с Рекомендацией H.245. Для передачи сообщений протокола H.245 может использоваться отдельный управляющий канал или эти сообщения могут включаться в сигнальные сообщения Q.931 в составе информационного элемента UUI (как на рис. 2.3). Поскольку чаще используется именно второй вариант, то остановимся именно на этом способе.

Протокол H.245 предполагает выполнение следующих действий:

- определение ведущего и ведомого оборудования MSD (master-Slave Determination);
- согласование функциональных возможностей оборудования TCS (Terminal Capability Set);
- открытие информационных (логических) каналов OLC (open Logical Channel).

Ведущим или ведомым в процессе открытия двунаправленного информационного канала может быть любой из терминалов. В процессе согласования терминалы вырабатывают и обмениваются случайными числами. Терминал, сгенерировавший большое число становится ведущим.

Обычно терминалы VoIP способны поддерживать несколько кодексов (см. табл. 1.1). Поэтому, в ходе согласования режимов работы исходящий терминал передаст полный список своих кодексов для передачи речи и видеоизображений TCS. В ответном сообщении входящий терминал указывает свой список поддерживаемых кодексов TCS и выбранный для данного соединения кодек. Исходящий терминал подтверждает выбор кодека.

Информация передается по RTP-сессиям непосредственно между двумя терминалами. Поэтому, на этапе открытия логических каналов оба терминала должны обладать информацией, необходимой для открытия RTP-сессии: IP-адреса терминалов и номера выбранных UDP-портов.

Временная диаграмма процесса установления и разъединения соединения представлена на рис. 2.4.

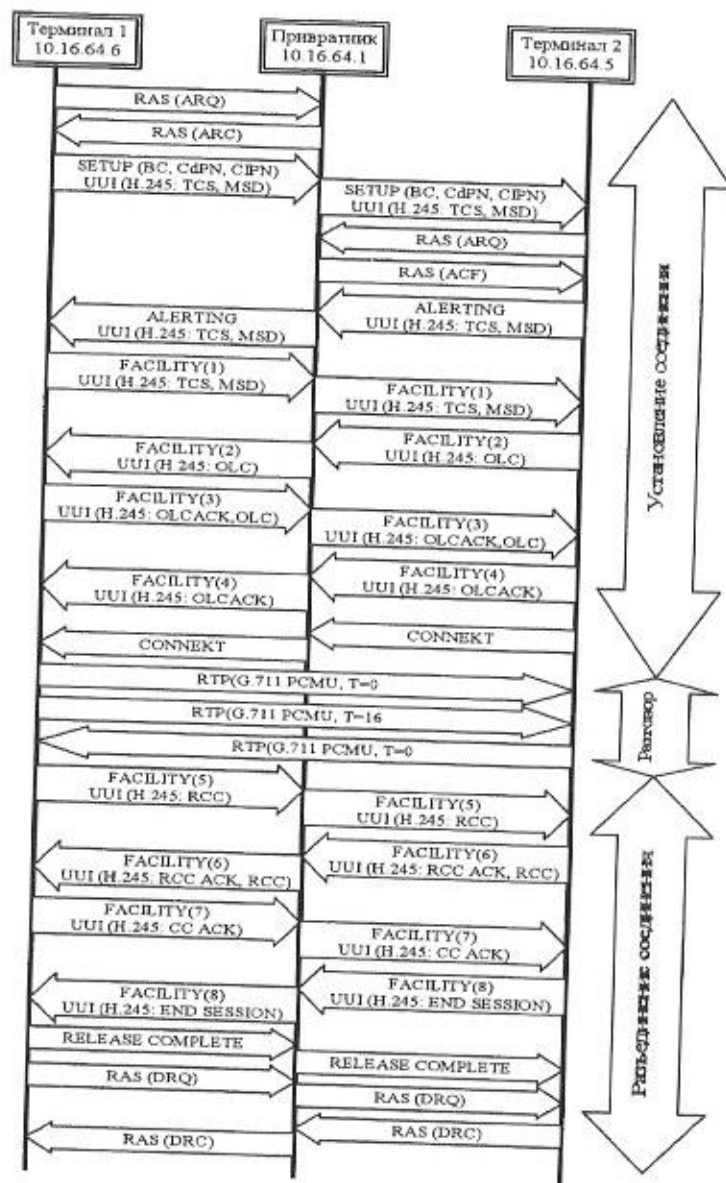


Рисунок 2.4 Временная диаграмма процесса установления и разъединения соединения VoIP под управлением привратника

Сценарий вызова начинается с отправки вызывающим терминалом запроса ARQ к своему привратнику с указанием имени вызываемого пользователя (dialed Digits: 5) и требуемой пропускной способности будущего соединения. В ответ привратник передает подтверждение ACF с указанием номера TCP-порта для будущего сигнального канала.

Вызывающий терминал устанавливает TCP-соединение по указанному номеру порта и передает сообщение SETUP, включающее информационные элементы: BC, CdPN, CIPN, UII 1. Последний информационный элемент содержит таблицу ко덉ов TCS, параметры MSD. Это сообщение привратник пересылает к вызываемому терминалу.

Терминал, проверив соответствие своих возможностей полученным параметрам, подтверждает прием вызова сообщением ALERTING, которое содержит список поддерживаемых ко덉ов TCS и тип выбранного кодака.

Вызывающий терминал, получив сообщение ALERTING, генерирует сигнал КПВ (контроль отправки вызова) и отвечает сообщением FACILITY 1, которое содержит подтверждение выбранного кодака и установление режима работы (Master/Slave).

Вызванный терминал посылает следующее сообщение FACILITY 2, которое содержит запрос на открытие логического управляющего канала RTCP с указанием IP-адреса терминала и зарезервированного UDP-порта. В ответ вызывающий терминал посылает сообщение FACILITY 3, которое содержит данные по логическому управляющему каналу со стороны вызывающего терминала (IP-адрес и UDP-порт).

Вызываемый терминал посылает в ответ сообщение FACILITY 4. Оно содержит данные по RTP и RTCP сессиям (IP-адрес терминала и номер UDP-порта для RTP-сессии, который всегда является четным числом на единицу меньшим, чем номер UDP-порта для RTCP-сессии).

Вызывающий терминал посылает сообщение CONNECT. Между двумя терминалами открывается RTP-сессия, которая контролируется RTCP.

Первым завершает сессию вызывающий терминал, посылая сообщение FACILITY 5, которое содержит запрос на закрытие логического канала RCC (request Channel Close). В ответе FACILITY

6 вызываемый терминал подтверждает закрытие логического канала RCC ACK и запрашивает закрытие логического канала со своей стороны.

Вызывающий терминал в сообщении FACILITY 7 посылает подтверждение закрытия логического канала со своей стороны (CC ACK) и команду закрытия сессии Disconnect (протокол H.245). Вызываемый терминал в сообщении FACILITY 8 подтверждает завершение сессии.

После чего, вызывающий терминал посылает сигнальное сообщение RELEASE COMPLETE. Далее вызывающий терминал закрывает TCP-соединение путем обмена пакетами FIN/ACK и ACK.

Теперь с помощью сообщения DRQ (Disengage Request) происходит извещение привратника об освобождении ресурсов завершеного соединения. Привратник подтверждает освобождение полосы пропускания сообщением DCF (Disengage Confirm) протокола RAS.

В приложении 1 представлена сокращенная трассировка процессов установления, обмена и разъединения соединения VoIP между двумя терминалами H.323, выполненная под управлением привратника. Читателям предлагается самостоятельно прочитать трассу, снятую при помощи сниффера Ethereal (Wire Shark). Трасса записана на стороне вызывающего терминала, поэтому представлены только сообщения между терминалом «б» и привратником. В целях сокращения занимаемого рисунком места, из трассы исключена информация канального уровня (описание Ethernet – кадров), а также информация, являющаяся излишней для понимания процессов установления и разъединения соединений.

2.4 Комментарий по чтению трассировок

Запись трассы осуществляется программой – сниффером WireShark на уровне принимаемых кадров Ethernet.

Каждая запись начинается с номера записанного кадра.

Информация кадров Ethernet исключена из трассировки для сокращения места.

Информация IP-уровня сведена до адреса источника (Src) и адреса назначения (Dst).

Информация протоколов транспортного уровня содержит название протокола (UDP, TCP) и номера используемых портов (Source Port, Destination Port).

Для TCP-сегментов также указываются флаги (SYN, ACK) и приводится значение полей числа переданных (Seq) и принятых (Ack) октетов.

Далее в трассировке указывается тип протокола, в соответствии с которым сформировано содержание пакета. Следовательно, при чтении трассировки для уточнения деталей можно обращаться к описанию указанного протокола. В большинстве случаев значения приведенных параметров интуитивно понятны.

В результате анализа трассы читатели должны ответить на контрольные вопросы.

Контрольные вопросы и задания

1. Объясните разницу в функциях протоколов H.225.0 (Q.931) и H.245 в процессах установления и разъединения соединений между терминалами H.323.
2. Определите номера кадров начала и завершения TCP-сессии между вызывающим терминалом и привратником.
3. Определите значения идентификаторов вызова, представленного на рис. 2.4, на уровне протоколов RAS, H.225.0 (Q.931) и H.245.
4. Укажите сигнальное сообщение, после которого между терминалами открывается RTP-сессия.
5. С какого сигнального сообщения начинается процесс разъединения?

Глава 3. ПРОТОКОЛ ИНИЦИАЦИИ СЕССИЙ SIP

3.1 Структура протокола SIP

Протокол инициации сессий SIP (Session Initiation Protocol) был разработан группой MMUSIC (Multiparty Multimedia Session Control) и описан в RFC 2543. Также как и протокол H.323, SIP был создан для управления аудио- и видеоконференциями и входит в стек протоколов, обеспечивающих передачу мультимедийных сеансов.

Протокол SIP предназначен для организации, модификации и завершения мультимедийных конференций. При этом передачи информации, контроль качества обслуживания и другие функции возложены на разные протоколы, входящие в стек протоколов, который иногда называют по имени основного сигнального протокола SIP.

Стек протоколов поддержки мультимедийных сеансов представлен на рис 3.1.

Управление конференцией		Аудио и видео		Установление сессии	
RSVP	SCCP	RTP	RTCP	SDP	HTTP
				SIP	RTSP
	UDP			TCP	
IP					

Рисунок 3.1 Стек протоколов поддержки мультимедийных сеансов

Передача аудио- и видеoinформации выполняется при помощи известных протоколов RTP/RTCP. Управление конференциями осуществляется протоколом SCCP (Simple Conference Control Protocol). При резервировании пропускной способности каналов для конференции может использоваться протокол RSVP. Собственно SIP выполняет функции установления, поддержки и разъединения сессий, то есть является сигнальным протоколом. Вся информация по характеристикам устанавливаемой сессии определяется прото-

колом SDP (Session Description Protocol), данные которого вкладываются в сообщения SIP. Кроме информации протокола SDP в сообщения SIP могут вкладываться данные и других протоколов, например ISUP. Как видно из рис. 3.1, протокол SIP может использоваться в качестве транспорта как стек протоколов UDP/IP, так и стек TCP/IP. Однако, на практике стек TCP/IP обычно не используется.

Протокол SIP является текстовым протоколом, использующим синтаксис и структуру протокола HTTP. Протокол SIP построен по принципу «клиент – сервер». Клиент посылает запросы на сервер, в которых указывает, что он хочет получить от сервера. Сервер обрабатывает запросы и выдает ответы, которые могут содержать успешные результаты обработки или сообщения о сбоях и ошибках.

Основным сетевым элементом, обеспечивающим управление соединением, является терминал, который выполняет функции агента пользователя UA (User Agent). Программное обеспечение UA имеет клиентскую и серверную части, которые также размещаются в терминале. Сервера в архитектуре SIP (SIP server) отвечают за маршрутизацию вызовов и предоставление дополнительных услуг. В зависимости от своего назначения, различают несколько типов серверов SIP:

- *прокси-сервер* (Proxy server) – обеспечивает взаимодействие с терминалами;
- *сервер определения месторасположения* (Registrar server или Location Server) – обеспечивает определение текущего адреса вызываемого абонента;
- *сервер переадресации* (Redirect server) – обеспечивает переадресацию вызова на текущий адрес вызываемого абонента.

3.2 Сообщения SIP

Все сообщения SIP представляют собой последовательности текстовых строк (RFC 2279), организованных в следующую структуру:

1. стартовая строка сообщения;
2. заголовки (общие, содержания, запросов/ответов);
3. содержание сообщения (тело).

В протоколе SIP определено шесть типов запросов. Тип запроса указывается терминалом в стартовой строке.

Запрос *REGISTER* посылается для указания своего текущего месторасположения, новой адресной информации и продолжительность регистрации.

Запрос *INVITE* приглашает вызываемого пользователя участвовать в сеансе связи, а также содержит SIP-адрес вызываемого пользователя и описание сеанса.

Запрос *ACK* подтверждает прием ответа на запрос *INVITE* и содержит окончательное (согласованное) описание сеанса связи.

Запрос *BYE* посылается оборудованием терминала, который хочет завершить сеанс связи. Терминал, получивший *BYE* должен прекратить передачу информации и подтвердить свои действия ответом.

Запрос *CANCEL* отменяет обработку ранее переданных запросов с указанными идентификаторами.

Запрос *OPTIONS* посылается для получения информации о возможностях терминального оборудования вызываемого пользователя.

Все ответы делятся на *информационные* и *окончательные* (финальные).

Информационные ответы кодируются трехзначным числом из второй и третьей сотни 1xx. Информационные ответы переносят сообщения о выполняемых в настоящий момент действиях, например 100 Trying – процесс установления сеанса продолжается, 180 Ringing – КГВ.

Ответы 2xx означают, что запрошенное действие успешно выполнено.

Ответы 3xx информируют вызывающего пользователя о перемещении вызываемого пользователя. Например, 302 Moved Temporarily – пользователь временно находится по другому адресу.

Ответы 4xx информируют о наличии ошибки в полученном запросе. Например, 402 Unauthorized – означает необходимость

проведения процедуры аутентификации.

Ответы 5xx информируют о невозможности выполнения запроса из-за отказа сервера. Например, 503 Service Unavailable – служба недоступна.

Ответы 6xx информируют о невозможности связи с вызываемым пользователем. Например, 600 Busy Everywhere – вызываемый абонент занят.

В качестве адресов в SIP используются универсальные указатели ресурсов – URL (Universal Resource Locators) – SIP URL.

SIP-адреса бывают 4-х типов:

- Имя @ домен;
- Имя @ хост;
- Имя @ IP – адрес;
- N телефона @ шлюз.

Таким образом, адрес состоит из 2-х частей. Первая включает имя пользователя или номер телефона. Вторая указывает имя домена, хоста или шлюза.

Примеры SIP-адресов:

SIP: asa@mtuci.ru

SIP: victor@192.168.0.3

SIP: 1886229@sipgate.de

3.3 Сценарий установления соединения

Рассмотрим алгоритм установления сессии через 2 прокси-сервера, каждый из которых обслуживает свою группу пользователей. В качестве начальных условий положим, что терминал 1 зарегистрирован на SIP-сервере 1, а терминал 2 – на SIP-сервере 2.

1. Перед началом сессии терминал 2 должен быть зарегистрирован на Proxy сервере (запрос REGISTER).
2. Терминал 1 посылает запрос INVITE к своему SIP-серверу.
3. SIP-сервер 1 отвечает сообщением 100 TRYING.
4. SIP-сервер 1 пересылает запрос INVITE SIP-серверу 2.

5. SIP-сервер 2 отвечает сообщением 100 TRYING.
6. SIP-сервер 2 посылает запрос INVITE терминалу 2.

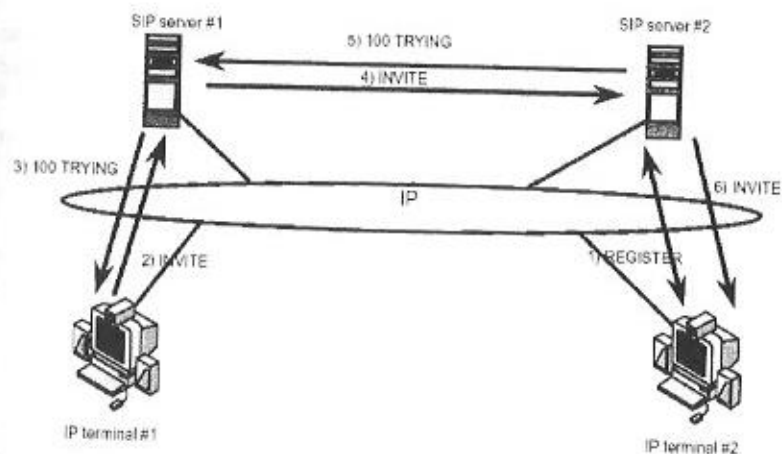


Рисунок 3.2 Сценарий установления сессии (часть 1)

7. Терминал 2 отвечает сообщением 180 RINGING.
8. SIP-сервер 2 пересылает сообщение 180 RINGING SIP-серверу 1.
9. SIP-сервер 1 пересылает сообщение 180 RINGING терминалу 1.
10. Терминал 2 отвечает SIP-серверу 2 сообщением 200 OK.
11. SIP-сервер 2 пересылает сообщение 200 OK к SIP-серверу 1.
12. SIP-сервер 1 пересылает сообщение 200 OK терминалу 1.
13. Терминал 1 отвечает SIP серверу 1 сообщением ACK.
14. SIP-сервер 1 пересылает это сообщение SIP серверу 2.
15. SIP-сервер 2 пересылает это сообщение терминалу 2.
16. Между терминалами устанавливается сессия (RTP/RTCP).

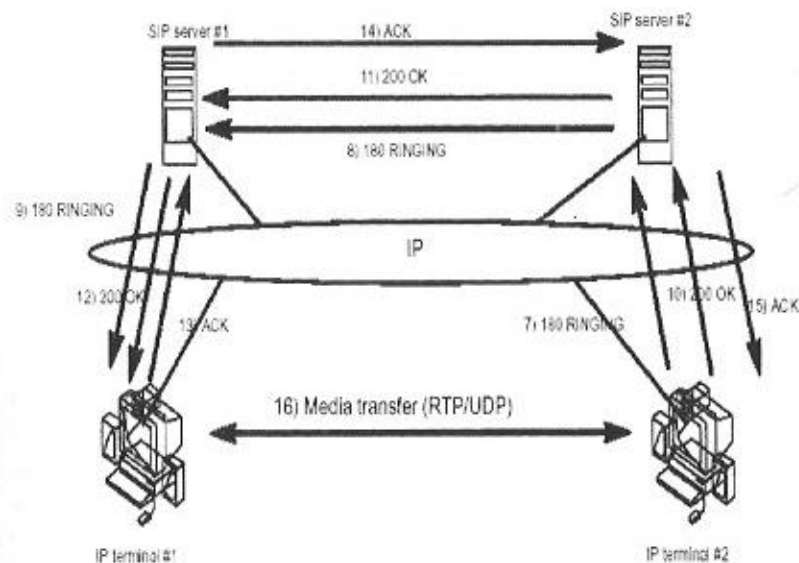


Рисунок 3.2 Сценарий установления сессии (часть 2)

После окончания разговорной фазы терминал 1 посылает запрос BYE, который транслируется прокси-серверами к терминалу 2. Терминал 2 посылает ответ 200 OK, после чего терминалы возвращаются в исходное состояние.

3.4 Формат сообщений SIP

Рассмотрим подробнее структуру SIP запросов и ответов.

	Запрос	Ответ
Стартовая строка	Request-Line	Status-Line
Заголовок сообщения	Поля: Via, From, To	
Пусковая строка(CRLF)		
Содержимое сообщения	Формируется протоколами SDP, ISUP ...	

Рисунок 3.3 Структура сообщения SIP

Каждое сообщение SIP (запрос или ответ) начинается со стартовой строки. Если сообщение является запросом, то в стартовой строке (Request-Line) указываются: тип запроса, адресат и номер версии протокола SIP. В стартовой строке ответа (Status-Line) указываются: номер версии протокола SIP, тип ответа и краткая расшифровка действий.

Заголовок сообщения содержит достаточно много полей, которые будут расшифрованы позже.

Пустая строка CLRF отделяет заголовок SIP сообщения от содержания, которое включает информацию по описанию будущей сессии при помощи протоколов SDP, ISUP...

В заголовке сообщения SIP размещаются следующие поля: Via (Через), From (От), To (Кому), Contact (Контакт), Call ID (Идентификатор вызова), Cseq (Номер запроса), Authorization (Авторизация), Max-Forwards (Макс. переадресаций), User Agent (Агент пользователя), Content Type (Тип содержимого) и Content-Length (Длина содержимого).

Поле Via содержит информацию о маршруте: при прохождении каждого прокси-сервера его адрес записывается в этом поле. Таким образом, в поле Via будет записан весь пройденный маршрут. Это дает возможность отправить ответ по тому же пути. Параметр branch означает, что на данном сервере запрос был размножен и передан по указанному направлению.

В поле From указывается адрес вызывающего пользователя. Кроме адреса здесь же указывается параметр tag для идентификации конкретного терминала пользователя.

В поле To указывается SIP-адрес вызываемого пользователя.

В поле Contact помещается SIP-адрес пользователя, по которому с ним можно установить контакт.

В поле Call ID помещается уникальный идентификатор сеанса связи, состоящий из буквенно-цифрового идентификатора и имени терминала, который присвоил этот идентификатор (например, 5CC933F2BAD5802@pc.alcatel.be).

В поле CSeq записывается уникальный идентификатор запроса, относящегося к данному соединению.

В поле Authorization записываются параметры, используемые при авторизации. Параметр Digest описывает метод авторизации по HTTP. Параметр Nonce включает случайное криптографическое

число, realm – содержит имя домена и т.д.

В поле Max-Forwards указывается максимальное число переадресаций. Используется для предотвращения петель.

В поле User Agent указывается тип терминала.

В поле Content Type указывается тип передаваемой информации.

В поле Content-Length указывается длина содержимого в октетах.

Рассмотрим конкретный пример записи сообщения Register, представленный на рис. 3.4.

Request-Line: REGISTER sip:sipgate.de SIP/2.0 Method: REGISTER
Message Header
Via: SIP/2.0/UDP 84.161.95.88:15742;rport;branch=z9hG4bK7F7404F0C882C075E8...
From: Leonhard Stiegler <sip:1886929@sipgate.de>; tag=637993201 SIP from address: Leonhard Stiegler <sip:1886929@sipgate.de> SIP tag: 637993201
To: Leonhard Stiegler <sip:1886929@sipgate.de>
Contact: "Leonhard Stiegler" <sip:1886929@84.161.95.88:15742>
Call-ID: 5CC91C331F2B4D69ADC5802173417C1A@sipgate.de
CSeq: 13012 REGISTER; Expires: 1800;
Authorization: Digest username="1886929", realm="sipgate.de", nonce="4268b8d310b8fe377...", response="6b81034685e2f2ac20b01e...", uri="sip:sipgate.de"
Max-Forwards: 70; User-Agent: X-Lite release 1103m; Content-Length: 0

Рисунок 3.4 Пример записи запроса REGISTER

На рис. 3.4 приведен текст запроса REGISTER, который посы-

дает пользователь Leonhard Stiegler на свой прокси-сервер.

В стартовой строке запроса указан адрес прокси-сервера (sip:sipgate.de), версия протокола SIP/2.0, и наименование запроса (Method: REGISTER).

В поле Via указан IP-адрес терминала и порт.

В поле From указан SIP адрес пользователя (sip:1886922@sipgate.de – в формате: № телефона@шлюз).

Поскольку пользователь предполагает получить ответ на регистрацию, то он указывает в поле «To» свой же SIP-адрес.

В поле Contact размещен SIP-адрес и IP-адрес + порт пользователя.

Поле Call ID содержит уникальный идентификатор вызова в пределах домена sipgate.de.

В поле Cseq указан порядковый номер запроса – 13012, а в подполе Expires = 1800 время длительности регистрации в секундах.

В поле Authorization приведены имя пользователя (username) и его универсальный идентификатор URI, имя сервера регистрации (realm), а также параметры авторизации (nonce, response).

В сообщении отсутствует содержание, поэтому в поле Content-Length стоит «0».

Допустим, что в ответ на приведенный запрос Register терминал получит сообщение 401 Unauthorized (рис. 3.5).

Это означает, что сервер отказывается регистрировать данного пользователя и посылает ему значение поля nonce = "43c23548f0..."

Если терминал сможет правильно обработать полученное значение, то при повторном запросе он будет зарегистрирован на этом сервере и получит ответ 200 OK.

В результате приема такого ответа терминал получает от сервера данные аутентификации: Digest realm = "sipgate.de", nonce = "43c23548f0...". Получив этот ключ и запросив собственную программу аутентификации, терминал вновь обращается к серверу и получает регистрацию.

- **Status-Line:** SIP/2.0 401 Unauthorized Status-Code: 401 Resent
- **Packet:** False
- **Message Header**
- **Via:** SIP/2.0/UDP 84.161.98.188:5060; rport=5062; branch=z9hG4bK6....
- **From:** Leonhard Stiegler <sip:1886922@sipgate.de>; tag=3910253284
- **SIP Display info:** Leonhard Stiegler
- **SIP from address:** sip:1886922@sipgate.de SIP tag: 3910253284
- **To:** Leonhard Stiegler <sip:1886922@sipgate.de>; tag=b11cb9bb27....
- **SIP Display info:** Leonhard Stiegler
- **SIP to address:** sip:1886922@sipgate.de
- **SIP tag:** b11cb9bb270104b49a99a995b8c68544.393e
- **Call-ID:** 53E4A3FAD68744B68A5F95AC8C624701@sipgate.de
- **CSeq:** 1155 REGISTER
- **WWW-Authenticate:** Digest realm="sipgate.de", nonce="43c23548f0..."
- **Server:** sipgate ser Content-Length: 0

Рисунок 3.5 Пример записи ответа 401 Unauthorized

3.5 Временная диаграмма процесса установления соединения

Рассмотрим запись трассы установления сеанса связи между двумя терминалами через один прокси-сервер, на котором они уже зарегистрированы.

Временная диаграмма процесса представлена на рис. 3.6, а подробная запись трассы при помощи сниффера WireShark приведена в приложении 3 (SIP-Proxy).

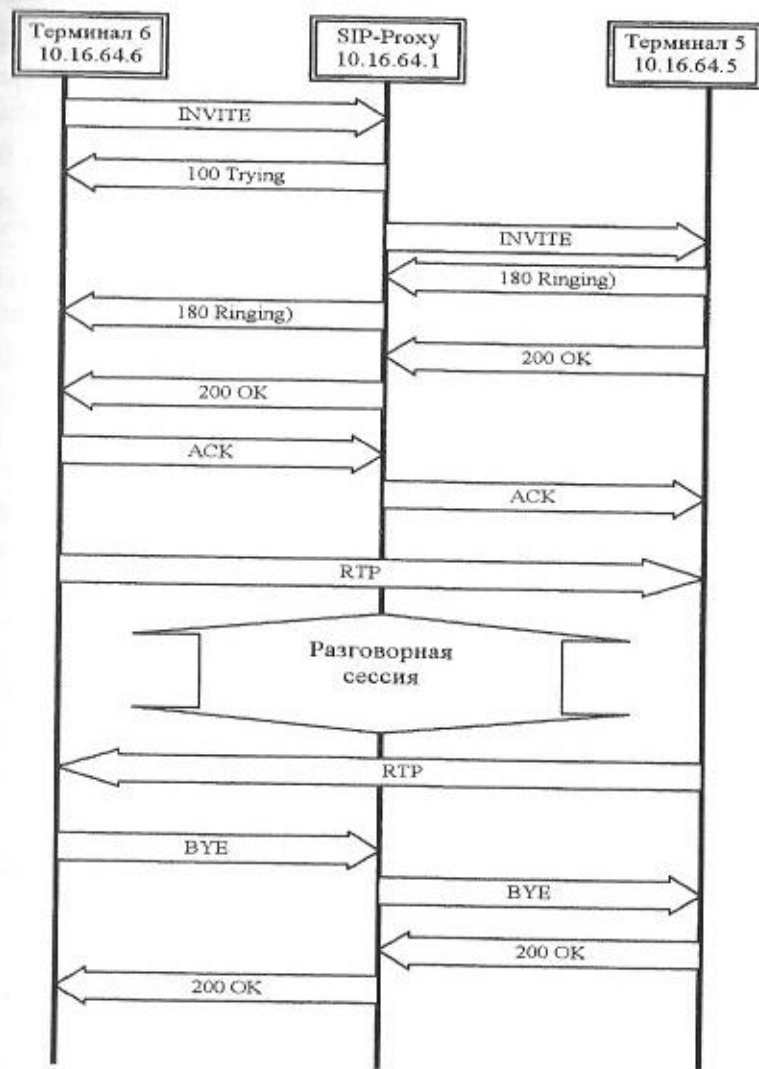


Рисунок 3.6 Временная диаграмма установления соединения VoIP, передачи речи и разъединения между двумя SIP терминалами через прокси-сервер

Терминал «6» посылает запрос INVITE на свой прокси-сервер. Текст заголовка этого сообщения представлен на рис. 3.7.

Session Initiation Protocol

Request-Line: INVITE sip:user5@10.16.64.1 SIP/2.0

Message Header

Via: SIP/2.0/udp 10.16.64.6;rport;branch=z9h....

From: "user6"<sip:user6@10.16.64.1>; tag=20707

To: <sip:user5@10.16.64.1>

Contact: <sip:user6@10.16.64.6:5060>

Call-Id: 3D534AE....@10.16.64.

Cseq: 1 INVITE

User-Agent: SJphone/1.50.217d

Content-Type: application/sdp

Content Length: 333

Рисунок 3.7 Заголовок запроса INVITE

Как видно из приведенного рисунка пользователь с терминала «6» (IP-адрес: 10.16.64.6) посылает запрос в прокси-сервер (IP-адрес: 10.16.64.1) на организацию сеанса связи с терминалом «5» (sip:user5@10/16/64/1). В качестве терминала используется программная реализация VoIP телефона: SJphone. Сообщение также имеет содержательную часть длиной 333 байта, сформированную протоколом SDP. Текст содержательной части представлен на рис. 3.8.

Содержимое рассматриваемого запроса INVITE включает стандартные данные протокола SDP. Синтаксис протокола SDP предполагает, что описание сессии представляется в следующем формате:

- Версия протокола SDP v=0;
- Имя создателя и идентификатор сессии 0=<имя создателя> <идентификатор сессии> <версия сессии> <тип адреса> <адрес>;
- Наименование сессии ps=<имя сессии>;

- Описание соединения $s=<\text{тип сети}> <\text{тип адреса}> <\text{адрес окончания}>$;
- Временные данные $t=<\text{время начала сессии}> <\text{время окончания сессии}>$;
- Описание транспортного соединения $m=<\text{вид информации}> <\text{номер порта}> <\text{стек протоколов}> <\text{типы кодеков}>$;
- Атрибуты транспорта (a): $<\text{протокол}> <\text{тип кодека}>$.

Message body

Session Description Protocol Version: 0

Owner/Creator, Session ID: - 3406345733 3406345733 IN IP4 10.16.64.6

Session Name: SJphone

Connection Information: IN IP4 10.16.64.64.6

Time Description, active time: 0 0

Session Attribute: direction: active

Media Description, name and address (m): audio 49162 RTP/AVP 0 8 3

Media Attribute (a) : rtpmap: 0 PCMU/8000

Media Attribute (a) : rtpmap: 8 PCMA/8000

Media Attribute (a) : rtpmap: 3 GSM/8000

Рисунок 3.8 Содержимое запроса INVITE, данные протокола SDP

Исходя из формата SDP, информацию, представленную на рис. 3.8, следует читать следующим образом:

$v=0$ (обычно используется эта версия протокола SDP);

$o=$ (имя создателя не указано) (идентификатор и версия сессии обычно одинаковы) (интеллектуальная сеть) (тип адреса IP4) (адрес создателя сессии 10.16.64.6);

$ns=$ (имя сессии SJphone);

$s=$ (интеллектуальная сеть) (тип адреса IP4) (адрес окончания 10.16.64.6);

$t=$ (время начала - 0) (время окончания - 0) – сессия еще не началась;

Атрибут сессии (a)= (направление активно):

$m=$ (аудио) (порт 49162) (стек: аудио/видео поверх RTP) (список кодеков: 0, 8, 3);

$a=$ (rtp) (0 – кодек G.711 μ -закон/ 8000 – частота отсчетов);

$a=$ (rtp) (8 – кодек G.711 А-закон /8000 – частота отсчетов);

$a=$ (rtp) (3 – кодек GSM /8000 частота отсчетов).

В ответ на запрос INVITE прокси-сервер посылает ответ 100 Trying и пересылает INVITE к терминалу «5». Терминал отвечает сообщением 180 Ringing, которое сервер пересылает терминалу «6». Когда абонент принимает вызов на терминале «5», последний формирует ответ 200 OK. В этом сообщении указывается, что для передачи голоса выбран кодек G.711 с μ -законом, а номер UDP-порта – 49160.

Между терминалами открывается RTP-сессия, по которой происходит обмен голосовыми пакетами. По значению временных меток этих пакетов можно судить о продолжительности разговора (Timestamp=0, 160, 320,...).

Завершение сессии инициирует терминал «6», посылая запрос BYE к прокси-серверу. Сервер пересылает запрос к терминалу «5», который отвечает 200 OK.

Читателям предлагается самостоятельно проанализировать трассу в приложении 3 более детально.

В настоящее время протокол SIP получает все более широкое распространение в сетях NGN. Он не только заменяет протокол H.323 в традиционных приложениях VoIP, но и используется для взаимодействия между программными коммутаторами SX, о чем будет рассказано в главе 4.

Контрольные вопросы и задания

1. Определите, какой из перечисленных SIP адресов не соответствует формату: vladimir@tc.alcatel.ru, 6730270@tc.alcatel.ru,

Vladimir@6730270.

2. Для чего необходимо подполе tag в поле заголовка From?
3. Поясните назначение поля Cseq в заголовке SIP-сообщения.
4. По трассировке сообщений в приложении 3 определите идентификаторы установленной RTP сессии (IP-адреса, № UDP-портов, SSRC).
5. Каким образом можно определить, что приведенная в приложении 2 трасса соответствует одному сеансу, а не двум разным?

Глава 4.

СЕТИ NGN С ПРОГРАММНЫМИ КОММУТАТОРАМИ (SOFTSWITCH)

4.1 Построение сетей NGN на базе программных коммутаторов

Функциональная модель сетей следующего поколения NGN [3, 6] содержит следующие уровни:

1. уровень доступа, включающий устройства агрегации абонентского трафика и средства адаптации к IP-сетям;
2. транспортный уровень, реализующий единую среду передачи на базе IP/MPLS;
3. уровень управления сеансами, обеспечивающий обработку сигнализации и управление медиапотокami;
4. уровень услуг, обеспечивающий реализацию различных услуг посредством доступа к серверам приложений.

Основной особенностью сетей следующего поколения является разделение процессов управления и собственно передачи информации. Этот принцип реализуется за счет того, что сигнализация обрабатывается в сетевых узлах управления – программных коммутаторах Softswitch (SX). На основании анализа полученной сигнальной информации SX управляет установлением RTP-сессии между окончаниями (терминалами или шлюзами). Сами информационные потоки (аудио, видео) передаются в пределах RTP-сессии через транспортную IP-сеть, минуя программные коммутаторы SX. Таким образом, программные коммутаторы SX пропускают через свои аппаратные платформы только часть контролируемого трафика в отличие, например, от телефонных станций.

Программные коммутаторы SX (рис. 4.1) должны обеспечивать управление как собственно терминалами VoIP, так и транспортными шлюзами на границах с сетями с коммутацией каналов (ТфОП, СПС). Для взаимодействия с абонентами VoIP используются сигнальные протоколы H.323 (глава 2) и SIP (глава 3). Соответственно, для терминалов H.323 программный коммутатор SX выполняет функции привратника (Gatekeeper), а для пользователей SIP-функции сервера SIP-Proxy.

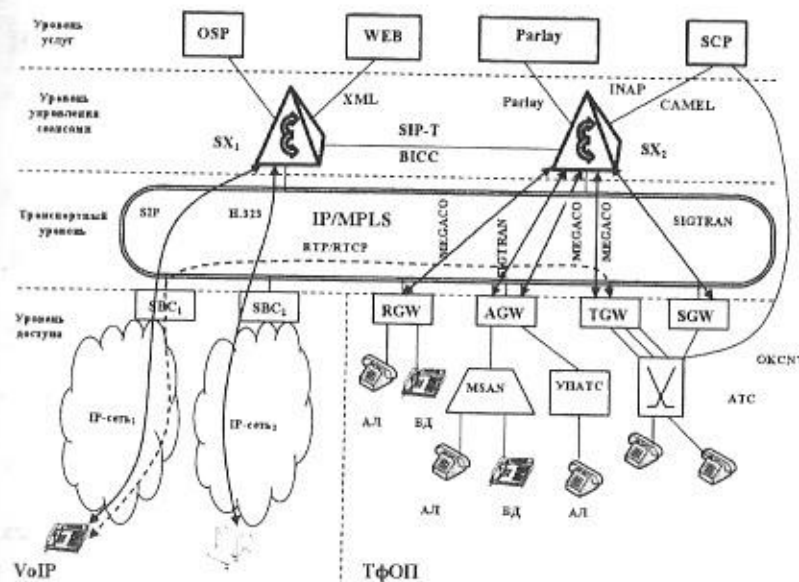


Рисунок 4.1 Функциональная схема сети NGN

Важнейшей функцией SX является обеспечение корректного взаимодействия с телефонными сетями. В этом случае SX работает в качестве контроллера транспортных шлюзов MGC (Media Gateway Controller). Контроллер шлюзов MGC обеспечивает сопряжение сетей по сигнализации и управляет транспортными шлюзами. Каждый MGC понимает и обрабатывает сигнализацию телефонных сетей: ОКС №7 (ISUP) [1], ЦАС №1 (Q.931), протокол V5.2. Если сигнальные каналы (E1) могут быть физически подключены к MGC, то проблем с их обработкой не возникает. Однако, если до SX можно добраться только через IP-сеть, то необходимо обеспечить передачу сигнальной информации через пакетную сеть с сохранением не только содержания сигнальных сообщений, но и порядка их следования и поддержки процедур защиты от ошибок. Эти функции выполняют сигнальные шлюзы (SGW), которые со стороны телефонной сети поддерживают окончание звеньев сигнализации и с помощью протокола транзита сигнализации (SIGTRAN [3, 9]) обеспечивают надежную пересылку сигнальных сообщений в MGC. В зависимости от вида телефонной сигнализации

(ОКС №7, Q.931, V5.2) существуют различные модификации протоколов адаптации SIGTRAN (M2UA, M3UA, IUA, V5UA), которые подробно описаны в следующей главе.

Транспортные шлюзы должны:

- обеспечивать прием аудио потоков из телефонной сети;
- при необходимости выполнять их перекодирование (например, из формата G.711 в G.729);
- выполнять пакетизацию речи (глава 1);
- обеспечивать контроль текущих параметров качества передачи по установленным RTP-сессиям.

Исходя из выполняемых функций транспортные шлюзы можно разделить на:

- шлюзы соединительных линий (Trunking Gateway);
- шлюзы доступа (Access Gateway);
- абонентские шлюзы (Residential Gateway).

К шлюзам соединительных линий TGW подключаются потоки E1, в которых нет сигнальных каналов, а все 30 каналов каждого потока E1 используются как соединительные линии между АТС и сетью NGN. Шлюзы доступа AGW обеспечивают подключение цифровых УПАТС по первичным доступам (PRA), т.е. потокам E1, в которых по 16-тому каналу передается сигнализация Q.931. Также к AGW могут подключаться мультисервисные платформы доступа (MSAN), которые взаимодействуют с сетью по протоколу V5.2. В абонентские шлюзы RGW (иногда также называемые интегрированными устройствами доступа IAD) непосредственно включаются аналоговые и цифровые абонентские линии.

Контроллеры MGC управляют работой транспортных шлюзов при помощи протокола H.248/MEGACO [2, 3, 12], который подробно описан в главе 6. Протокол H.248/MEGACO обладает широкими функциональными возможностями для управления транспортными шлюзами (TGW, AGW), когда MGC координирует свое взаимодействие с ТфОП посредством сигнализации ОКС №7 и Q.931. При работе с абонентскими шлюзами (RGW) протокол H.248/MEGACO обрабатывает этапы аналоговой абонентской сигнализации (снял трубку, набрал цифру ...) как последовательность событий, о наступлении которых шлюз уведомляет MGC. Таким образом, MGC получает сигнальную информацию от абонентов, используя только возможности протокола H.248/MEGACO.

Для защиты ядра сети NGN от внешних угроз (подробнее в главе 7) на границе между магистральной сетью IP/MPLS и внешними сетями устанавливаются пограничные контроллеры сессий SBC (Session Border Controller). Пограничные контроллеры сессий SBC обеспечивают:

- безопасность взаимодействия IP-сетей за счет сокрытия их внутренней структуры;
- контроль за установлением новых соединений (Call Admission Control);
- управление качеством обслуживания QoS (Quality of Service).

Каждый программный коммутатор SX управляет терминалами определенной области (домена). Так на рис. 4.1 SX1 управляет терминалами VoIP по протоколам H.323 и SIP, т.е. выполняет функции сервера IP-телефонии. SX2 выполняет функции контроллера шлюзов MGC. Взаимодействие SX между собой выполняется при помощи протокола SIP-T (SIP for Telephony) [3], который кроме данных по описанию RTP-сессии (данные SDP), содержит также вложенные сигнальные сообщения (ISUP, Q.931). Между SX возможно использование более старого протокола BICC (Bearer Independent Call Control).

Уровень услуг в сети NGN представлен различными серверами приложений, в качестве которых могут выступать как традиционные платформы интеллектуальной сети SCP, так и открытые сервисные платформы OSP, OSA/PARLAY. Для взаимодействия SX с традиционными серверами SCP используются протоколы INAP (для стационарных сетей) и протокол CAMEL (Customized Applications for Mobile Network Enhanced Logic) (для сетей GSM). Связь SX с открытыми сервисными платформами может осуществляться через PARLAY-интерфейс. Для связи с WEB-порталом применяется XML.

4.2 Взаимодействие сигнализаций в NGN

Даже краткое знакомство с функциональной схемой сети NGN, построенной на программных коммутаторах SX (рис. 4.1), выявляет главную проблему данных сетей – необходимость обеспечения корректного взаимодействия различных сигнализаций для обеспечения сеанса связи между разнотипными абонентами.

Для установления сеансов между терминалами VoIP не представляет сложностей, если оба терминала используют один и тот же протокол сигнализации. Сценарии таких соединений подробно описаны в главах 2 и 3. Если же терминалы используют разные сигнальные протоколы, то их взаимодействие контролируется SX, в котором реализована специальная функция взаимодействия IWF (Inter Working Function).

Еще более сложные правила взаимодействия применяются при организации сеансов между терминалами VoIP и абонентами ТфОП.

Рассмотрим сценарий установления соединения от абонента телефонной сети к терминалу VoIP, работающему по протоколу SIP (рис. 4.2).

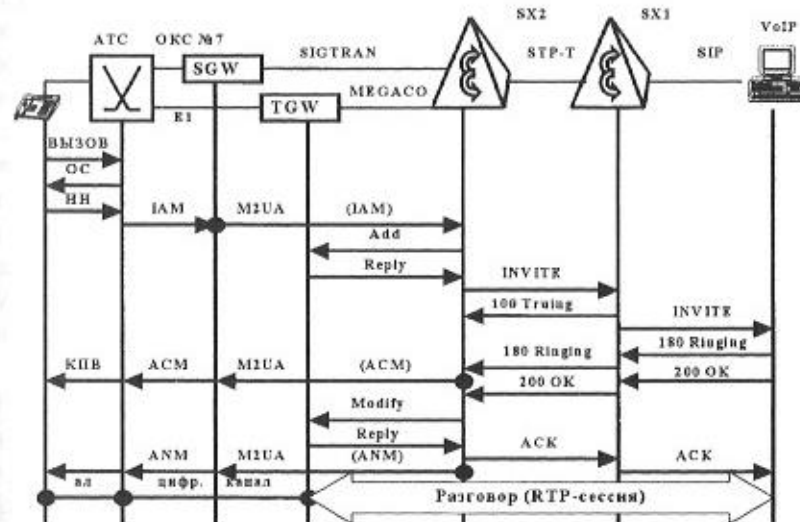


Рисунок 4.2 Сценарий установления соединения между телефонным абонентом терминалом VoIP

Абонент снимает трубку, чем формирует сигнал «вызов», воспринимаемый телефонной станцией. АТС посылает тональный сигнал «ответа станции». После чего, абонент производит набор полного номера вызываемого абонента. Станция выполняет процедуру маршрутизации и отправляет сигнальное сообщение IAM

(Initial Address Message), которое содержит номер выбранной соединительной линии (CIC) и номер вызываемого абонента (DN) в сигнальный шлюз SGW. Последний осуществляет упаковку IAM в IP-пакет при помощи процедуры адаптации M2UA (подробнее в главе 5) и отправляет в SX2. Программный коммутатор обрабатывает принятое сообщение IAM и определяет, что исходящая соединительная линия включена в шлюз TGW, а вызываемый абонент относится к домену, управляемому SX1. SX2 посылает в шлюз TGW сообщение протокола MEGACO с запросом на создание контекста (соединения) между соединительной линией (физическим портом) шлюза и виртуальным (UDP) портом будущей RTP-сессии. Шлюз TGW выполняет эту команду и создает контекст между соединительной линией и UDP-портом, сообщая номер порта в ответе на команду (Reply). После этого, SX2 отправляет сообщение INVITE, которое содержит SDP-данные (IP-адрес шлюза TGW и номер UDP-порта), в программный коммутатор SX1. SX1 отвечает сообщением 100 Trying. По полученной информации SX1 определяет, что вызываемый абонент находится в его домене и находит его текущий IP-адрес. Затем SX1 отправляет сообщение INVITE к вызываемому терминалу. Терминал принимает вызов и отвечает сообщением 180 Ringing. Получив это сообщение, SX1 формирует сигнальное сообщение ACM и отправляет его в IP-пакете (процедура M2UA) в сигнальный шлюз SGW, который обеспечивает пересылку этого сообщения к АТС. Станция включает сигнал «контроль посылки вызова» (КПВ).

Вызываемый абонент принимает поступивший вызов и его терминал посылает сообщение 200 OK в SX1. Программный коммутатор SX1 пересылает полученное сообщение в SX2. Программный коммутатор SX2 посылает команду протокола MEGACO с SDP параметрами (IP-адрес терминала и номер UDP-порта) и требованием изменить (Modify) режим работы на прием/передачу. После этого SX2 отправляет сообщение ACK в SX1 и отправляет сигнальное сообщение OKC №7 ANM (Answer Message) в ATC. После чего, абоненты приступают к разговору по составному тракту: телефонный аппарат – аналоговая линия – цифровая соединительная линия – RTP-сессия между шлюзом TGW и терминалом VoIP.

Рассмотрим еще один пример взаимодействия сигнализаций в

NGN. Допустим, что вызов сгенерирован с SIP-терминала, а вызываемый абонент включен в УПАТС, которая включена в шлюз доступа. Таким образом, необходимо определить как взаимодействуют протоколы SIP и Q.931 (рис. 4.3).

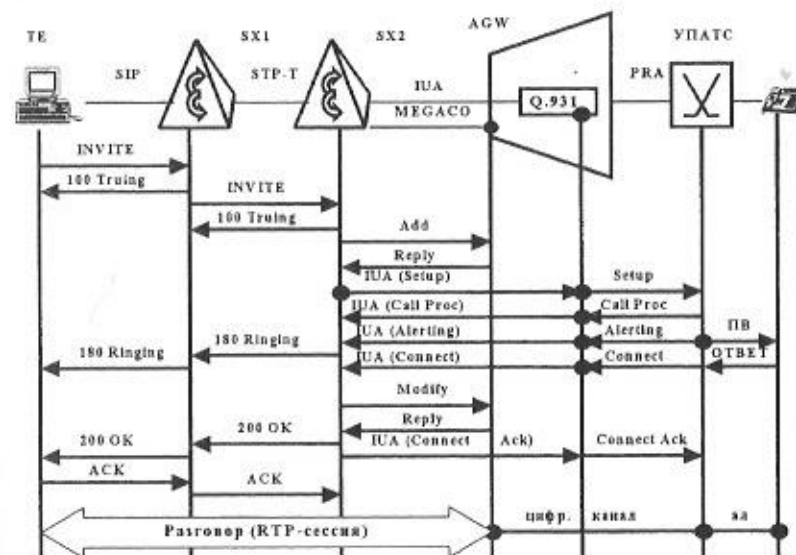


Рисунок 4.3 Установление сеанса между SIP терминалом и абонентом УПАТС (Q.931)

Терминал посылает в SX1 сообщение INVITE. Программный коммутатор принимает это сообщение и отвечает сообщением 100 Trying. Такой же обмен сообщениями происходит между SX1 и SX2. Программный коммутатор SX2 определяет, что вызов должен быть отправлен в шлюз доступа AGW. SX2 посылает команду протокола MEGACO: «Add», в которой указывает шлюзу какой канал будет задействован для этого соединения. Шлюз AGW отвечает сообщением Reply, в котором указывает номер созданного контекста и выбранный UDP-порт. SX2 формирует сообщение протокола Q.931: Setup, содержащее номер вызываемого абонента и номер выбранного канала в первичном доступе PRA, который будет использоваться для разговора. Сообщение Setup поступает в УПАТС, которая отвечает сообщением Call Proceeding. Проведя

анализ номера вызываемого абонента, УПАТС посылает ему «вызов» (ПВ). Одновременно УПАТС отправляет к SX2 сообщение Alerting. Приняв это сообщение, SX2 отправляет сообщение 180 Ringing в SX1. Последний пересылает его к вызываемому терминалу и абонент слышит сигнал контроля посылки вызова. Когда вызываемый абонент снимает трубку, то посылается сигнал «ответ». УПАТС формирует сообщение Connect, которое транслируется сигнальным шлюзом в SX2. Программный коммутатор посылает в шлюз команду протокола MEGACO: Modify, в которой режим работы порта изменяется на прием/передача. Шлюз подтверждает выполнение команды сообщением Reply. SX2 направляет к SX1 сообщение 200 OK, которое содержит полное описание удаленного окончания сессии (IP-адрес шлюза, номер UDP-порта, режим передачи: аудио и тип кодека). После этого SX2 отправляет к шлюзу сообщение Connect Acknowledge, которое транслируется сигнальным шлюзом в УПАТС. SIP-терминал, получив сообщение 200 OK, отвечает сообщением ACK и активизирует RTP-сессию. Таким образом, разговор происходит по составному тракту: SIP-терминал, RTP-сессия – AGW – цифровой канал в PRI – УПАТС – аналоговая линия – телефонный аппарат.

4.3 Сценарии перехода от ТфОП к NGN

Сети NGN не могут сразу сменить существующие телефонные сети, построенные на принципе коммутации каналов. Это означает, что период их одновременного сосуществования будет достаточно продолжителен. Особое значение приобретает и сам процесс перехода от старых сетей ТфОП к сетям NGN, построенным на базе SX. Существует несколько типовых сценариев перехода, уже апробованных при построении NGN за рубежом и в опытных зонах РФ.

При создании городской и междугородней сети IP/MPLS появляется возможность перевести весь городской и междугородний телефонный трафик на эту сеть. В этом, случае программные коммутаторы заменяют АМТС и УАК, что по западной терминологии соответствует узлам 4-го класса (Class 4). В сценарии предполагается, что ПАТС сохраняются в качестве концентраторов абонентского трафика (рис. 4.4). Также сохранение ПАТС упрощает раз-

мещение шлюзов соединительных линий TGW. Если в городе отсутствуют абоненты VoIP, то программный коммутатор работает только в режиме управления шлюзами MGC (Media Gateway Controller). Такое решение принято называть построением сети NGN на базе MGC Class 4.

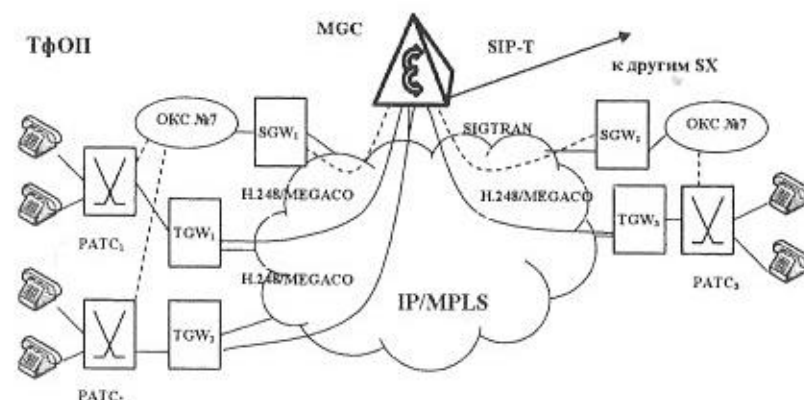


Рисунок 4.4 Сеть NGN на базе MGC Class 4

Более радикальным является сценарий, при котором из телефонной сети города исключаются также устаревшие ПАТС, которые по западной терминологии называются узлами 5-го класса (Class 5).

В этом случае, на сети устанавливаются шлюзы доступа AGW, в которые включаются УПАТС и мультисервисные узлы доступа MSAN с сигнализацией V 5.2 (рис. 4.5).

Аналоговые и цифровые абоненты включаются непосредственно в абонентские шлюзы RGW. Шлюзы доступа взаимодействуют с MGC по протоколу H.248/MEGACO, а сигнализация Q.931 передается в программный коммутатор с помощью протокола адаптации IUA (ISDN User Adaptation), входящего в состав группы протоколов SIGTRAN. Аналогично для транзита сигнализации V5.2 используется протокол V5UA. Абонентские шлюзы могут взаимодействовать с MGC по протоколам SIP или MEGACO. Такое решение обычно называется построением сети NGN на базе MGC Class 5.

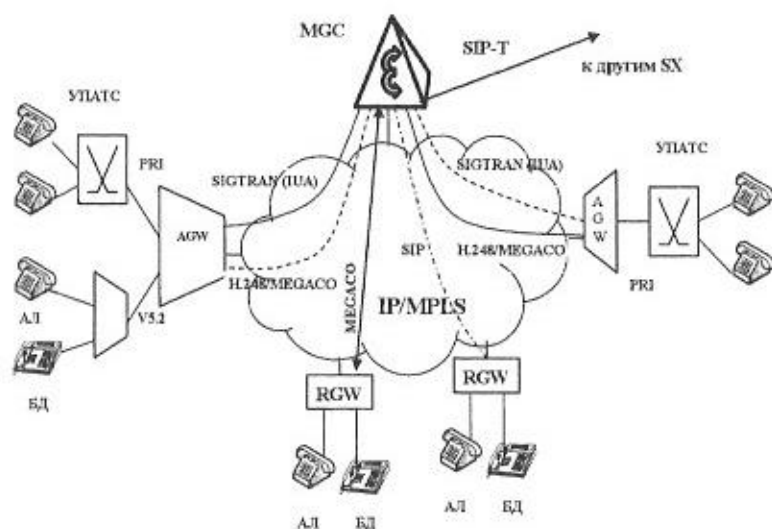


Рисунок 4.5 Сеть NGN на базе MGC Class 5

Собственно вид сценария перехода от ТфОП к NGN на практике диктуется уровнем развития транспортной сети. Если между-городная сеть IP/MPLS конкретного оператора может обеспечивать передачу значительного телефонного трафика с соответствующим качеством обслуживания, то замена АМТС на MGC Class 4 происходит быстро и безболезненно. Замена устаревших ПАТС (координатных, квазиэлектронных, электронных) является актуальной задачей для многих городов РФ, однако, для успешного перехода к NGN на базе MGC Class 5 требуется как хорошо развитая городская транспортная сеть, так и достаточный уровень развития широкополосной сети доступа. Только при наличии этих двух факторов замена ПАТС на группу абонентских шлюзов и шлюзов доступа дает необходимый эффект. В работах [8, 12] достаточно подробно рассмотрены варианты перехода от ТфОП РФ к NGN с учетом особенностей построения существующих городских и сельских телефонных сетей, однако все они могут быть сведены к рассмотренным вариантам MGC Class 4 или Class 5.

4.4 Функциональная схема программного коммутатора SX

В качестве аппаратной базы для построения SX обычно используется серверные платформы ведущих компаний производителей (Hewlett Packard, IBM...). Собственно характеристики платформы (производительность, объем дисковой памяти, наличие кластера) определяются требованиями по числу обслуживаемых вызовов в ЧНН и по надежности.

Программное обеспечение SX формируется из стандартных модулей, которые составляют 3-х уровневую структуру (рис. 4.6). Основу этой архитектуры составляет ПО управления вызовами и сеансами (Call/Session Control), которое обеспечивает реализацию различных сценариев обработки вызовов и организации сеансов связи.



Рисунок 4.6 Архитектура программного обеспечения SX

Нижний уровень составляют программные модули поддержки различных интерфейсов:

- стек протоколов ОКС №7;
- программная поддержка протоколов управления шлюзами MGCP, H.248/MEGACO;
- программные реализации протоколов сигнализации для VoIP: SIP, H.323.

Верхний уровень составляют так называемые функциональные

менеджеры:

- менеджер эксплуатации и техобслуживания;
- менеджер виртуальных частных сетей;
- менеджер расположения;
- менеджер авторизации, аутентификации и тарификации;
- менеджер служб.

Программные модули поддержки протокольных интерфейсов (ОКС №7, MGCP, H.248/MEGACO, H.323, SIP) могут быть уникальными разработками производителей SX, но чаще используются стандартные программные модули, поставляемые производителями серверных платформ (HP, IBM...).

Программные модули управления вызовами и сеансами всегда разрабатываются создателями SX с использованием различных вариантов операционной системы UNIX (True 64, LINUX...) и составляют основу ПО программного коммутатора.

Реализация законченного набора функций возложена на функциональные менеджеры.

Менеджер эксплуатации и техобслуживания (OAM Manager) обеспечивает круглосуточно возможность конфигурирования SX, мониторинга основных параметров функционирования программного коммутатора, а также поддержку процедур эксплуатации и техобслуживания.

Менеджер виртуальных частных сетей (VPN Manager) обеспечивает формирование и управления VPN сетями (см. также главу 7).

Менеджер расположения (Location Manager) расширяет возможности маршрутизации SX за счет оптимизации используемых маршрутов по критериям наименьшей цены или используемых ресурсов.

Менеджер авторизации, аутентификации и тарификации (AAA Manager) осуществляет процедуры авторизации и аутентификации абонентов. Он также формирует детальные тарификационные записи CDR (Call Detailed Records) по каждому осуществленному сеансу связи. Если для реализации этих функций используются выделенные платформы, то модуль взаимодействует с ними по протоколам RADIUS и LDAP.

Менеджер служб (Service Manager) обеспечивает взаимодействие между SX и серверами приложений, которые могут поддержи-

вать функции трансляции номера (Number Translation), поддержки маршрутизации (Clearing House), функций авторизации и аутентификации (на выделенных платформах).

Менеджер внутренних процедур (InterSoftswitch Manager) обеспечивает поддержку процедур взаимодействия между отдельными программными модулями. Например, выполнение функции взаимодействия между абонентами VoIP с разными типами сигнализации: SIP и H.323 (Inter Working Function).

Модульное построение ПО позволяет легко адаптировать его для конкретных сетевых проектов. Например, существенное снижение стоимости проекта возможно, если оператор планирует использовать SX только в режиме контроллера шлюзов MGC, поскольку не потребуется покупать ПО поддержки протокольных интерфейсов SIP и H.323. Точно также, если оператор планирует использовать SX только для управления сеансами VoIP абонентов, то ему не нужно приобретать ПО управления шлюзами. Кроме этого, модульная структура облегчает расширение функций SX за счет включения новых функциональных менеджеров.

Контрольные вопросы и задания

1. Перечислите основные функции программного коммутатора?
2. Укажите разницу в функциях разных типов транспортных шлюзов: TGW, AGW, RGW.
3. Может ли программный коммутатор MGS Class 4 управлять абонентскими шлюзами RGW?
4. В каком случае необходима реализация функции IWF?
5. Поясните, зачем в программном коммутаторе используется менеджер частных виртуальных сетей (VPN Manager)? (см. также главу 7).

Глава 5.

ПРОТОКОЛЫ ТРАНЗИТА СИГНАЛИЗАЦИИ SIGTRAN

Основой взаимодействия объектов сетей NGN с существующими сетями ТфОП остается сигнализация ОКС №7 [1, 4, 11]. Являясь наиболее развитой, а часто и единственной системой сигнализации между цифровыми коммутационными станциями как в сетях ТфОП, так и сетях связи с подвижными объектами стандарта GSM, данная система сигнализации вполне вписывается в идеологию сетей NGN по своей функциональности.

Однако, возникают существенные проблемы при практическом внедрении ОКС №7 в сети следующего поколения, поскольку вместо синхронного цифрового канала для передачи сигнальных сообщений приходится использовать пакетную сеть, в которой могут возникать как существенные задержки, так и потери пакетов. Для решения вопросов транспортировки сигнальных сообщений ОКС №7, DSS1 в IP-сетях и решения вопросов взаимодействия сетевых элементов (MGC, SGW) с центрами коммутации различных сетей с коммутацией каналов в рамках IETF была разработана группа протоколов SIGTRAN.

В соответствии с концепцией SIGTRAN, при обеспечении транзита сигнальных сообщений сами сообщения не изменяются, тогда как протоколы более низких уровней (1-3) заменяются на протоколы из мира IP. Между исходными уровнями сигнализации и IP-стеком появляются промежуточные протоколы, называемые в SIGTRAN протоколами адаптации. В зависимости от заменяемого уровня эти протоколы выполняют адаптацию на 2-ом, 3-ем или более высоких уровнях модели OSI. Кроме протоколов адаптации в концепции SIGTRAN используется специальный транспортный протокол управления потоками SCTP (Stream Control Transmission Protocol), обеспечивающий надежную доставку сигнальных сообщений.

5.1 Архитектура протоколов SIGTRAN

На рис. 5.1 представлен стек протоколов SIGTRAN. Как видно из рисунка, в стандартном стеке протоколов ОКС №7 протоколы адаптации могут заменять различные протоколы, начиная с MTP 2

и заканчивая SCCP.

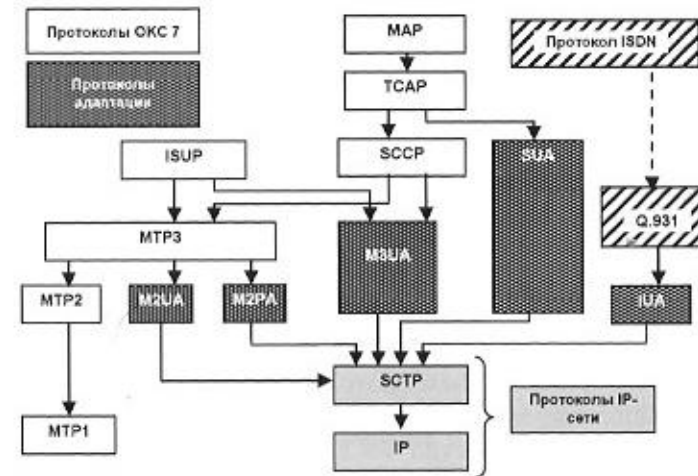


Рисунок 5.1 Архитектура протоколов SIGTRAN

Для надежной передачи сигнальных сообщений через мультисервисные IP-сети используется стек SCTP/IP, который фактически заменяет гарантированную передачу сообщений по синхронному каналу (MTP1-2). Задачи преобразования передаваемой информации протоколов более высокого уровня к возможностям протокола SCTP решаются протоколами адаптации.

Протокол M2UA (MTP-2 User Adaptation Layer) обеспечивает передачу сообщений MTP-3 через каналный уровень таким образом, что MTP-3 не ощущает, что его пакеты передаются через стек SCTP/IP, а не через обычный MTP-2. При использовании этого протокола сигнальный шлюз не имеет своего кода сигнализации (Point Code) и других атрибутов 3-его уровня, которые реализуются непосредственно в программном коммутаторе (Softswitch). Протокол M2UA имеет зарегистрированный номер порта 2904.

Протокол M2PA (MTP-2 Peer-to-Peer Adaptation Layer) [3] также обеспечивает передачу пакетов MTP-3 аналогично MTP-2. Однако, в случае использования этого протокола сигнальный шлюз выполняет функции транзитного пункта сигнализации ОКС №7 STP и, соответственно, имеет собственный код пункта сигнализации (Point Code), а также может выполнять функции более высоких уровней.

Протокол M3UA (MTP-3 User Adaptation Layer) обеспечивает передачу сигнальных сообщений ISUP и SCCP через стек SCTP/IP. Данный протокол не поддерживает некоторые стандартные функции MTP-3. Например, отсутствует часть функций эксплуатационного управления сетью.

Протокол SUA (SCCP User Adaptation Layer) обеспечивает передачу сообщений протокола MAP/TCAP через стек SCTP/IP с сохранением всех функций протокола SCCP (Signalling Connection Control Protocol).

Протокол IUA (ISDN Q.931 User Adaptation Layer) выполняет прозрачную передачу сигнальных сообщений протокола Q.931 через стек SCTP/IP, имитируя работу протокола канального уровня Q.921 в ЦСИС. Расширением протокола IUA является V5UA (V5.2 User Adaptation Layer), который обеспечивает поддержку универсального интерфейса доступа V5.2, построенного на базе расширения Q.931/Q.921.

Содержимое рис. 5.1 наглядно показывает многовариантность выбора для построения стека протоколов SIGTRAN. Так, например, для поддержки надежной передачи сообщений ISUP могут использоваться следующие варианты:

1. ISUP/MTP-3/M2UA/SCTP/IP;
2. ISUP/MTP-3/M2PA/SCTP/IP;
3. ISUP/M3UA/SCTP/IP.

Каждый из представленных вариантов обладает своими преимуществами и недостатками. Однако обсуждение различных свойств представленных вариантов стеков протоколов SIGTRAN мы продолжим в параграфе 5.3 после более детального знакомства с протоколом SCTP.

5.2 Транспортный протокол с управлением потоками SCTP

Необходимость разработки нового транспортного протокола в рамках технологии SIGTRAN была вызвана особыми требованиями, которые предъявляет передача сигнальных сообщений к IP-сетям. В первую очередь эти требования касаются строгих ограни-

чений на время передачи сигнальных сообщений, соблюдение их порядка и надежной доставки сообщений адресату. Несоблюдение этих требований будет приводить к сбоям сигнализации и, соответственно, к отказам в установлении соединений. Учитывая, что из 2-х широко известных транспортных протоколов UDP и TCP, только последний обеспечивает надежную доставку, приведем аргументы разработчиков SCTP [3], которые не позволили им использовать TCP:

1. Протокол TCP может вносить значительные задержки при передаче сегментов данных. Это происходит из-за того, что пока не осуществлена повторная передача потерянного сегмента, вся информация не может быть передана на обработку в вышележащий уровень. Такая ситуация называется *блокировкой начального сегмента* (head-of-line blocking) и может разрешаться разделением общего потока данных на отдельные потоки (streams), в пределах которых осуществляются отдельные процедуры восстановления сегментов. Аналогичная ситуация разрешается в современных браузерах путем открытия нескольких параллельных TCP сессий.
2. Протокол TCP является байт-ориентированным. Деление на сегменты данных определяется только размером максимального блока MTU и никак не связано с размерами передаваемых сигнальных сообщений. Поэтому сигнальные приложения должны вставлять дополнительные разделители границ сообщений и использовать операцию push для своевременной отправки сигнальных сообщений.
3. Протокол TCP не имеет встроенных функций обеспечения высокой надежности при сбоях на канальном уровне.
4. Протокол TCP не имеет встроенных механизмов защиты от атак типа переполнения за счет поступления SYN (SYN flooding).

Таким образом, разработчики протокола SCTP (RFC 2960) постарались решить перечисленные проблемы TCP в своем новом транспортном протоколе. Рассмотрим последовательно основные свойства протокола SCTP как надежной транспортной среды передачи сигнальных сообщений SIGTRAN.

Важнейшей особенностью протокола SCTP является возможность использования множественной адресации. В этом случае, каждому объекту может присваиваться несколько IP-адресов (multihoming) с одним и тем же номером порта. Один IP-адрес считается активным (primary), а остальные резервными (secondary). Если активный адрес становится недоступным, то используются другие транспортные адреса из списка резервных. Этим существенно повышается надежность передачи сигнальных сообщений. Использование множественной адресации наглядно представлено на рис. 5.2.

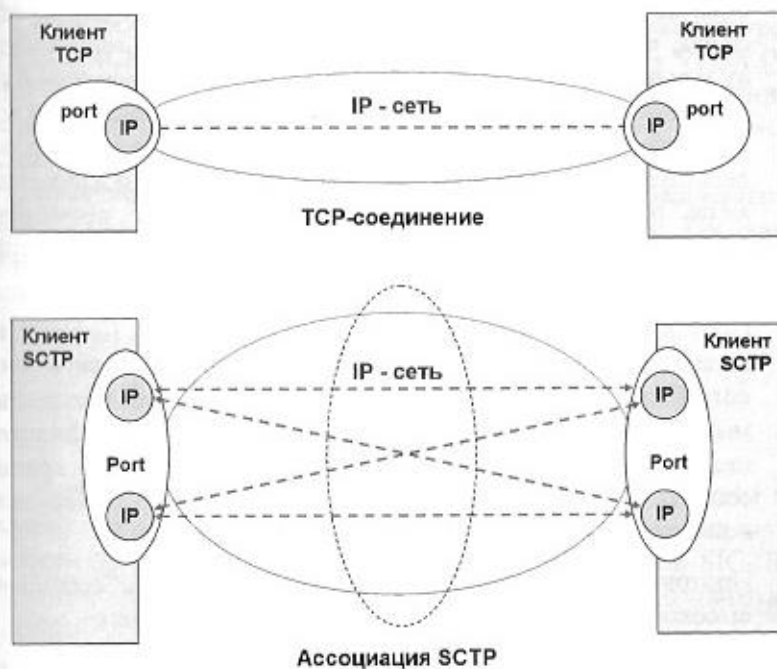


Рисунок 5.2 Множественная адресация и ассоциации SCTP

В отличие от TCP в рамках протокола SCTP вводится понятие не соединения, а *ассоциации* (association) между двумя узлами. В рамках ассоциации могут использоваться несколько сетевых интерфейсов с различными IP-адресами. При этом, ассоциации соответствует один номер порта. Каждый интерфейс в принципе может

получать информацию от любого IP-адреса удаленного хоста. С каждым интерфейсом может быть связана отдельная сеть. Таким образом, в рамках ассоциации организуется несколько путей от одного узла к другому.

Такая организация обмена используется не для разделения нагрузки, а для резервирования. Резервирование осуществляется следующим образом.

1. При повторной отправке не доставленного сообщения может использоваться альтернативный путь.
2. В SCTP встроен механизм контроля работоспособности путей (см. далее). Если один из путей оказывается неработоспособным, то используется резервный.

Множественная адресация может использоваться различными способами.

1. Предположим, что на каждой стороне обмен сигнальной информацией поддерживается некоторыми блоками (рис. 5.3), при этом используется двойное резервирование по принципу 1+1, то есть один из блоков работает в активном режиме, другой в пассивном. У каждого из блоков может быть собственный сетевой интерфейс, с которым связан собственный IP-адрес. При выходе из строя активного блока и выполнении резервного переключения начинает использоваться резервный блок и его IP-адрес.
2. Два (или более) интерфейсов узла могут иметь выход на различные сети (например, могут быть соединены с транспортной сетью через различные маршрутизаторы). При выходе из строя одного из маршрутизаторов может использоваться альтернативный маршрут.

Ассоциация SCTP – это связь между двумя конечными точками SCTP, которая характеризуется списком IP-адресов и номерами портов, а также идентификатором (Verification tag) и списком организованных потоков в пределах ассоциации (рис. 5.4).

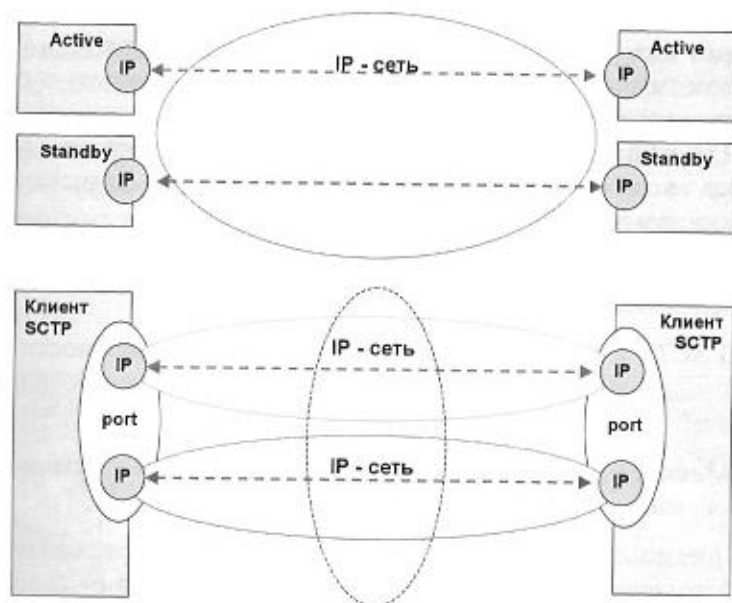


Рисунок 5.3 Использование основного и резервного IP-адресов



Рисунок 5.4 Организация потоков в одной ассоциации

В рамках одной ассоциации SCTP может быть организовано несколько различных потоков обмена данными. В этом случае каждому потоку присваивается определенный номер (Stream Identifier). Каждый поток обеспечивает последовательную доставку сообщений, но при этом различные потоки являются независимыми

(так, например, потеря сообщения в одном потоке никак не сказывается на других потоках).

Использование многопотоковости существенно для задач SIGTRAN (например, информация различных звеньев сигнализации ОКС №7 может передаваться через различные потоки).

Число потоков согласуется при установлении ассоциации. Потоки могут быть последовательными (ordered). В этом случае все сообщения в потоке нумеруются посредством последовательных номеров SSN (Stream sequence number), а также потоки могут передаваться без нумерации сообщений (unordered). В таком потоке каждое сообщение представляет собой единый блок данных пользователя.

Еще одной особенностью SCTP является сохранение границ сообщений. Если TCP (традиционный транспортный протокол) передает поток байт, то SCTP передает именно сообщения. Как показано на рис. 5.5, SCTP передает на обработку в вышележащий уровень сообщения, а не поток байт.



Рисунок 5.5 Сохранение границ сообщений в SCTP

Пакеты SCTP состоят из общего заголовка и фрагментов данных (chunk) (рис. 5.6). Общий заголовок включает номера портов источника и адресата, идентификатор ассоциации (Verification tag) и проверочное поле (Adler-32 checksum). Проверочное поле SCTP пакета формируется после того, как все фрагменты уже собраны и

охватывает все содержимое пакета. В приемнике проверочное поле заменяется нулями. После этого, проводится вычисление проверочной суммы по алгоритму Adler-32. Вычисленные проверочные разряды сравниваются с полученными. При обнаружении ошибки принятый пакет стирается (discarding).

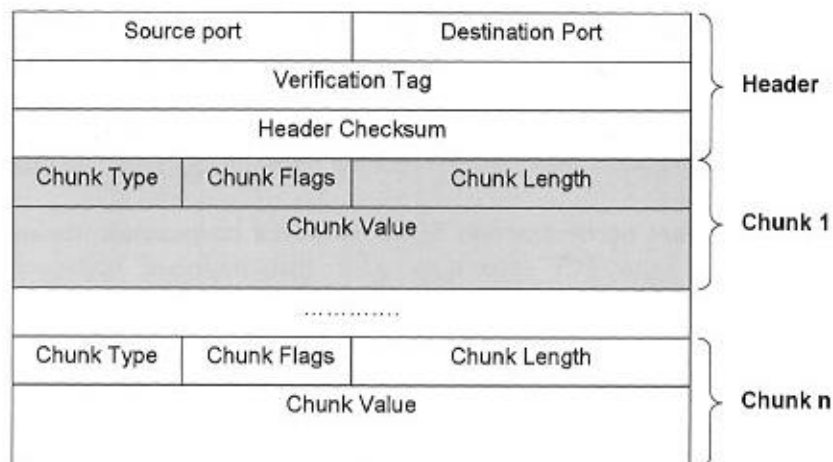


Рисунок 5.6 Структура SCTP пакета

Каждый фрагмент данных (Chunk) имеет следующую структуру (рис. 5.6):

- поле *Chunk Type* определяет код типа фрагмента;
- поле *Chunk Flags* содержит флаги фрагмента;
- поле *Chunk Length* указывает длину фрагмента;
- поле *Chunk Value* содержит данные фрагмента.

Имеется набор типов фрагментов, которые делятся на следующие категории:

1. фрагменты данных;
2. служебные фрагменты;
3. фрагменты расширений.

Идентификатор ассоциации (Verification Tag) представляет

собой случайное число. Оно используется для маркировки и отличия сообщений, относящихся к данной ассоциации от сообщений, относящихся к другим ассоциациям (например, к предыдущей ассоциации данных узлов).

Список служебных фрагментов протокола SCTP представлен на рис. 5.7.

Фрагмент	Код	Назначение
INIT	1	Установление ассоциации
INIT ACK	2	Подтверждение установления ассоциации
SACK	3	Селективное подтверждение
HEARTBIT REQUEST	5	Проверка доступности получателя
HEARTBIT ACK	5	Подтверждение доступности получателя
ABORT	6	Немедленный разрыв ассоциации
SHUTDOWN	7	Разъединение ассоциации
SHUTDOWN ACK	8	Подтверждение разъединения ассоциации
ERROR	9	Ошибка в порту
COOKIE ECHO	10	Завершение установления ассоциации отправителя
COOKIE ACK	11	Завершение установления ассоциации получателя
SHUTDOWN COMPLETE	15	Завершение разъединения ассоциации

Рисунок 5.7 Список служебных фрагментов протокола SCTP

Фрагменты INIT, INIT ACK, COOKIE ECHO, COOKIE ACK используются при установлении ассоциации.

Фрагменты SACK (Selective Acknowledgement – селективное подтверждение) используются для подтверждения приема данных пользователя.

Фрагменты HEARTBIT REQUEST и HEARTBIT ACK используются для проверки работоспособности альтернативных путей передачи.

Фрагменты SHUTDOWN, SHUTDOWN ACK и SHUTDOWN COMPLETE используются при стандартной процедуре разъединения ассоциации, фрагмент ABORT служит для немедленного разъединения.

Фрагмент ERROR служит для передачи на удаленную сторону информации об обнаруженной ошибке.

При установлении ассоциации (рис. 5.8) клиент посылает служебный фрагмент INIT, который содержит следующую информацию: тег верификации, информацию о потоках, IP-адреса.

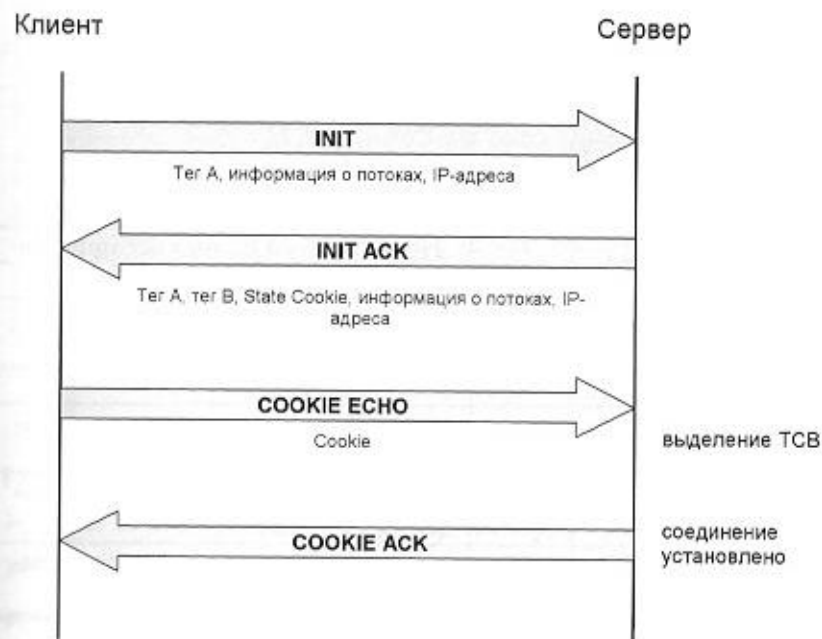


Рисунок 5.8 Процесс установления ассоциации

Сервер отвечает фрагментом INIT ACK. Фрагмент отправляется на тот IP-адрес, с которого было послано сообщение INIT. В сообщении INIT ACK сервер отправляет свой тег верификации. Кроме того, сообщение содержит State Cookie, метку времени Timestamp. В State Cookie находится информация, необходимая для аутентификации.

Клиент отвечает сообщением COOKIE ECHO, содержащим

информацию Cookie, посланную сервером.

Сервер производит необходимые вычисления, выполняет авторизацию и отвечает сообщением COOKIE ACK, после чего ассоциация считается установленной.

После установления ассоциации происходит обмен пакетами SCTP, которые содержат фрагменты данных (DATA) и селективных подтверждений (SACK).

Фрагмент DATA предназначен для переноса информации протоколов более высокого уровня. Формат фрагмента представлен на рис. 5.9. Поле Type = 0 указывает, что это фрагмент данных. Поле флагов содержит следующие три флага: U – нумерованный (Unordered), B – начало сегмента (Beginning of Segment), E – конец сегмента (End of Segment).

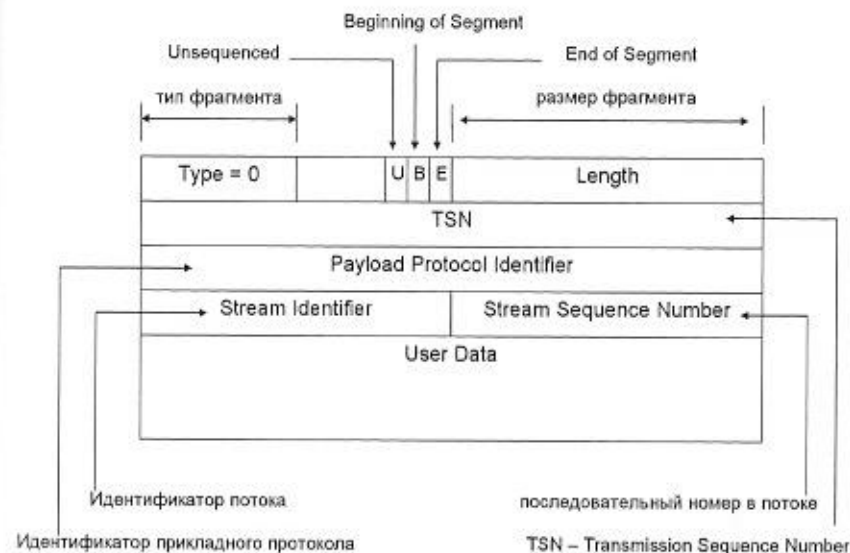


Рисунок 5.9 Формат фрагмента данных (DATA) протокола SCTP

Флаг U=1 означает, что фрагмент представляет собой одиночное сообщение (поток без нумерации). SCTP поддерживает фрагментацию-дефрагментацию сегментов передаваемых пользователем. Флаг B означает первый фрагмент сегмента. Флаг E означает последний фрагмент сегмента. Таким образом, сочетания флагов

BE имеют следующие значения:

- 10 – первый фрагмент сегмента;
- 00 – промежуточный фрагмент сегмента;
- 01 – последний фрагмент сегмента;
- 11 – нефрагментированный сегмент.

TSN (Transmission Sequence Number) – последовательный номер на передаче фрагмента представляет собой 32-битовое число. Оно назначается оконечным пунктом SCTP при создании ассоциации. При передаче каждого последующего фрагмента данных это число увеличивается на единицу.

Поле Stream Identifier содержит идентификатор потока, к которому относится фрагмент. Поле Stream Sequence Number содержит последовательный номер фрагмента в потоке. Для фрагментов с установленным флагом U=1 поле Stream Sequence Number не имеет смысла.

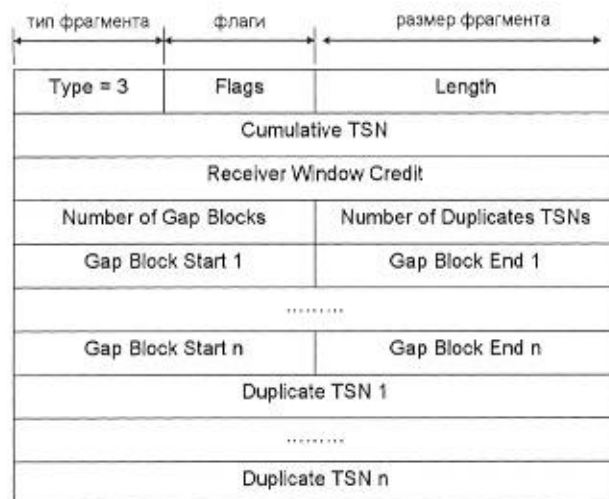


Рисунок 5.10 Формат фрагмента SACK протокола SCTP

На рис. 5.10 показана структура служебного фрагмента SACK – Selective Acknowledgement (селективное подтверждение). Поле

типа фрагмента содержит значение 3, что указывает на SACK. Фрагмент содержит следующие поля:

- *Cumulative TSN* – номер последнего фрагмента, до которого все фрагменты были приняты без потерь;
- *Receiver Window Credit* – размер окна (число фрагментов, которые могут быть переданы без получения подтверждения).

Дальнейшая информация касается отрезков полученных фрагментов с номерами больше, чем номер последнего правильно принятого фрагмента (Cumulative TSN):

- *Gap Block Start* – номер начала отрезка;
- *Gap Block End* – номер конца отрезка.

Начало и конец отрезка означает смещение относительно Cumulative TSN.

Duplicate TSN – поле, в которое записываются TSN фрагментов, принятых несколько раз.

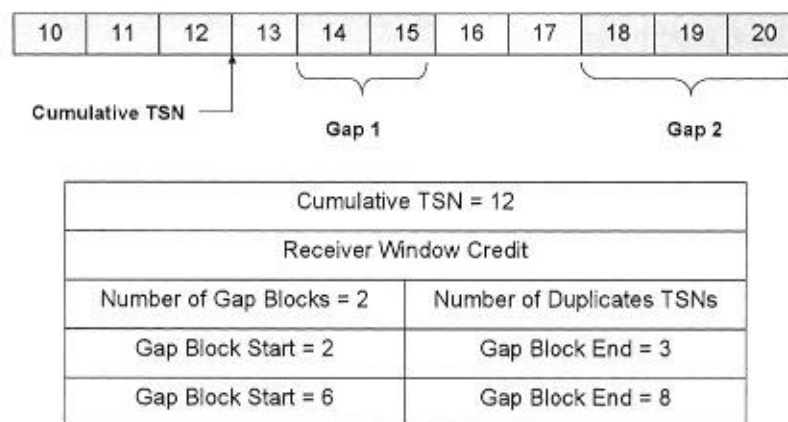


Рисунок 5.11 Пример работы селективного подтверждения SACK

Рассмотрим принцип формирования селективного подтверждения SACK (рис. 5.11).

Пусть к моменту отправки селективного подтверждения получены фрагменты с номерами меньшими или равными 12, а также

получены фрагменты с номерами 14, 15, 18, 19 и 20. В этом случае фрагмент SACK будет сформирован следующим образом.

Cumulative TSN = 12, поскольку все фрагменты до 12 включительно получены без потерь. После фрагмента с номером 12 получено два отрезка фрагментов, поэтому поле Number of Gap Blocks = 2.

Первый отрезок характеризуется следующим образом:

- начало блока пакетов (Gap Block Start) = 2;
- конец блока пакетов (Gap Block End) = 3.

Второй отрезок характеризуется следующим образом:

- начало блока пакетов (Gap Block Start) = 6;
- конец блока пакетов (Gap Block End) = 8.

Получив такой пакет, передатчик немедленно начнет передачу потерянных пакетов с TSN = 13, 16, 17.

В SCTP предусмотрен механизм защиты от перегрузки, который базируется на использовании 3-х переменных:

- окно перегрузки (cwnd);
- окно приемника (rwnd);
- счетчик переданных байт (flightsize).

Окно перегрузки – это переменная, которая показывает, сколько еще байт может послать передатчик до наступления перегрузки.

Окно приемника показывает свободную емкость приемного буфера.

Счетчик числа переданных байт показывает, сколько байт было передано и на них еще не получено подтверждение.

Таким образом, передача данных в SCTP осуществляется по следующим правилам:

1. Передатчик должен прекратить передачу данных, если уже передано число байт, указанных в параметре cwnd равно размеру окна перегрузки.
2. Передатчик должен прекратить передачу, если в приемни-

ке исчерпан размер приемного буфера (rwnd = 0).

3. В первую очередь должны передаваться фрагменты данных (DATA), запрошенные на повторную передачу.
4. Если приемник отправляет в передатчик фрагмент данных (DATA), то он обязан включать в SCTP-пакет служебный фрагмент SACK, подтверждающий прием принятых сегментов.
5. После приема одного SCTP-пакета приемник должен отправить SACK в течение 200 мс.
6. После приема 2-х SCTP-пакетов приемник должен немедленно отправить SACK в передатчик.
7. После приема дублированного фрагмента данных приемник немедленно должен отправить SACK с указанием TSN дублированных фрагментов.

Выполнение приведенных правил обеспечивает эффективную работу механизма защиты от перегрузки в протоколе SCTP [3].

Если в течение какого-то времени данные не передаются, то происходит обмен сообщениями HEARTBIT REQUEST и HEARTBIT ACK.

Сторона, инициирующая разъединение (рис. 5.12), отправляет сообщение, содержащее служебный фрагмент SHUTDOWN (разъединение).

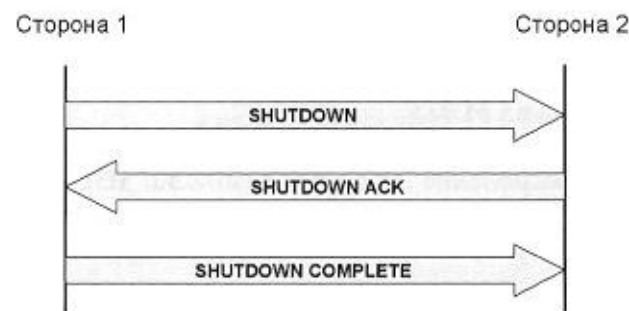


Рисунок 5.12 Процесс разъединения ассоциации

Другая сторона отвечает на это сообщением SHUTDOWN

ACK (подтверждение разъединения).

Сторона, инициирующая разъединение, отправляет сообщение, содержащее служебный фрагмент SHUTDOWN COMPLETE (разъединение завершено).

5.3 Протоколы адаптации SIGTRAN

Общие принципы построения протоколов адаптации изложены в RFC 4166. Считается, что в контроллере MGC имеется набор логических объектов, называемых *серверами приложений AS* (Application Server). Они обрабатывают сигнализацию. Для каждого AS определен набор параметров. Например, для AS, обрабатывающего сигнализацию ISUP, данный список включает коды OPC/DPC и заданный диапазон значений идентификаторов соединительных линий CIC (Circuit Identification Code).

Каждый сервер приложений AS может иметь один или несколько процессов ASP (Application Server Process) [3]. Обмен сигнальной информацией происходит между пунктами сигнализации SGW и ASP или между пунктами сигнализации и группами ASP.

Каждый ASP должен иметь свой код пункта сигнализации (PC). Однако, назначение этих кодов может быть достаточно гибким. Например, несколько ASP, связанных с конкретным шлюзом SGW, имеют один и тот же код пункта сигнализации, такой же, как и у сигнального шлюза. Поэтому, с точки зрения сети ОКС №7 это будет один пункт сигнализации. Если ASP имеют различные коды, отличные от кода SGW, тогда сеть ОКС №7 будет рассматривать SGW как пункт транзита сигнализации STP.

5.3.1 Протокол M3UA

Основное назначение протокола адаптации M3UA – это обеспечение прозрачной передачи сигнальных сообщений подсистем ISUP или SCCP через стек SCTP/IP, полностью поддерживая функции MTP3.

На рис. 5.13 показана организация стека протоколов при использовании M3UA (MTP3 User Adaptation, протокол описан в RFC 4666). Протокол M3UA использует SCTP, который, в свою очередь, передает информацию через IP-сеть.

M3UA поддерживает необходимую функциональность MTP3. При этом, с точки зрения организации сети сигнализации ОКС №7 при использовании M3UA SGW является пунктом сигнализации. В нем реализован уровень MTP3.

Сообщения ОКС №7, поступающие в SGW, обрабатываются в MTP3 и пересылаются в M3UA. На основании полученных параметров DPC/OPC/диапазон CIC производится выбор соответствующего AS и ASP. M3UA подготавливает полученное сигнальное сообщение для передачи SCTP в качестве фрагмента DATA в заданном потоке (Stream). В MGC принятый фрагмент обрабатывается в SCTP и поступает в M3UA, который отправляет это сообщение в ASP.

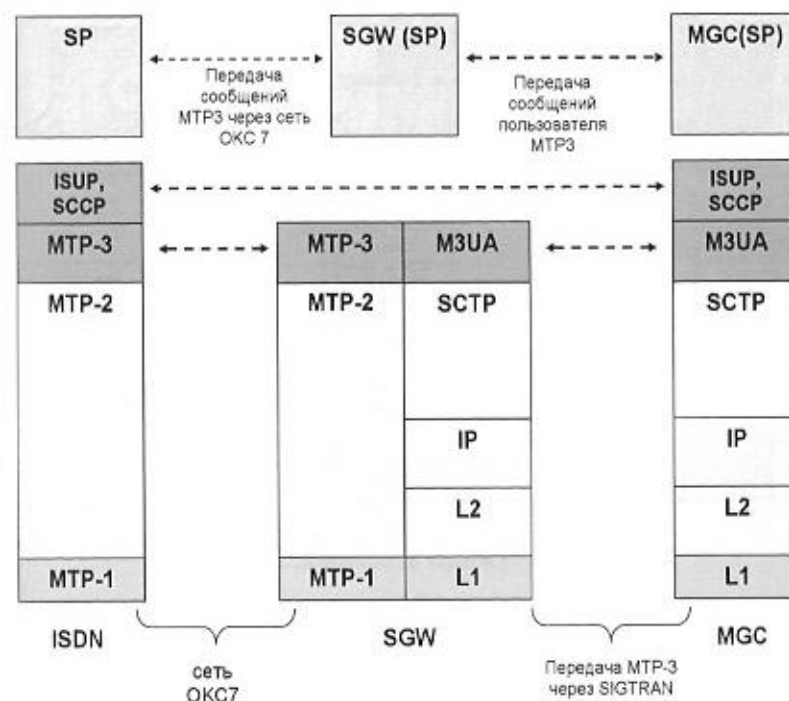


Рисунок 5.13 Функциональная схема реализации M3UA между сигнальным шлюзом SGW и контроллером MGC

Возможны различные варианты организации сети (рис. 5.14).

1. С точки зрения сети сигнализации OKCN7 имеется PC, соответствующий ASP в MGC. В этом случае сеть сигнализации OKCN7 "заканчивается" в SGW. M3UA используется для передачи сигнальных сообщений протокола пользователя MTP3 в ASP.
2. Имеется PC, соответствующий ASP в MGC. Также имеется отличный от него PC в SGW. В этом случае PC = B с точки зрения сигнализации OKCN7 SGW является STP, через который достижимы PC = C и PC = D.

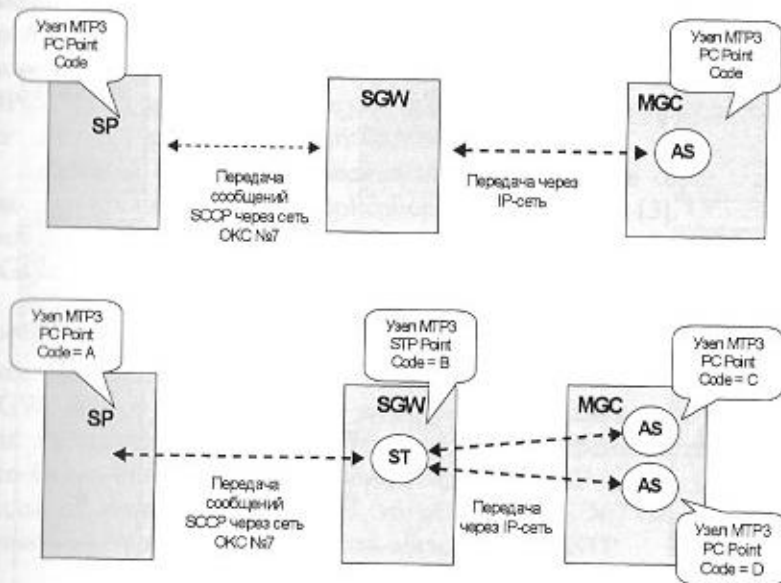


Рисунок 5.14 Режимы взаимодействия M3UA

Если SGW назначается PC, и SGW рассматривается как STP, то это дает возможность организации альтернативных маршрутов.

Допустим, что имеется возможность передачи сигнальной информации через SGW1 и через SGW2. В этом случае SGW1 и SGW2 могут рассматриваться, как STP, через которые достигим пункт сигнализации с PC D (рис. 5.15).

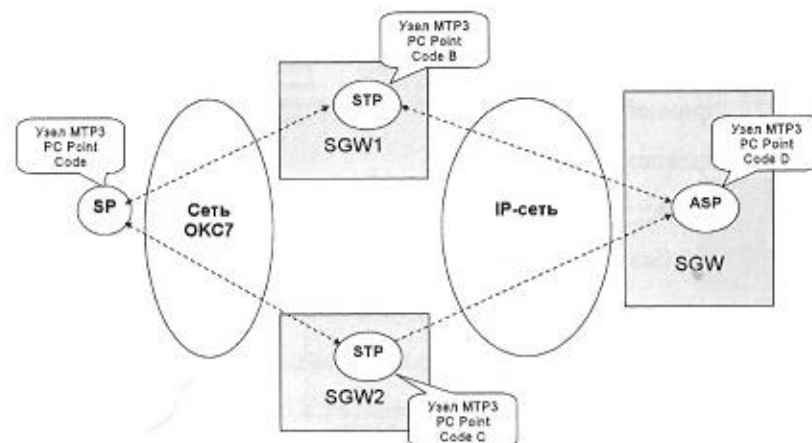


Рис.5.15 Использование альтернативных маршрутов

Формат сообщений M3UA представлен на рис. 5.16.

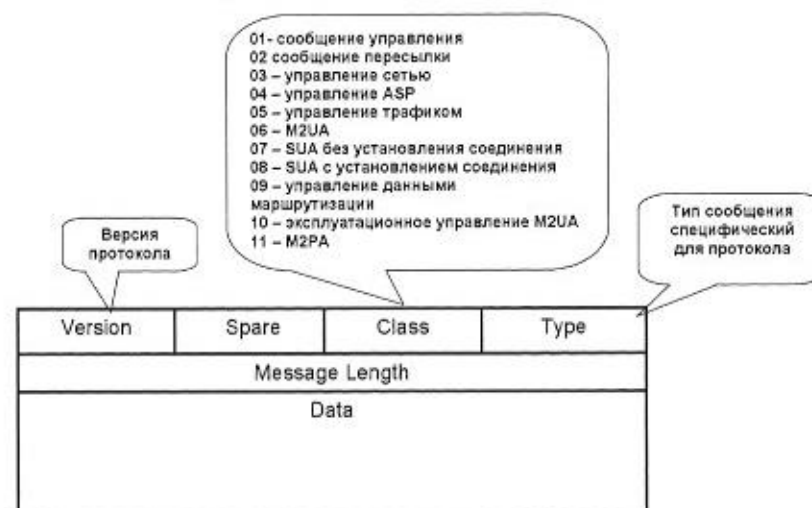


Рисунок 5.16 Формат сообщений M3UA

В поле версия (Version) указывается номер версии протокола M3UA. Свободное поле Spare занимает 8 бит. В поле Класс (Class) определяется тип сообщения:

01 – сообщение управления;

- 02 – сообщение пересылки;
- 03 – управление сетью;
- 04 – управление ASP;
- 05 – управление трафиком;
- 06 – M2UA;
- 07 – SUA без установления соединения;
- 08 – SUA с установлением соединения;
- 09 – управление данными маршрутизации;
- 10 – эксплуатационное управление M2UA;
- 11 – M2PA.

Номера с 12 по 127 зарезервированы комитетом IETF, а номера со 128 по 256 зарезервированы для расширений класса сообщений.

Кроме сообщений, переносящих информацию о соединениях, M3UA может передавать сообщения эксплуатационного контроля и управления. Это более подробно описано в книге [3].

5.3.2 Протокол SUA

SUA (SCCP User Adaptation) – протокол, позволяющий передавать через IP-сеть информацию пользователя SCCP (рис. 5.17).

Этот протокол обеспечивает передачу сообщений TCAP и поддерживает все функции протокола SCCP, включая поддержку услуг, как без соединения, так и ориентированных на соединение.

С точки зрения организации сети сигнализации OKCN7 SGW является узлом сети SCCP, у этого узла имеется SCCP-адрес. На участке между пунктом сигнализации и SGW информация передается через сеть SCCP (используется традиционный стек протоколов сигнализации OKCN7). На участке между SGW и MGC передаются сообщения пользователя SCCP (используется SUA, который работает поверх стека SCTP/IP). Протокол описан в RFC 3868 и имеет зарегистрированный номер порта 14001.

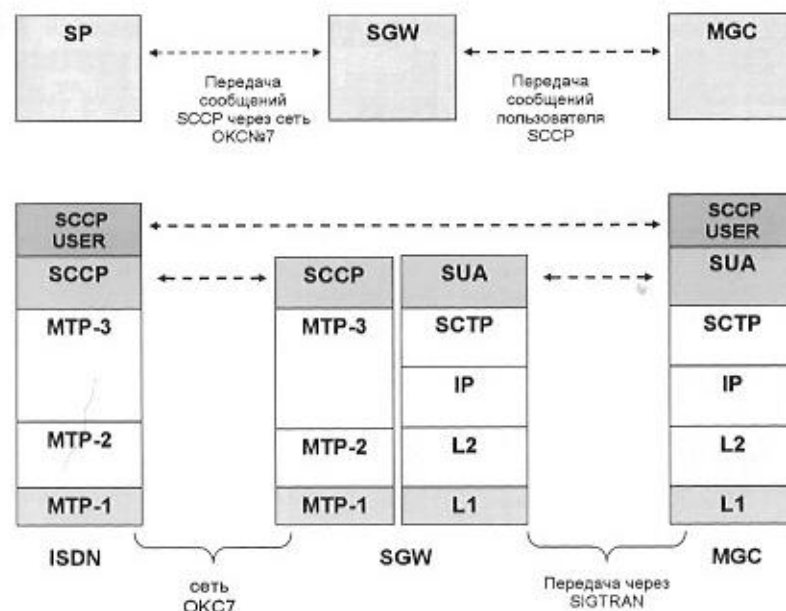


Рисунок 5.17 Функциональная схема реализации SUA между сигнальным шлюзом SGW и контроллером MGC

С точки зрения организации сети сигнализации OKC N7 возможны различные варианты построения сигнальной сети (рис.5.18).

1. Один из вариантов (для протокола, не ориентированного на соединение) заключается в том, что маршрутизация сообщений в SGW (выбор ASP) осуществляется по DPS + SSN. В этом случае для сети сигнализации OKCN7 SGW представляет собой конечный узел.
2. Второй вариант заключается в том, что выбор ASP в MGC является результатом трансляции GT (Global Title). В этом случае для сети сигнализации OKC N7 SG также является конечным узлом.
3. Для протоколов ориентированных на соединение, выбор ASP производится при установлении логического соединения.

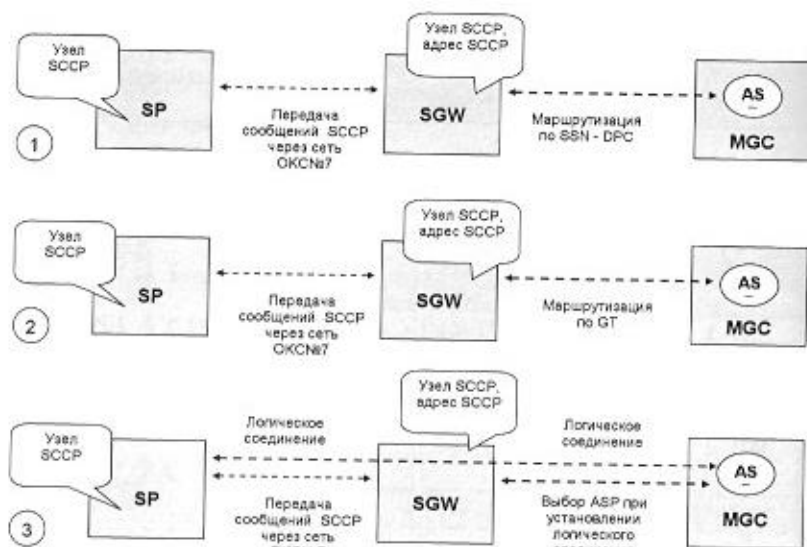


Рис.5.18 Варианты организации связи при использовании SUA

В случае применения протокола не ориентированного на установление логического соединения в SCTP-ассоциации могут использоваться потоки типа unordered.

В случае применения протокола ориентированного на установление логического соединения организуются потоки с последовательной нумерацией (ordered).

5.3.3 Протокол M2UA

При использовании протокола M2UA в сигнальном шлюзе SGW реализуются только функции 2-го уровня, тогда как в контроллере MGC реализованы функции MTP-3.

На рисунке 5.19 показана организация стека протоколов при использовании M2UA. Протокол M2UA использует SCTP. Он, в свою очередь, передает информацию через IP-сеть. Протокол M2UA описан в RFC 3331.

M2UA поддерживает необходимую функциональность MTP2. При этом поддерживается передача информации через звенья сигнализации, подключенные к SGW. Поэтому, с точки зрения организации сети сигнализации ОКС №7 при использовании M2UA

SGW не является пунктом сигнализации. В нем не реализован уровень MTP3.

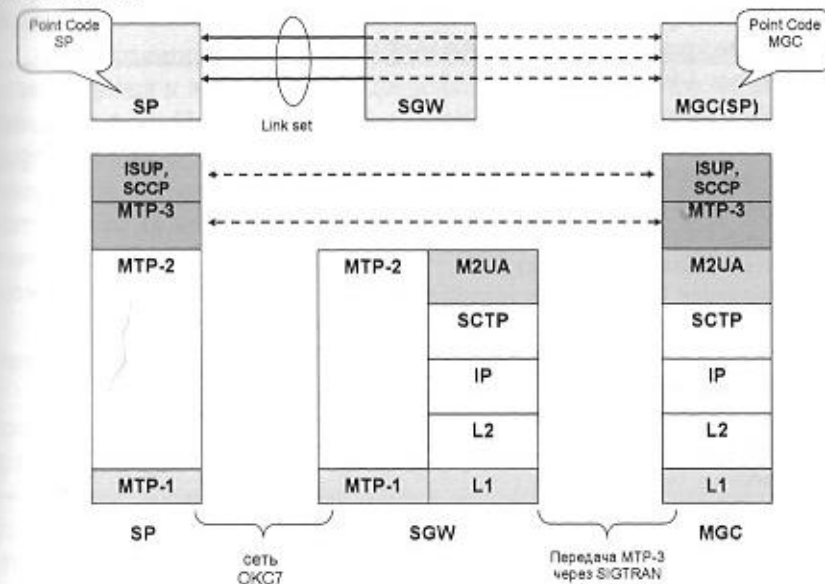


Рисунок 5.19 Функциональная схема реализации M2UA

Рассмотрим в качестве примера упрощенную трассировку сообщения IAM, которое передается от SGW к MGC (рис. 5.20).

```

Internet Protocol, Src Addr: 149.204.67.133 (149.204.67.133), Dst Addr:
172.23.94.2 (172.23.94.2)
Stream Control Transmission Protocol
Source port: 2904
Destination port: 2904
Verification tag: 0x1b374ee0
Checksum: 0x12a935f7 (correct CRC32C)
DATA chunk (ordered, complete segment, TSN: 2463531566, SID: 1, SSN:
297, PPID: 2, payload length: 60 bytes)
Chunk type: DATA (0)
Chunk flags: 0x03
.... 1 = E-Bit: Last segment
.... 1 = B-Bit: First segment
.... 0 = U-Bit: Ordered delivery
Chunk length: 76
  
```

TSN: 2463531566 Stream Identifier: 0x0001 Stream sequence number: 297 Payload protocol identifier: M2UA (2)
MTP 2 User Adaptation Layer Version: Release 1 (1) Reserved: 0x00 Message class: MTP2 user adaptation messages (6) Message type: DATA (DATA) (1) Message length: 60 Interface identifier (integer) (0) Parameter Tag: Interface identifier (integer) (0x0001) Parameter length: 8 Interface Identifier (integer): 0 Data 1 parameter Parameter Tag: Protocol data 1 (0x0300) Parameter length: 42 Padding: 0000
Message Transfer Part Level 3 Service information octet 10.. = Network indicator: National network (0x02) ..00 = Spare: 0x00 0101 = Service indicator: ISUP (0x05) Routing label 11 0111 1001 0001 = DPC: 14225 1010 0000 0111 01.. = OPC: 10269 0110).... = Signalling Link Selector: 6
ISDN User Part CIC: 70 Message type: Initial address (1) Nature of Connection Indicators: 0x0 Forward Call Indicators: 0x2001 Calling Party's category: 0xa (ordinary calling subscriber) Transmission medium requirement: 0 (speech) Called Party Number: 965711 Pointer to start of optional part: 7 Access transport (=> Q.931) Low-layer compatibility (Speech, 64 kbit/s, Recommendation G.711 A-law) High-layer compatibility (Telephony)

Рисунок 5.20 Трассировка сигнального сообщения IAM, пересылаемого от SGW к MGC с использованием M2UA

Трассировка снята на уровне IP-пакетов, поэтому первый блок информации содержит IP-адреса MGC (Dst. Addr) и SGW (Src. Addr).

Информация протокола SCTP указывает, что передается пакет, относящийся к ассоциации, определяемой тэгом верификации (Verification tag). Пакет принят без ошибок (correct CRC32C). Он содержит один фрагмент данных (DATA) с TSN: 2463531566, передаваемый в 1-ом потоке (SID: 1), с сохранением нумерации (ordered), без сегментации (complete segment), порядковый номер в потоке SSN: 297 и содержимое фрагмента сформировано протоколом M2UA (PPID: 2).

На уровне MTP2 указывается класс сообщения 6 (M2UA), и тип сообщения – данные (DATA), а также параметры интерфейса.

На уровне MTP3 указывается, что используется национальная система кодов пунктов сигнализации (National network (0x02)) и содержательная часть пакета сформирована протоколом ISUP.

Далее указывается этикетка маршрутизации (Routing label), которая содержит следующие параметры: коды DPC: 14225/ OPC: 10269, указатель звена сигнализации Signalling Link Selector: 6.

Информация уровня ISUP показывает, что передается сообщение IAM (Initial address Message). Оно включает в себя: код идентификатор соединительной линии (CIC: 70), номер вызываемого абонента (Called Party Number: 965711), совместимость на нижних уровнях LLC (Speech, 64 kbit/s, Recommendation G.711 A-law) и ряд других параметров.

Таким образом, видно, что формирование сигнального пакета выполняется в соответствии со стеком ISUP/MTP3/MTP2/M2UA/SCTP/IP.

5.3.4 Протокол M2PA

Протокол M2PA предназначен для обеспечения прозрачной передачи пакетов MTP3.

На рис. 5.21 показана организация стека протоколов при использовании M2PA. Протокол M2PA использует SCTP, который, в свою очередь, передает информацию через IP-сеть. Протокол описан в RFC 4165.

M2PA поддерживает необходимую функциональность MTP2.

С точки зрения организации сети сигнализации ОКС №7 при использовании M2PA эмулируется набор сигнальных звеньев. SGW является пунктом сигнализации, в нем реализован уровень MTP3 и SGW назначается PC (Point Code).

M2PA поддерживает все служебные функции, необходимые для функционирования MTP3:

- поддерживается переключение (Changeover);
- для MTP3 передается информация о состоянии звена;
- поддерживается функция повреждение процессора (Processor Outage);
- поддерживается процедура фазирования (Link Alignment).

Для передачи сигнальных сообщений организуются SCTP-ассоциации между SGW и MGC.

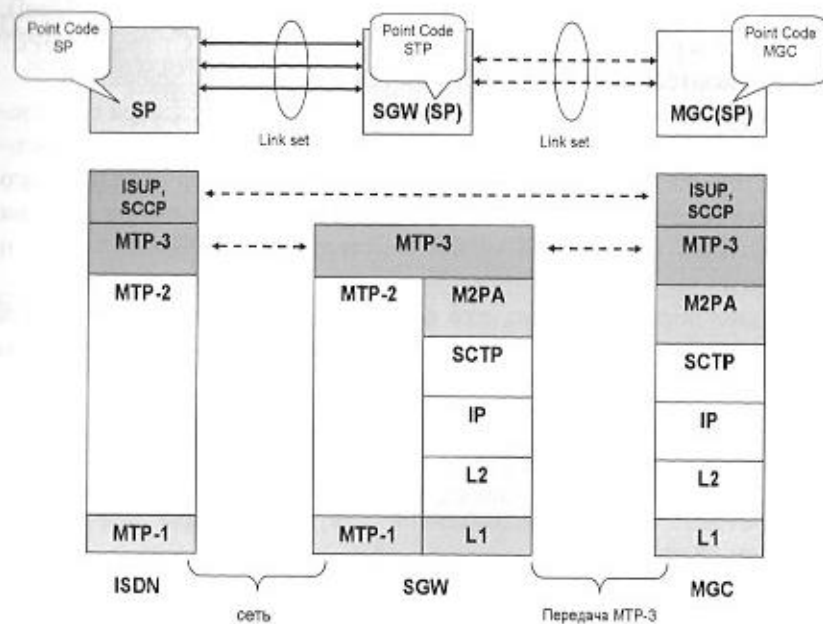


Рисунок 5.21 Функциональная схема реализации M2PA

M2PA эмулирует сигнальные звенья. Каждому виртуальному

сигнальному звену (т.е. каждому SLC – Signalling Link Code) соответствует ассоциация SCTP (рис. 5.22). Внутри нее организуется два различных потока SCTP:

1. Поток с номером 1 для передачи информации MTP3 (передаваемой в звене ОКС№7 при помощи MSSU).
2. Поток с номером 0 для передачи информации о состоянии звена (передаваемой в звене ОКС№7 при помощи LSSU).

В MTP2 предусмотрены FISU (Filling In Signalling Unit) – заполняющие сигнальные единицы. В M2PA FISU не используются.

Каждой ассоциации SCTP на обеих сторонах соответствуют свои IP-адреса и номера портов. При этом, поскольку одна из сторон должна быть готова к установлению соединения (находиться в состоянии Listening), то на одной из сторон номер порта должен иметь стандартное значение, закрепленное за M2PA (порт 3565).

Информация сигнального трафика, передаваемая внутри потока 1, передается между обработчиками уровня MTP3. Информация о состоянии звена, передаваемая в потоках 0, используется в процедурах управления звеном, осуществляемых со стороны MTP3.

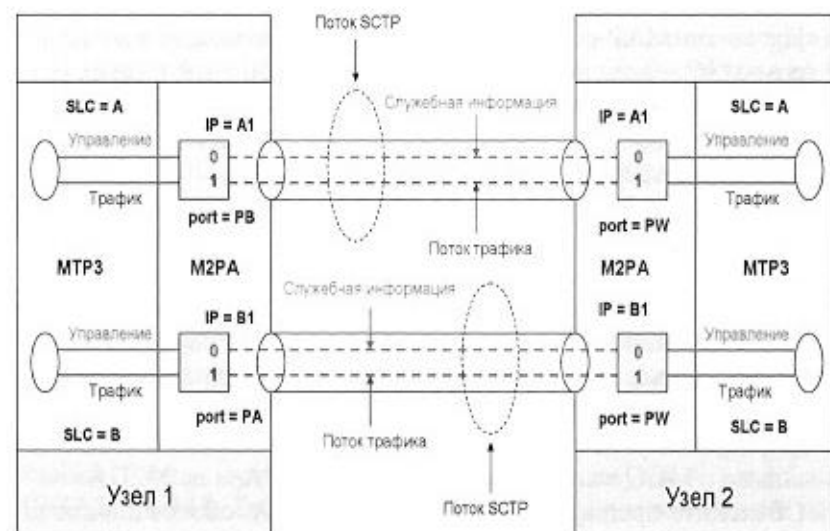


Рисунок 5.22 Схема эмуляции сигнальных звеньев в M2PA

5.3.5 Протокол IUA

Данный протокол предназначен для эмуляции канального уровня Q.921 сигнализации ЦАС№1 (DSS1). При этом кадры Q.921 могут передаваться через IP-сеть между сетевыми устройствами, которые реализуют сигнализацию Q.931.

Протокол IUA описан в RFC 3057, как инструмент поддержки сигнализаций Q.931 и QSIG для базового и первичного доступов. Зарегистрированный номер порта для этого протокола – 9000.

Таким образом, мы рассмотрели все возможные в настоящее время способы взаимодействия сигнальных шлюзов SGW с программными коммутаторами SX (контроллерами транспортных шлюзов MGC). У каждого из представленных вариантов есть свои достоинства и недостатки, поэтому выбор того или иного варианта взаимодействия этих сетевых элементов NGN осуществляется на этапе проектирования сети и учитывает ограничения функциональных возможностей, закладываемые производителями этого оборудования.

Контрольные вопросы

1. Протокол MAP описывает взаимодействие между коммутатором MSC и домашним регистром абонентов HLR в сетях сотовой связи стандарта GSM. Определите все возможные варианты стеков протоколов SIGTRAN, при помощи которых возможна передача сообщений MAP через IP-сеть.
2. Нарисуйте временную диаграмму обмена пакетами SCTP, если при передаче 3-его фрагмента DATA на стороне приемника обнаружена ошибка при проверке Adler32.
3. Составьте структуру пакета SCTP (аналогично рис.5.20), который будет передан от MGC к сигнальному шлюзу SGW в ответ на сигнальное сообщение IAM и будет содержать сигнальное сообщение ACM.
4. Определите условия, при которых для соединения сигнального шлюза с MGC выгоднее использовать M2PA, а не M2UA.
5. Объясните преимущества протокола M3UA, обеспечившие его достаточно широкое применение на начальном этапе создания NGN.

Глава 6. ПРОТОКОЛ УПРАВЛЕНИЯ ТРАНСПОРТНЫМИ ШЛЮЗАМИ MEGACO/H.248

6.1 Развитие протоколов управления шлюзами

Программный коммутатор SX выполняет функции управления всеми типами транспортных шлюзов:

- транковыми шлюзами (TGW);
- шлюзами доступа (AGW);
- резидентными шлюзами (RGW).

В зависимости от типа шлюза процедуры управления могут в некоторой степени меняться, но суть происходящих процессов сохраняется.

Протоколы управления шлюзами развивались вместе с технологией сетей NGN и имеют свою историю. В начале подключение шлюзов осуществлялось при помощи первичного доступа ЦСИС (PRI). При этом сигнальная информация Q.931 поступала на шлюз в D-канале (16 временной интервал E1). Таким образом, шлюз имел всю необходимую для установления соединения информацию. Первоначально концепция построения сетей предполагала, что транспортные шлюзы могут сами управлять установлением соединения в пакетной сети. На это были ориентированы протоколы SGCP, IPDC. Однако, с расширением емкости транспортных шлюзов в них стали включаться только пучки соединительных линий (потoki E1), тогда как все сигнальные сообщения передавались через выделенные сигнальные шлюзы SGW ОКС №7. Таким образом, транспортные шлюзы перестали получать сигнальную информацию со стороны телефонной сети, а все процессы установления соединений в пакетных сетях стали управляться программным коммутатором. Для этого использовался протокол MGCP (Media Gateway Control Protocol). В настоящее время практически во всех реализациях используется протокол MEGACO/H.248. Его двойное название обусловлено тем, что данный протокол является совместной разработкой IETF и ITU-T. Функциональность протокола и набор команд едины и согласо-

ны обеими организациями. Отличия заключаются в том, что протокол MEGACO, разработанный IETF, является текстовым протоколом, тогда как в основу H.248 положена концепция абстрактного синтаксиса ASN.1, принятая в ITU-T.

6.2 Концепция и основные определения

Протокол управления транспортными шлюзами MEGACO (MEdia GAteway COntrol Protocol) описан в документе IETF RFC 3015, содержание которого полностью согласовано с Рекомендацией H.248 МСЭ-Т (ITU-T). Поскольку форматы сообщений и их содержание, сценарии взаимодействия в этих совпадают, то принято рассматривать их как единый протокол.

Протокол MEGACO/H.248 относится к уровню приложений и для передачи своих сообщений может использовать как стек TCP/IP, так и стек UDP/IP. В основном используется стек UDP/IP.

Концепция протокола MEGACO/H.248 предполагает, что в транспортном шлюзе имеется набор окончаний или портов. Физические порты соответствуют соединительным линиям, подключенным к шлюзам со стороны телефонной сети, и существуют постоянно. Порты со стороны пакетной сети представляют собой окончания RTP-сессий, создаваемых на время соединения в пакетной сети. Все окончания имеют свои идентификаторы:

- физические порты определяются номером потока EI и номером канала в потоке;
- виртуальные RTP порты характеризуются номером UDP порта, присвоенным данному соединению на этапе его установления.

Каждое окончание может быть свободно или соединено с одним или несколькими другими окончаниями. Для определения такого соединения вводится понятие *контекста*. Контекст является отображением логических связей между физическими и виртуальными портами.

На рис. 6.1 представлены возможные варианты контекстов. Считается, что все порты, не участвующие в соединении, относятся к фиктивному (нулевому соединению). В ассоциацию может входить 2 порта, как это показано для первого контекста (Context 1) или несколько портов, как это показано для второго контекста

(Context 2).

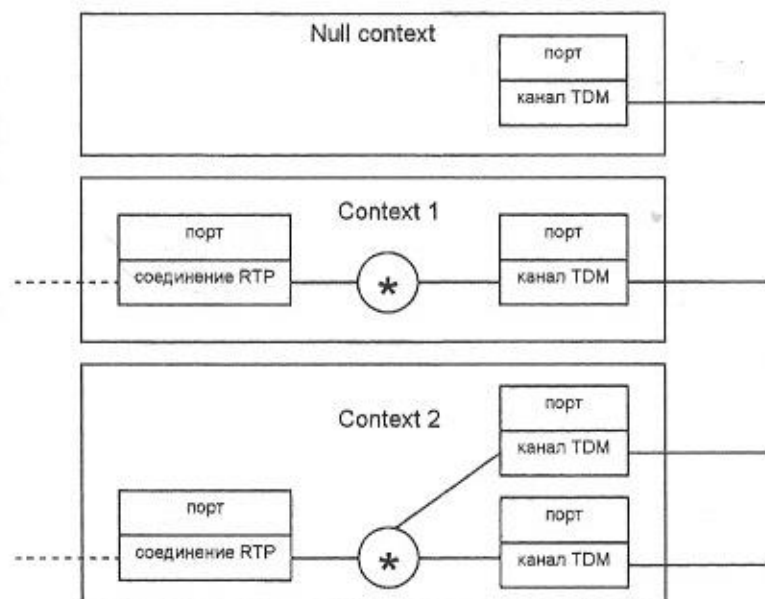


Рисунок 6.1 Типы контекстов

Каждое сообщение MEGACO может содержать одну или несколько транзакций. *Транзакцией* называется группа команд, пересылаемых в одном блоке. Каждой транзакции назначается идентификатор. Программный коммутатор MGC отправляет к транспортному шлюзу MGW сообщение Transaction: Request, на которое следует ответное сообщение Transaction: Reply. Таким образом, взаимодействие построено по принципу запрос-ответ.

Каждая транзакция состоит из последовательности действий, относящихся к определенному контексту (указывается идентификатор контекста).

Каждое действие, в свою очередь, состоит из последовательности команд относящихся к определенному окончанию. В каждой команде может содержаться последовательность дескрипторов окончания.

Список команд можно представить в виде таблицы 6.1.

Таблица 6.1

Список команд протокола MEGACO

Команда	Назначение
ADD	Команда добавления окончания в контекст. Контекст может еще не существовать, в этом случае ADD является командой создания контекста.
MODIFY	Команда, требующая изменить свойства окончания.
SUBTRACT	Команда удаления окончания из контекста. Удаление последнего окончания из контекста является удалением контекста.
MOVE	Команда, позволяющая переместить окончание из одного контекста в другой.
AUDITVALUE	Команда, позволяющая получить текущую информацию об окончании.
NOTIFY	Позволяет уведомить программный коммутатор MGC о событиях, связанных с окончанием.
SERVICECHANGE	Позволяет уведомить MGC о том, что окончание или группа окончаний будут выведены из рабочего состояния (или возвращены в рабочее состояние).
AUDITCAPABILITIES	Позволяет получить информацию о возможных значениях свойств, событий и сигналов.

Каждая команда содержит дескрипторы окончаний, которые предназначены для описания определенных групп параметров.

Предусмотрены следующие дескрипторы окончания, представленные в таблице 6.2.

Таблица 6.2

Дескрипторы окончания

Дескриптор	Назначение
Modem	Содержит информацию об использовании модема.
Mux	Содержит информацию о мультиплексировании.
Media	Содержит информацию о состоянии окончания и о потоках в транспортной среде (используемые кодеки, ресурсы и т.д.).
Events	Содержит информацию о событиях, связанных с окончанием.
Signals	Содержит информацию о передаваемых сигналах.
Audit	Данные о параметрах, которые могут контролироваться в MGW.
Packages	Данные о типовых наборах характеристик, связанных с окончанием.
Digit Map	Содержит информацию об обработке цифр номера.
Service Change	Данные, связанные с изменением процесса обслуживания вызова.
Observed Events	Данные о зарегистрированных событиях.
Statistics	Статистические данные, связанные с окончанием.

Многие дескрипторы имеют вложенную структуру. Например, в дескрипторы транспортной среды (Media) вкладываются деск-

рипторы потока (Stream), описывающие потоки. В свою очередь, дескрипторы потока Stream могут содержать дескрипторы, приведенные в таблице 6.3.

Таблица 6.3
Дескрипторы транспортной среды

Дескриптор	Назначение
Local Control Descriptor	Дескриптор, описывающий управление потоком трафика на локальной стороне. Может содержать параметр Mode, описывающий режим приема и режим передачи.
Local Descriptor	Дескриптор, описывающий поток на местной стороне.
Remote Descriptor	Дескриптор, описывающий поток на удаленной стороне

Local Descriptor и Remote Descriptor содержат описание потока в соответствии с протоколом описания сессий SDP (Session Description Protocol). Если в качестве транспортной среды используется IP-сеть, то дескриптор может включать следующие данные: IP-адрес, версию IP-протокола, номер UDP-порта и транспортный протокол, который используется для передачи трафика и его версию.

На рис. 6.2 приведена расшифровка дескриптора транспортной среды, который включает дескриптор управления на местном окончании (Local Control Descriptor) и дескрипторы местного (Local) и удаленного (Remote) окончаний.

Дескриптор управления указывает режим работы местного окончания. В данном случае – передача и прием (Mode: SR).

Для местного дескриптора (Local Descriptor) приведена сокращенная запись вложенных параметров протокола SDP (см. также формат записи в 3.5), значение которых расшифровано в следующих строках.

Media Descriptor

M{O{M

Local Control Descriptor: MO=SR

Mode: SR

Media Descriptor

M{L{\n

Local Descriptor: v=0\r\no=bell 53655 53655 IN IP4

128.3.4.6\r\nnc=IN IP4 100.100.105.133\r\nnm=audio 40014

RTP/AVP 8\r

Remote Descriptor: v=0\r\no=bell 865833 865833 IN IP4

149.204.67.216\r\ns=SDP from Megacopi\r\nnc=IN IP4

100.100.105.216\r\nt=0 0\r\nm=audio 30512 RTP/AVP 8\r

Рисунок 6.2 Расшифровка описаний дескрипторов местного и удаленного окончаний

Так, запись начинается с указания используемой версии V=0 протокола SDP. Затем идет наименование создателя сессии Owner Username: bell. Далее следует идентификатор сессии Session ID: 53655 и версия Session Version: 53655 (как правило, используются одинаковые значения). Затем указывается тип сети Owner Network Type: IN (интеллектуальная сеть) и тип адреса IP4, а также сам адрес создателя Owner Address: 128.3.4.6. Записано название сессии (s) – SDP from Megacopi. Описание соединения (c) включает следующие параметры: тип сети – IN, тип адреса – IP4, адрес окончания – 100.100.105.133. В описании транспортной среды указывается:

- вид передаваемой информации – Media Type: audio – аудио;
- номер порта – Media Port: 40014;
- стек используемых протоколов Media Proto: RTP/AVP – передача аудио и видео информации поверх протокола RTP;
- тип используемого кодека – Media Format: ITU-T G.711 PCMA (т.е. номер протокола 8 соответствует ИКМ-кодеку G.711 с А-законом компандирования).

Для дескриптора удаленного окончания (Remote Descriptor)

приведена сокращенная запись расшифровка, которой аналогична записи для местного окончания. Удаленное окончание имеет:

- IP-адрес 149.204.67.216;
- временные параметры сессии (т.е. время начала и окончания) равны нулю $t=0$, поскольку сессия еще не началась;
- тип передаваемой информации – аудио;
- используемый порт – 30512;
- тип кодека – G.711 с А-законом компаундирования.

На рис. 6.3 представлен процесс получения информации о событиях от шлюза MGW.

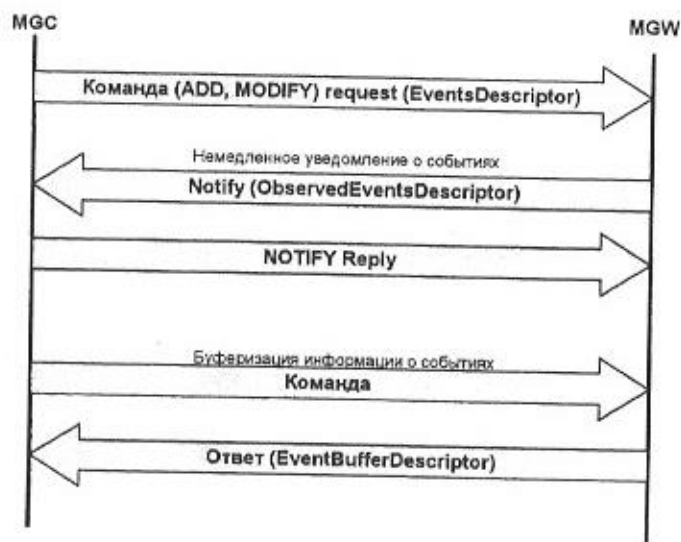


Рисунок 6.3 Процесс получения информации о событиях от шлюза MGW

Дескриптор событий (EventsDescriptor) служит для информирования шлюза MGW о событиях, подлежащих регистрированию и о которых должен оповещаться MGC. Дескриптор содержит идентификатор запроса и список событий, которые должны регистрироваться (hook-on или hook-off, прием DTMF-сигнала и т.д.).

Реакция MGW на такой запрос со стороны MGC может быть различной в зависимости от значения параметра EventControlBuffer

в дескрипторе состояния окончания (TerminationStateDescriptor):

1. Если значение параметра EventBufferControl = Off, то информация о событиях немедленно отправляется в MGC в формате команды Notify (которая содержит ObservedEvents-Descriptor).
2. Если EventBufferControl = On, то информация о событиях может накапливаться в буфере и передаваться в MGC в дескрипторе EventBufferDescriptor.

В шлюзах различных типов могут использоваться окончания, имеющие большие различия в характеристиках. Для организации корректного взаимодействия между MGW и MGC в протоколе MEGACO имеется механизм, позволяющий шлюзу MGW передавать в программный коммутатор MGC информацию о свойствах окончаний. MGC может запросить информацию о свойствах окончания при помощи команды Auditvalue. В ответе на команду информация о свойствах окончания будет представлена в виде пакетов (Packages) (рис. 6.4).

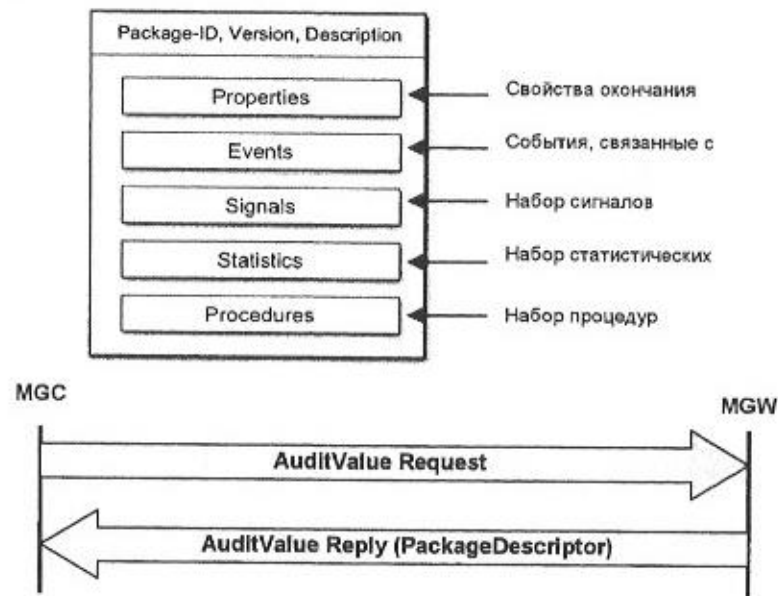


Рисунок 6.4 Структура типового набора характеристик и процесс его получения от шлюза

Типовой набор характеристик (Package) содержит общее описание пакета, его идентификатор и следующие разделы:

- раздел *Properties* определяет свойства и для каждого свойства содержит его идентификатор, тип, допустимые значения, характеристики (чтение или запись);
- раздел *Events* содержит информацию о событиях, идентификатор (с каждым типом события связывается идентификатор события), допустимые параметры дескриптора EventsDescriptor и параметры дескриптора ObservedEventsDescriptor;
- раздел *Signals* определяет набор сигналов. С каждым сигналом связывается идентификатор, и определяются параметры (например, сигналы ответа станции);
- раздел *Statistics* определяет статистические параметры, регистрируемые MGC. С каждым таким параметром связывается идентификатор, и определяются его характеристики;
- раздел *Procedures* определяет дополнительные аспекты использования типового набора.

Команда **ADD** служит для добавления окончания к контексту. В рамках MEGACO определено 13 типовых наборов, определяющих свойства окончания. Более подробно примеры основных и дополнительных наборов рассмотрены в [3].

Рассмотрим запись транзакции с командой Add, приведенной на рис. 6.5.

Сообщение содержит идентификатор транзакции Transaction ID: 184, идентификатор контекста Context: Choose one (означает, что контекст еще не создан и шлюз должен присвоить ему идентификатор).

Командная строка содержит идентификатор окончания A=tdm/1/7 (т.е. указан физический порт 1(E1), 7-ой временной интервал). Если вместо идентификатора окончания используется специальный символ \$, то это означает, что окончание не определено.

В зависимости от типа окончания оно может быть либо создано (окончание RTP-соединения) или извлечено из нулевого контекста. Если сообщение не содержит идентификатора контекста, то это означает, что должен быть создан новый контекст.

Команда может содержать характеристики окончания, задан-

ные в виде дескрипторов окончания. В рассматриваемом примере Media Descriptor физического порта содержит только Local Control Descriptor: MO=SR, который указывает, что порт работает в двухстороннем режиме (передача/прием).

```
MEGACO
Version: 1
MediagatewayID: [172.23.94.2]
Transaction: Request
Transaction ID: 184
Context: Choose one
Command line: A=tdm/1/7
Command: Add
Termination ID: tdm/1/7
Media Descriptor
M{O{M
Local Control Descriptor: MO=SR
Mode: SR
Command line: A=$
Command: Add
Termination ID: WildCard any
Media Descriptor
M{L{\n
Local Descriptor: v=0\r\no=bell 53655 53655 IN IP4
128.3.4.6\r\nnc=IN IP4 $ \r\nm=audio $ RTP/AVP 8\r\n}}}
```

Рисунок 6.5 Запись транзакции с командой Add.

Для RTP окончания порт еще не выбран A = \$, но указано Termination ID: WildCard any – возможно только полное разъединение. Также приведен локальный дескриптор, не все характеристики которого уже определены.

В ответе (Reply) на транзакцию, следующем на команду Add будет обязательно содержаться идентификатор созданного контекста, полное описание местного окончания Local Descriptor, а также могут содержаться дополнительные дескрипторы, такие, как Mux, Observed Events или Statistics.

Команда **SUBSTRACT** служит для удаления окончания из контекста (рис. 6.6). Сообщение содержит идентификатор транзакции

Transaction ID: 187, идентификатор контекста Context: 18. Сама команда может иметь идентификатор окончания, а также опционально может содержать дескриптор Audit.

Удаление последнего окончания из контекста означает разрушение контекста. Если в качестве идентификатора окончания указывается специальный символ (*), то это означает удаление всех окончаний из контекста.

MEGACO

```
Version: 1
MediagatewayID: [172.23.94.2]
Transaction: Request
Transaction ID: 187
Context: 18
Command line: S=*}}\nK
Command: Subtract
Termination ID: WildCard all
T=187{C=18{S=*}}\n
```

Рисунок 6.6 Запись транзакции, содержащей команду Subtract

В ответе на эту команду могут содержаться дополнительные дескрипторы, такие, как Mux, Observed Events или Statistics. По умолчанию ответ содержит дескриптор Statistics.

На рис. 6.7 приведены параметры дескриптора Statistics (S). Статистические данные относятся к физическому порту или виртуальному RTP-порту. По каждому порту указывается продолжительность соединения (dur=6200) в секундах, число переданных октетов (os=48960) и принятых октетов (or=47040). Для RTP-порта также указываются значения числа переданных пакетов (ps=308), принятых пакетов (pr=294, числа потерянных пакетов (pl=0), измененное значение джиттера (jit=4) и среднее время задержки в мсек (delay=25).

Команда **MOVE** служит для перемещения окончания из текущего контекста в контекст, идентификатор которого указан в сообщении. Сообщение содержит идентификатор транзакции и идентификатор контекста. Сама команда содержит идентификатор окончания и дескрипторы окончания. В ответе, следующем на команду, могут содержаться дополнительные дескрипторы (такие

же, как в случае команды **ADD**). Команда **MOVE** является единственной командой, которая выполняется не только с контекстом, идентификатор которого указан в сообщении.

MEGACO

```
Version: 1
MediagatewayID: [149.204.67.133]
Transaction: Reply
Transaction ID: 188
Context: 46
Command line: S=*}}\nK
Command: Subtract
P=188{C=46{S=tdm/5/4{SA{nt/dur=6150,nt/os=48960,nt/or=47040}},
S=rtp/1/0/40014{SA{nt/dur=6200,nt/os=49280,nt/or=47040,tp/ps=308,
rtp/pr=294,rtp/pl=0,rtp/jit=4,rtp/delay=25}}}}
```

Рисунок 6.7 Запись транзакции ответа на команду Subtract, содержащая статистические данные о разговоре

Команда **MODIFY** служит для модификации характеристик окончания. Сообщение содержит идентификатор транзакции и идентификатор контекста. Сама команда имеет идентификатор окончания. В ответе на команду могут содержаться дополнительные дескрипторы, такие, как Mux, Observed Events или Statistics.

Команда **AUDIT VALUE** служит для получения информации об окончании. Сообщение содержит идентификатор транзакции и идентификатор контекста. Сама команда имеет идентификатор окончания, а также опционально может содержать дескриптор Audit.

Команда **AUDIT CAPABILITIES** используется для проверки возможных свойств, событий или сигналов одного или нескольких окончаний. Данная команда отличается от предыдущей тем, что в результате ее выполнения программный коммутатор получит не только текущие значения запрошенных параметров, но и все их возможные значения.

Команда **NOTIFY** передается шлюзом к программному коммутатору для извещения о наступлении некоторых событий в шлюзе.

Команда **SERVICE CHANGE** посылается шлюзом к контроллеру для извещения последнего об изменении режима обслуживания одного или нескольких окончаний.

6.3 Порядок установления соединения через сеть NGN, управляемую программным коммутатором SX

Рассмотрим пример установления соединения между абонентами двух телефонных станций через IP-сеть, управляемую программным коммутатором А 5020 MGC (рис. 6.8).

На границе между исходящей телефонной станцией и IP-сетью установлен шлюз А 7505 MG, который выполняет функции транспортного и сигнального шлюзов. На границе между удаленной телефонной станцией и IP-сетью установлен шлюз А 7515 MG, который также выполняет функции транспортного и сигнального шлюзов. На рисунке приведены коды пунктов сигнализации обеих станций и программного коммутатора. Также указаны IP-адреса шлюзов и контроллера.

1. Исходящая станция посылает сигнальное сообщение ОКС №7 IAM (начальное адресное сообщение). Оно состоит из номера вызываемого абонента CPN=965711, идентификатора выбранной соединительной линии CIC=70 (1-ый порт E1, 7-ой канальный интервал), а также этикетки маршрутизации (DPC=11300, OPC=10269) по сигнальному звену SLS=6 в сигнальный шлюз А7505 MG. Сигнальный шлюз А7505 MG передает сообщение IAM в программный коммутатор А 5020 MGC в содержимом IP-пакета, который пересылается через ассоциацию SCTP в виде фрагмента данных DATA в первом потоке SID=1 с порядковым номером SSN=297 (см. подробную расшифровку в 5.3.4).

2. Программный коммутатор А 5020MGC обрабатывает сообщение сигнальное сообщение IAM и по номеру вызываемого абонента CPN=965711 определяет, что он включен в станцию А1000 C12 с PC=11300 и связь с ним должна осуществляться через шлюз А7515 MG. После этого, MGC начинает подготавливать установление RTP-сессии, для чего посылает к исходящему шлюзу А7505 MG сообщение протокола MEGACO (транзакция Р=184) с запросом на создание нового контекста, включающего физический порт 1,7-ой канальный интервал (A=tdm/1/7).

3. Транспортный шлюз А7505 MG создает новый контекст с номером C=18, который связывает физический порт A=tdm/1/7 с виртуальным портом A=rtsp/4. Виртуальное окончание № 4 имеет IP-адрес шлюза (149.204.67.216) и номер UDP-порта 30512, тип ко-

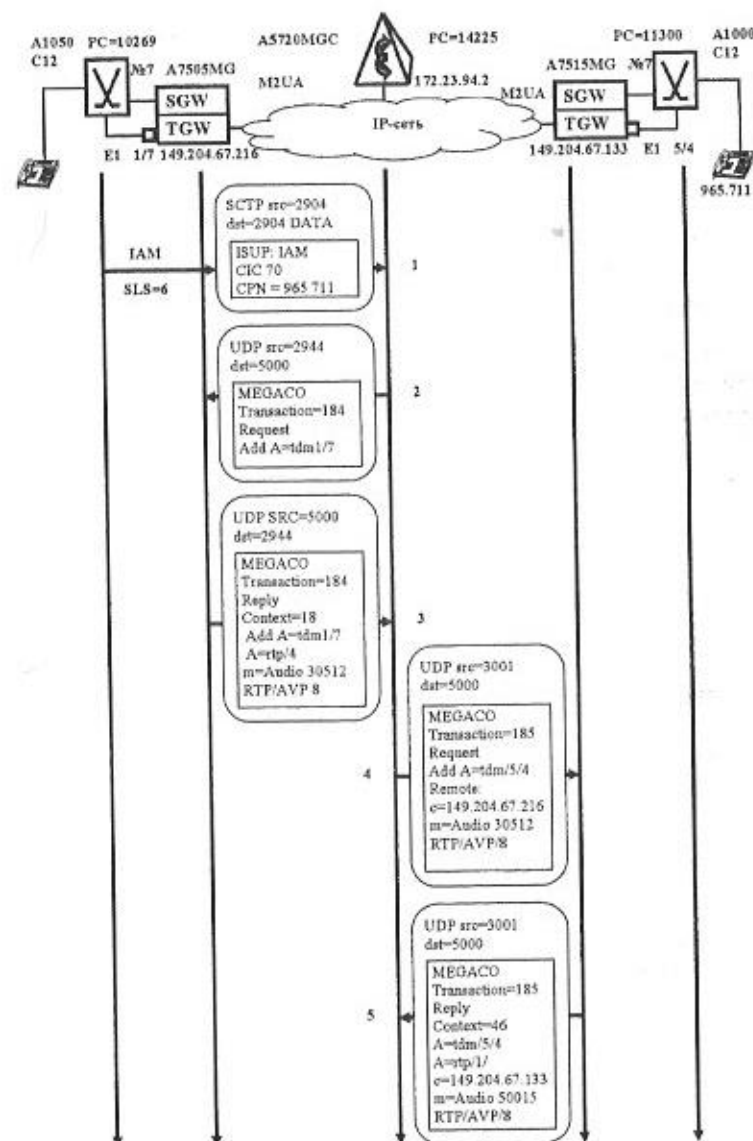


Рисунок 6.8 Временные диаграммы установления соединения между абонентами двух телефонных сетей через сеть NGN, управляемую программным коммутатором SX (этап 1-5)

дека G.711 с А-законом компрессирования. Информация о созданном контексте передается шлюзом в MGC в виде ответа (Reply) на транзакцию P=184.

4. MGC посылает в шлюз A7515 MG сообщение протокола MEGACO (транзакция 185) с запросом на создание нового контекста, включающего физический 5 порт E1, 4-ый канальный интервал (A=tdm/5/4). При этом, сообщение также содержит удаленный дескриптор (Remote Descriptor: v=0\r\no=bell 865833 865833 IN IP4 149.204.67.216\r\ns=SDP from Megacopi\r\nc=IN IP4 100.100.105.216\r\nt=0 0\r\nm=audio 30512 RTP/AVP 8\r).

5. Шлюз A 7515 MG создает новый контекст с номером C=46, который включает физический порт A=tdm/5/4 и виртуальный порт A=trp/1. Виртуальное окончание №1 имеет IP-адрес шлюза (149.204.67.133) и номер UDP-порта 40014, тип кода G.711с А-законом компрессирования. Информация о созданном контексте передается шлюзом в MGC в виде ответа (Reply) на транзакцию P=185.

6. После подготовки RTP-сессии на обоих шлюзах, MGC пересылает в удаленный сигнальный шлюз A7515 MG сообщение IAM. Оно содержит номер вызываемого абонента CPN=965711, идентификатор выбранной соединительной линии CIC=36 (5-ый порт E1, 4-ый канальный интервал) и этикетку маршрутизации (DPC=11300, OPC=10269) по сигнальному звену 4 в сигнальный шлюз A7505 MG. Поскольку в шлюзе реализован протокол M2UA, то содержимое сигнального сообщения IAM, также данные MTP2 и MTP3 вкладываются в блок данных (DATA) протокола SCTP и передаются в A 7515 MG.

7. MGC отправляет на шлюз A7505 MG сообщение протокола MEGACO (транзакция 186) с запросом на изменение (MODIFY) контекста C=18, с целью уточнения параметров удаленного окончания (Remote Descriptor: v=0\r\no=bell 865833 865833 IN IP4 149.204.67.133\r\ns=SDP from Megacopi\r\nc=IN IP4 100.100.105.133\r\nt=0 0 \r\nm=audio 40014 RTP/AVP 8\r\na=ptime:20).

8. В ответ на полученную команду (транзакция 186) шлюз A7505 MG посылает подтверждение о внесенном изменении в контекст C=18.

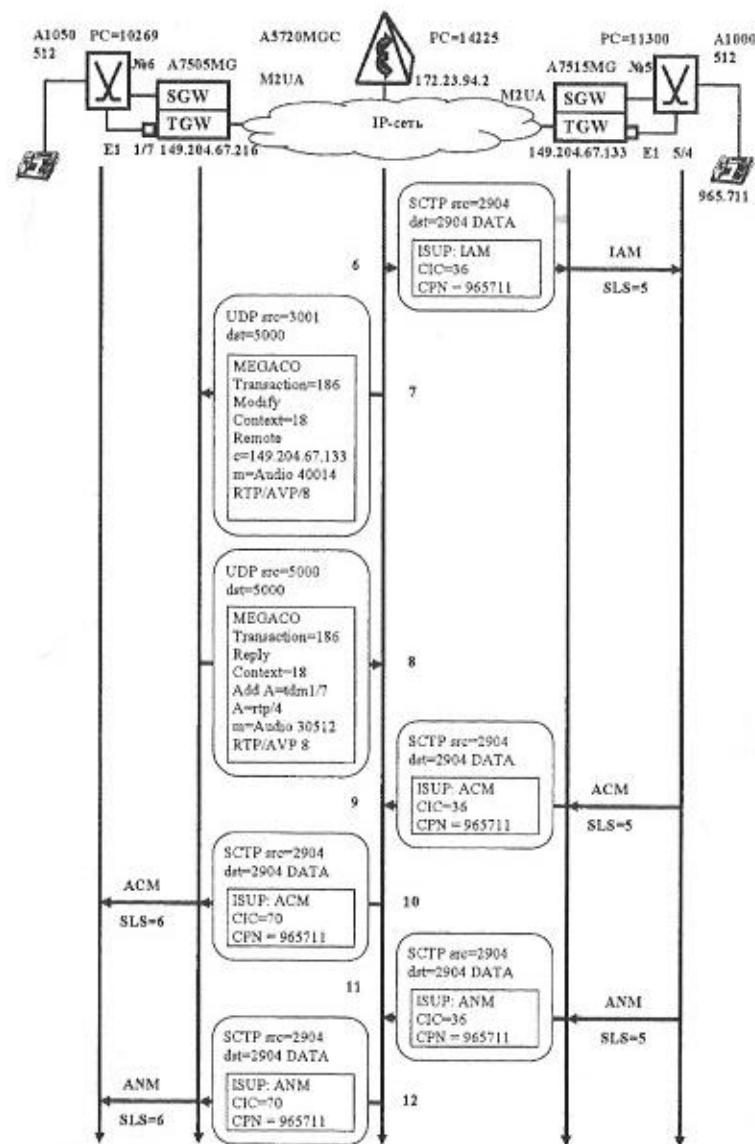


Рисунок 6.8 Временные диаграммы установления соединения между абонентами двух телефонных сетей через сеть NGN, управляемую программным коммутатором SX (этап 6-12)

9. Оконечная вызываемая станция посылает в программный коммутатор сигнальное сообщение ACM (Адрес полный) по сигнальному звену №4. Сигнальный шлюз A7515 MG вкладывает это сообщение в блок данных (DATA) протокола SCTP и отправляет данное сообщение к MGC.

10. MGC пересылает сообщение ACM в исходящий сигнальный шлюз A7505 MG. Шлюз пересылает это сообщение ОКС №7 в исходящую станцию по сигнальному звену №6.

11. Вызываемый абонент снимает трубку, и входящая коммутационная станция посылает в сигнальный шлюз A7515 MG сообщение ANM (ответ). Шлюз пересылает данное сообщение в MGC.

12. MGC пересылает сигнальное сообщение ОКС №7 ANM к исходящему сигнальному шлюзу A7505 MG, который отправляет его на исходящую станцию по сигнальному звену №6.

После этого абоненты переходят к разговору. Звуковые пакеты пересылаются между шлюзами по установленной RTP сессии: исходящий шлюз – сокет: 149.204.67.216:30152, входящий сокет – 149.204.67.133:40014. При этом на исходящей стороне связь с соединительной линией на 1 порту/7-ой канальный интервал с виртуальным портом определяется контекстом C=18. На входящем шлюзе связь с соединительной линией на 5 порту/4-ый канальный интервал с виртуальным портом №1 определяется контекстом C=46.

13. Абонент, осуществивший вызов, первым заканчивает разговор и кладет трубку. Исходящая станция посылает сообщение Release с указанием причины разъединения Cause = 16 (нормальное разъединение) в сигнальный шлюз A 7505 MG. Шлюз отправляет сигнальное сообщение Release в виде блока данных протокола SCTP к MGC.

14. MGC начинает разрушение RTP-сессии, отправляя в шлюз A 7505 MG сообщение MEGACO (транзакция 187) с командой SUBSTRACT (удалить) контекст C=18.

15. Шлюз A 7505 MG удаляет контекст C=18 и отправляет ответ Reply, который также содержит статистические данные (Statistics) по завершенной сессии.

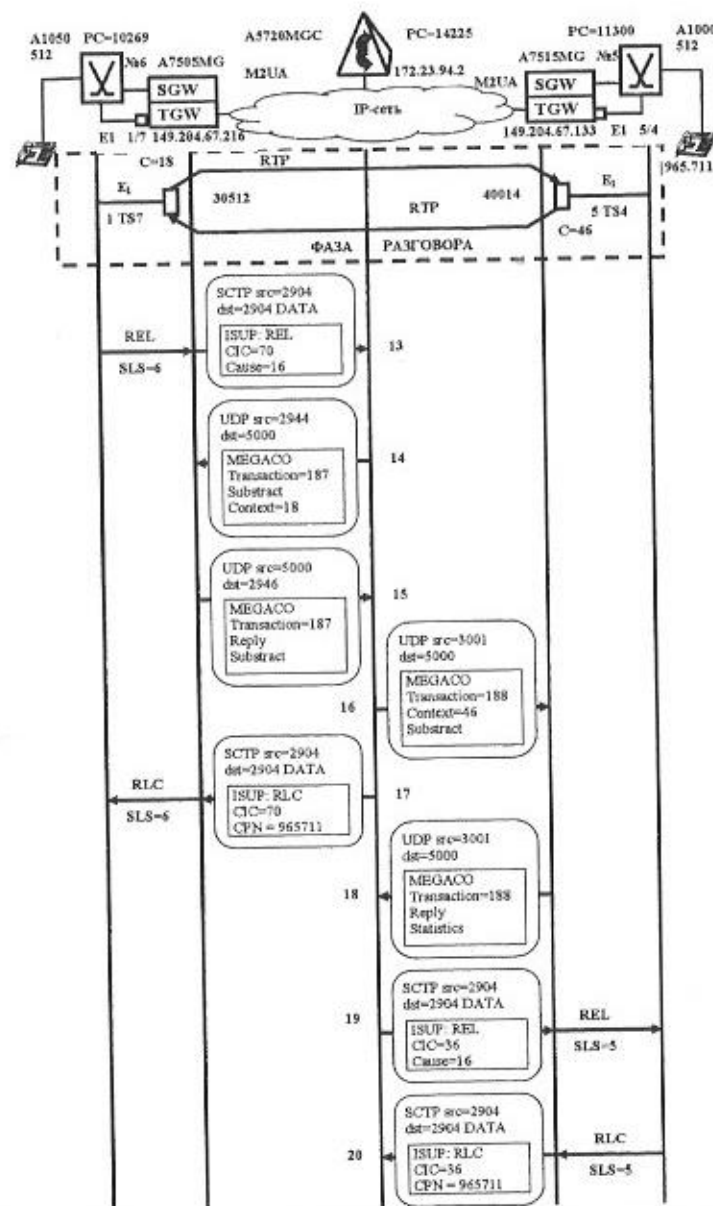


Рисунок 6.8 Временные диаграммы установления соединения между абонентами двух телефонных сетей через сеть NGN, управляемую программным коммутатором SX (этап 13-20)

16. MGC отправляет в удаленный шлюз A 7515 MG сообщение MEGACO (транзакция 188) с командой SUBSTRACT (удалить) контекст C=46.

17. Программный коммутатор MGC посылает в исходящий сигнальный шлюз A 7505 MG сообщение Release Complete (RLC – освобождение завершено) с указанием освобождаемой соединительной линии CIC=70. Сигнальный шлюз A 7505 MG пересылает сообщение RLC к исходящей станции через сигнальное звено №6.

18. Транспортный шлюз A 7515 MG отвечает на транзакцию 188 сообщением Reply об успешном удалении контекста C=46 и передает в MGC статистические данные по завершенной сессии.

19. Программный коммутатор MGC посылает в сигнальный шлюз A 7515 MG сообщение Release, которое транслируется последним к входящей телефонной станции.

20. Входящая коммутационная станция посылает в MGC сообщение RLC (освобождение завершено).

Детальная трассировка процессов установления сессии и ее завершения представлена в приложении 3. Читателям предлагается самостоятельно прочитать приведенную трассировку.

Контрольные вопросы и задания

1. Могут ли входить в один контекст следующие порты: A=tdm/1/7, A=rtp/4 и A=tdm/5/4?
2. Назовите команду MEGACO, при помощи которой MGC может получить информацию о текущих параметрах заданной сессии.
3. Какую команду должен отправить MGC, для того, чтобы изменить состояние порта MO=RC (только прием) на состояние MO=SR (прием и передача)?
4. Укажите номера портов, которые используются в MGC для приема и передачи сигнальных сообщений M2UA и сообщений MEGACO.
5. Рассчитайте число пакетов, переданных и принятых в RTP-сессии, трассировка которой приведена в приложении 3.

Глава 7 ПРИНЦИПЫ ПОСТРОЕНИЯ ЗАЩИЩЕННЫХ СЕТЕЙ NGN

7.1 Необходимость защиты информации в NGN

Существуют три типа причин, по которым обеспечение защищенности в сетях NGN требует значительно больше затрат, чем в традиционных телефонных сетях общего пользования. К этим типам причин относятся:

- Технологические;
- Законодательные;
- Организационные.

7.1.1 Технологические изменения

Технология сетей следующего поколения движется от закрытых корпоративных решений к открытым приложениям. В отличие от сети ТфОП, инфраструктура которой предназначена для передачи речи, инфраструктура NGN изначально используется для служб передачи голоса, данных и мультимедийных служб. NGN работает с разными типами доступа и сервис провайдерами. Она также может поддерживать дополнительные услуги. Например, интеллектуальные услуги (IN), которые могут реализовываться на открытых сервисных платформах (OSP), принадлежащих другим операторам.

Существующая сеть ТфОП характеризуется закрытыми технологиями. МСЭ-Т определил сигнализацию ОКС №7 как глобальный телекоммуникационный стандарт, который описывает процедуры взаимодействия элементов сети ТфОП через цифровую сеть сигнализации для обеспечения процессов установления соединений, маршрутизации вызовов и управления. Такие сети являются закрытыми и в значительной степени изолированными от других сетевых служб. Так же значительно меньшее число пользователей разбирается в протоколах сигнализации ОКС №7, чем, например, в протоколе SIP. В сети ТфОП в основном используется сигнализация по выделенным (не пользовательским) каналам. Это само по

себе обеспечивает некоторый уровень защиты от угроз со стороны конечных пользователей. Оконечные устройства пользователей являются закрытыми («черными ящиками») и не дают возможностей для некорректного использования сетевых устройств. В сетевых центрах используется специфическое закрытое программное обеспечение. Таким образом, благодаря закрытому характеру всей инфраструктуры операторы поддерживают полный контроль над всеми сетевыми интерфейсами.

С другой стороны, сети следующего поколения имеют достаточно открытую архитектуру, обеспечивающую большую гибкость и взаимодействие. Они используют общеизвестные межконцевые протоколы, ориентированные на технологию IP. В отличие от ТфОП, технологии IP более широко известны, чем внутренние протоколы телефонных сетей. Сетевая инфраструктура NGN открыта для совместного использования различными службами. Такими как передача речи, данных и мультимедийных служб, включая доступ в Интернет и услуги, предоставляемые сторонними компаниями (не являющимися владельцами сети). Сообщения сигнализации и управления передаются в одном канале вместе с данными пользователя. Компоненты сетей NGN также используют общеизвестные аппаратные платформы и программное обеспечение.

Оконечные устройства пользователей тоже развиваются в сторону открытых платформ, таких как, например, персональные компьютеры. В конечном счете, открытые интерфейсы были созданы для поддержки приложений, разработанных сторонними компаниями для провайдеров услуг.

7.1.2 Законодательные изменения

Правительства разных стран инициируют законы, по которым на операторов телекоммуникационных сетей возлагается все большая ответственность за защищенность критических инфраструктур. В них сети передачи голоса и мультимедийные службы составляют основу. Это происходит без учета классических требований по защищенности, которые уже существуют в сети ТфОП и приобретают все большую значимость в связи с эволюцией к пакетным сетям (например, требования к легальному прослушиванию, которые могут оказывать влияние на всю систему защиты,

требования по поддержке вызовов к аварийным службам и т.д.).

Все эти требования хорошо реализованы в сети ТфОП, но при реализации сетей NGN они вызывают дополнительные трудности. В 2002 году OECD (Organization for Economic Cooperation & Development) опубликовала руководящие указания, в которых рекомендовано рассматривать защищенность как фундаментальный элемент всех продуктов, служб, систем и сетей, а также как неотъемлемую часть всех разрабатываемых систем и архитектур.

В Европе существует директива ЕС по защите информации. Она требует от операторов и провайдеров услуг гарантировать, что их инфраструктура и службы были надежно защищены и услуги, предоставляемые пользователям, тоже являлись защищенными. Более того, пользователи должны быть извещены о возможных рисках, с которыми они могут столкнуться при нарушении защиты в предоставляемых услугах.

7.1.3 Организационные изменения

Фундаментальные изменения на рынке телекоммуникаций также усложняют вопросы по организации защиты информации. Относительно высокие темпы смены персонала, как в компаниях-производителях телекоммуникационного оборудования, так и в компаниях-операторах сетей повышают риски того, что новый персонал может предпринять несанкционированные действия. Поскольку персонал компаний операторов больше не представляет собой небольшой клуб единомышленников, в котором каждый знает остальных коллег, поддерживать доверительные отношения становится все труднее. Такие аспекты оказывают влияние на общий уровень защищенности внедряемых сетей NGN. Это фактически увеличивает риск внутренних атак, которые должны учитываться с той же степенью серьезности, как и внешние атаки.

7.1.4 Причины необходимости защиты информации в NGN

При внедрении защищенных сетей NGN операторы должны стремиться к следующим целям и принимать во внимание следующие соображения:

- минимизировать дополнительные затраты на защищенное ре-

шение путем выбора оптимального решения, которое исключит непомерные затраты (базовый принцип выбора защищенного решения на основе оценки стоимости возможного ущерба);

- применять наиболее общие защищенные решения, применимые к большинству приложений и служб NGN, которые оказывают минимальное влияние на архитектуру и размещение сетевых элементов;
- убедиться, что примененные меры защиты корректно взаимодействуют друг с другом, так чтобы не возникало проблем с их взаимодействием, которые могут привести к возникновению «дыр» в системе защиты;
- убедиться в том, что учтены требования по обеспечению качества обслуживания мультимедийного трафика (QoS). Передача речи требует обеспечения особых условий по передаче (гарантированная полоса пропускания) и работе в режиме реального времени (ограничения на задержки и джиттер пакетов голосового трафика, а также своевременная передача сигнальных сообщений). В мультимедийных приложениях также имеются ограничения. Например, при передаче видеосигналов требуется учитывать их чувствительность к потерям пакетов. Любые защитные мероприятия, а в особенности механизмы кодирования информации, должны соответствовать установленным ограничениям. Такие меры защиты как кодирование влияют на пропускную способность каналов и быстродействие сетевых центров в сетях VoIP. Требования по обеспечению режима реального времени ограничивают число защитных шлюзов, которые могут размещаться на пути потока голосовых пакетов без значительного увеличения времени задержки и джиттера.

Передача речи также требует надежности 99,999 и выполнения таких требований, как легальное прослушивание и гарантированный доступ к спецслужбам, что необходимо для получения лицензии на операторскую деятельность.

Выполнение этих требований приводит к значительному усложнению традиционных сетей. Такие требования обычно не предъявляются к сетям передачи данных, а легальные требования

к сетям по технологии VoIP еще не разработаны. В настоящее время инфраструктура сетей VoIP часто включает механизмы переключения на традиционные системы в случае аварии и для обеспечения доступа к спецслужбам.

В конечном счете, для выбора защищенного решения критическим фактором является простота его использования конечным пользователем. Это также включает простоту усовершенствования системы защиты с применением новых технологий при минимальном влиянии на инфраструктуру.

7.2 Анализ уязвимостей и факторов риска в NGN

Сети следующего поколения (NGN), как и всякая открытая система подвержены атакам различных нарушителей, которые используя системные недоработки, стремятся часто не только получить доступ к чужой персональной информации, но иногда и разрушить функциональность всей сети в целом. В настоящее время существует большое число публикаций по информационной безопасности [5, 7, 10], для сохранения преимущества воспользуемся определениями и терминами, приведенными в книге [7].

7.2.1 Основные понятия и определения

Информационная безопасность – это комплекс мер по обеспечению защиты информации от внешних или внутренних угроз: от нежелательного разглашения, искажения, утраты или снижения степени доступности информации, а также от ее незаконного тиражирования, которые приводят к материальному или моральному ущербу для владельца или пользователя информации.

Угрозы (threats) – потенциально возможные события, действия или процессы, которые посредством воздействия на компоненты сети могут привести к нанесению ущерба.

Уязвимость (vulnerability) – характеристика или свойство системы, использование которой нарушителем может привести к реализации угрозы. Таким образом, уязвимости – это слабые места системы, которые могут быть использованы как для нарушения ее функциональности, так и для получения информации.

Вторжение (intrusion) – процесс попытки несанкционирован-

ного проникновения в какой-либо элемент сети. Под вторжением может пониматься любое действие нарушителя, приводящее к реализации угрозы путем использования уязвимостей (реализовавшаяся угроза).

Атака (attack) – это событие, при котором нарушитель проникает внутрь системы или совершает по отношению к ней какое-либо несанкционированное действие. Атака является результатом вторжения.

Злоупотребление (misuse) – это действие, которое нарушает стратегию использования сети, которое может заключаться в краже паролей или засорении сети спамом. В отличие от вторжения, злоупотребление не предполагает активных действий, направленных на разрушение системы защиты сети.

Обнаружение вторжений (intrusion detection) – это процесс обнаружения несоответствующих, неправильных или аномальных действий и событий в сети. Следует различать обнаружение вторжений и обнаружение злоупотреблений. При вторжении атака начинается извне сети, тогда как злоупотребление начинается после первоначального санкционированного входа в сеть, то есть происходит внутри сети.

Система обнаружения вторжений (Intrusion Detection System, IDS) – это система, обеспечивающая своевременное обнаружение вторжений.

Система предотвращения вторжений (Intrusion prevention System, IPS) – это система, обеспечивающая выявление и предотвращение вторжений.

Риск нарушения информационной безопасности (security risk) – это фактор, отражающий возможный ущерб компании от реализации угрозы информационной безопасности.

Нарушитель (intruder) – это лицо, совершающее несанкционированные, противоправные действия в отношении сети и передаваемой в ней информации.

Объект защиты (security object) – это любой объект сети (шлюз, программный коммутатор, сервер приложений, рабочая станция управления...), для которого проводится обнаружение вторжений и выполняются мероприятия по защите.

Аудит (audit) – это получение информации о системе, касающейся контроля ее функционирования и внутреннего поведения.

Существуют международные стандарты по обеспечению информационной безопасности: ISO/IEC 15508 «Информационная технология – методы защиты – критерии оценки информационной безопасности» и ISO/IEC 17799 «Управление информационной безопасностью», которые также приняты в Российской Федерации, и которые определяют основные подходы к анализу рисков и определению уязвимостей. Воспользовавшись этой методикой, попробуем рассмотреть с этих позиций сети следующего поколения.

7.2.2 Наиболее вероятные риски в NGN

Для того, чтобы компании операторы могли разрабатывать меры защиты, необходимо точно определить главные риски и атаки, которым могут быть подвержены сети NGN. Это можно сделать путем анализа возможных воздействий и точек их возможного приложения.

Примерами источников дополнительных рисков могут быть следующие факторы:

- Большое число точек соединений с другими операторами, с приложениями сторонних производителей и сервис провайдерами (например, через шлюзы OSA/Parlay), а также с публичным Интернетом.
- Совместное использование сетевой инфраструктуры NGN несколькими сервис провайдерами 2 и 3 уровней.
- Наличие общего физического доступа для пользовательского и сигнального трафика в NGN облегчает прослушивание и манипуляции в инфраструктуре по сравнению с сетью ТфОП. Например, путем вторжения и установления шпионского программного обеспечения на пользовательских устройствах и сетевых узлах через удаленный доступ.

Кроме собственно инфраструктуры NGN, новое абонентское оборудование в силу своей открытости и мультимедийности может являться источником злонамеренных потоков (атаки типа отказ в обслуживании), вирусов, направленных как на операторские системы, так и на оборудование пользователей (включая спам). Операторы должны обеспечивать своих пользователей средствами защиты и фильтрации пользовательского трафика для защиты от

атак других пользователей (удаление вирусов и «червей» и подавление спама).

Поскольку в настоящее время пользователи имеют возможность управлять своим оборудованием, риски включают возможность кражи услуг и подделку биллинговых записей за счет третьей стороны (т.е. со стороны собственных или посторонних абонентов) маскирующейся под легального пользователя. Подделки также включают неавторизованный доступ к дорогим и привлекательным номерам 9xxx.

Поскольку в настоящем пособии рассматривается только фиксированный широкополосный доступ через DSL, то возникающие дополнительные риски, связанные с беспроводными технологиями доступа к инфраструктуре NGN (беспроводный Bluetooth, WiFi IEEE 802.11x) не будут анализироваться. Однако, по мнению операторов именно беспроводные технологии предоставляют наиболее уязвимые участки сети. В конечном счете, взаимодействие между ТфОП и NGN добавляет риски к возможности нарушения инфраструктуры сети ТфОП. Например, путем атаки на сеть ОКС №7 за счет вторжения на сигнальный шлюз. Хотя технически это возможно, но маловероятно, поскольку такое вторжение потребует взламывания нескольких уровней защиты.

7.2.3 Анализ мультимедийной архитектуры NGN

Обобщенная архитектура мультимедийной NGN, включающей узлы 4/5 классов, IP Centrex, видеоконференцию и мультимедийные приложения приведена на рис. 7.1. На нем отражены основные сетевые элементы и их приложения.

Анализ угроз для такой архитектуры включает систематическое и полное исследование всех составляющих: доменов и сайтов, сетевых элементов, интерфейсов и потоков между ними с целью определения возможности вторжения через каждый из перечисленных элементов. Результатом анализа должен являться список возможных угроз для сетевых элементов, сигнализации и управления. Большинство угроз может быть распределено по категориям. Например, отказ от обслуживания (DoS), прослушивание (Intruding), неавторизованный доступ и т.п. В документах ETSI TIPHON [8.2] приводится типовое распределение угроз по категориям. Угрозы, представляющие риски для защищаемых объектов в

соответствии с определением ETSI TIPHON, можно разделить на нарушения: конфиденциальности, целостности, доступности и отчетности. В программе TIPHON также изучалось соответствие между угрозами и объектами защиты.

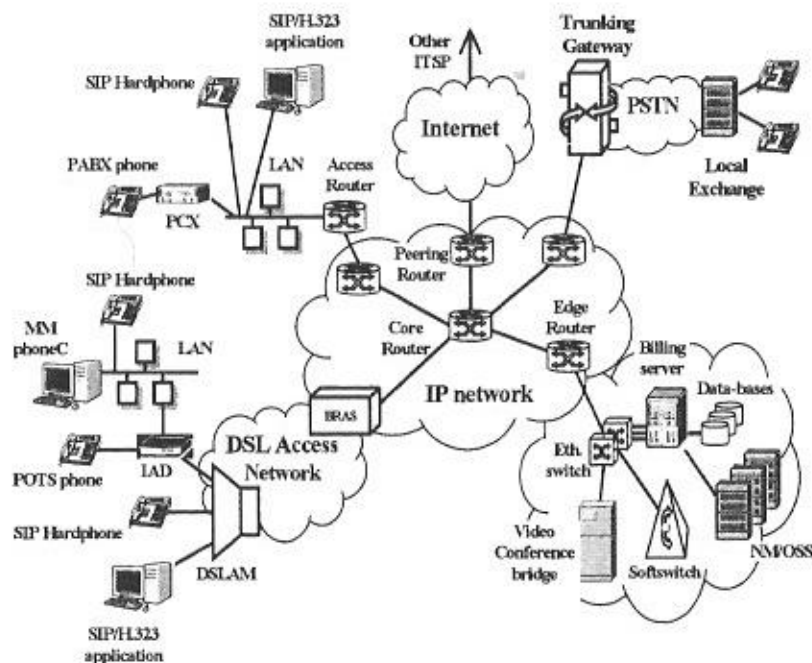


Рисунок 7.1 Структура мультисервисной сети NGN класса 5

Особую группу составляют протоколы – ориентированные угрозы. Например, специфические угрозы для протокола SIP включают симуляцию сообщений REGISTER, INVITE, BYE, несанкционированную посылку сообщений CANCEL и BYE. Специфическими угрозами для протоколов MGCP и MEGACO/H.248 являются, например, отказы в обслуживании, вызванные перегрузкой ресурсов сети за счет несанкционированных операций Add/Create Connection или избыточными операциями Modify/Modify Connection, влияющими на качество обслуживания (QoS). Сравнительный анализ возможных угроз и атак на сеть NGN является основой для создания защищенного решения, которое описывается в следую-

щем разделе.

В конечном счете, в будущем будут возникать новые виды угроз и обнаруживаться новые уязвимые места, которые потребуются анализировать. Наилучшее решение по организации защиты должно обеспечивать достаточную гибкость для отслеживания динамических изменений без нарушения целостности процесса защиты.

7.2.4 Необходимость приоритезации задач защиты сети

Расстановка приоритетов в области требований по организации защиты – это задача компании-оператора. Операторы сетей общего пользования оценивают риски в соответствии с типами их абонентов и спецификой предоставляемых служб. Они последовательно определяют уровни приоритетов для тех рисков, которые должны быть устранены в первую очередь. Хотя возможны существенные различия между подходами различных операторов, существует общий набор требований по безопасности, признаваемый всеми.

Во-первых, доступ к спецслужбам и легальное прослушивание по своей сути являются незащищенными услугами. Операторов обязывают предоставлять их. Следовательно, эти услуги должны предоставляться относительно защищенным способом.

Во-вторых, самым главным для каждого производителя является разработка глобальной защищенной архитектуры.

В-третьих, на основе требований операторов и глубокого анализа угроз, проведенного компаниями-производителями оборудования NGN, наивысший приоритет должен быть присвоен следующим аспектам:

- уменьшению влияния атак типа отказ в обслуживании (DoS) или распределенный отказ в обслуживании (DDoS), организованных конечными пользователями;
- решениям по аутентификации (как администраторов, так и конечных пользователей);
- обнаружению вторжения (IDS) и предотвращению вторжений (IPS);
- уменьшению влияния внутренних атак;

- защитному тестированию и защите сетевых элементов;
- процессу контроля уязвимости;
- средствам контроля доступа и аудирования;
- стандартам, которые должны поддерживаться.

Поясним основные из перечисленных аспектов. Значительная часть угроз устраняется корректными процедурами аутентификации. Однако если вторжение уже произошло, то защита от сетевых атак должна выполняться эффективной системой обнаружения и предотвращения вторжений (IDS/IPS).

Важную роль в системе защиты играет защитное тестирование, которое выполняется при помощи стандартных или корпоративных средств для систематического и полного тестирования всех известных уязвимостей в сети. Средства аудирования обеспечивают своевременное закрытие всех неиспользуемых служб и услуг (т.е. закрытие неиспользуемых портов и выключение неиспользуемых приложений).

Значительное усиление защиты достигается за счет рассылки и включения программных вставок и/или в быстром переходе на новые программные версии, чем устраняются ранее выявленные уязвимости. Большую роль играют постоянный контроль за персоналом и постоянное повышение его квалификации.

7.3 Виртуальные частные сети (VPN) – основа защищенного решения

Главной целью построения защищенной сети NGN является достижение уровня безопасности, сравнимой с безопасностью сетей ТфОП. Лучшим случаем является ситуация, когда вся инфраструктура сети NGN принадлежит одному оператору. Тогда у оператора появляется возможность применять сквозные меры по защите на уровне доступа, транспорта и уровня управления коммутацией.

Основой защищенного сетевого решения является разделение единой транспортной среды на изолированные друг от друга виртуальные частные сети (VPN). При этом разделение на VPN выполняется по следующим принципам:

- трафик голоса должен быть отделен от трафика данных;

- сигнальные сообщения должны передаваться в отдельной VPN;
- управляющие сообщения должны передаваться в отдельной сети.

Таким образом, в инфраструктуре сети NGN должны быть выделены, по крайней мере, 4 виртуальные сети:

1. сеть для голосовых и мультимедийных приложений;
2. сеть для передачи данных;
3. сеть для протоколов сигнализации;
4. сеть управления сетевыми элементами.

На рис. 7.2 представлена схема построения виртуальных частных сетей VPN при использовании на транспортной сети технологии IP/MPLS (служба 3-его уровня VPRN). Применение этой технологии позволяет при наличии единой транспортной IP-сети создать в каждом маршрутизаторе независимые VRF (см. подробнее в 1 части пособия). В рассматриваемом случае на уровне транспорта организованы 4 независимых VPN:

- VPN 1 – для передачи сигнализации (H.248, MEGACO, SIGTRAN...);
- VPN 2 – для передачи голоса и видео (RTP/RTCP...);
- VPN 3 – для передачи данных (HTTP, FTP...);
- VPN 4 – для управления сетью (SNMP, TFTP...).

Как видно из рис. 7.2 различные сетевые элементы подключаются в разные VPN в соответствии с типами передаваемого трафика. Так программный коммутатор подключается только к VPN 1 для получения и отправки сигнализационных сообщений и к VPN 4 для соединения с сетевой платформой управления BSS/OSS. Шлюзы имеют выходы на VPN 1, 2 и 4, поскольку в VPN 2 передается голосовой и видео трафик. Мультиплексоры DSLAM подключаются к VPN 3 для передачи данных и к VPN 4 для поддержки сетевого управления.

Поскольку в каждом маршрутизаторе реализованы независимые VRF, то на уровне транспорта происходит полное разделение всех потоков. На уровне доступа разделение потоков производится за счет организации виртуальных локальных сетей VLAN.

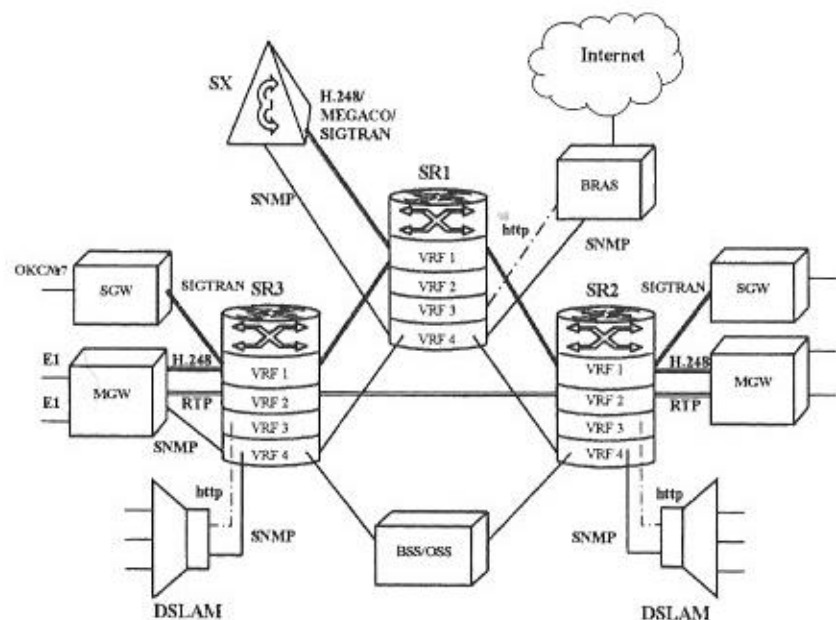


Рисунок 7.2 Организация VPN и подключение к ним сетевых элементов NGN

Для того, чтобы считать решения, построенные на VPN достаточно надежными, должны выполняться следующие условия:

- сетевая инфраструктура не может подвергаться рискам. Это предполагает наличие системы управления сетевой защитой;
- если для управления используется протокол SNMP, то должны применяться дополнительные средства защиты, описанные в SNMP v.3;
- доступ к сетевым элементам по простым и незащищенным протоколам FTP и telnet должен быть запрещен. Это предполагает замену FTP на удаленный login, а telnet на SSH (SSH обеспечивает защищенную альтернативу удаленной процедуре login (telnet, rsh), передаче файлов (ftp) и пересылке с портов TCP/IP или X.11 с защищенностью эквивалентной SSL/TLS);
- для приложений управления сообщения сигнализации передаются поверх стека CORBA/TCP, со специальной защитой на

транспортном уровне (TLS), использующей взаимную аутентификацию сетевых элементов и кодирование сигнальных сообщений;

- для всего персонала эксплуатации любой вид административного доступа требует регистрации (login) и ввода пароля. Это запускает процедуры аутентификации, контроля доступа, мониторинга и записи в файл хранения системных сообщений.

Предположения, сделанные при описании сценария защиты на базе VPN, позволяют в определенной степени облегчить требования по защищенности. Инфраструктура VPN позволяет исключить некоторые виды угроз присущие пользовательскому доступу. Например, несанкционированный перехват сигнальных или пользовательских сообщений, нелегальное проникновение в узлы, а также изменение сигнальных и пользовательских сообщений.

Однако, данный сценарий не исключает возможных атак от индивидуальных или корпоративных пользователей. Никогда нельзя доверять оборудованию пользователя. Оконечное оборудование может быть IP-телефоном с протоколами SIP или H.323, персональным компьютером или другим оборудованием, подключенным через резидентный шлюз (RGW) или устройство интегрированного доступа (IAD), которое может преобразовывать сигнализацию SIP/H.323 в сообщения протоколов MGCP или Megaco/H.248. Следовательно, эти четыре протокола могут использоваться для организации лавинной атаки в сети.

Угрозы, которые не могут исключаться инфраструктурой VPN, и, следовательно, должны подавляться дополнительными средствами, включают следующие:

- похищение идентификатора пользователя (маскировка под легального пользователя). Это может привести к краже услуг (ToS);
- использование ложного IP-адреса для организации различных атак типа внедрения или лавины;
- неавторизованный доступ (атаки вторжения). Способы уменьшения этих угроз будут пояснены позже.

В дополнение к перечисленному следует отметить, что похищение пароля администратора приводит к возникновению внутренних атак. В конечном счете, если основная сетевая инфраструктура

(магистральная сеть IP) не является собственностью оператора NGN или используется совместно несколькими операторами, то защита коммуникаций между сетевыми элементами, которые проходят через эту совместно используемую область и инфраструктуру магистральной сети IP, должна быть четко продумана.

7.4 Защищенное решение для сети NGN класса 5

Кроме сценария обеспечения защиты на базе VPN, вся архитектура NGN, включающая VoIP и мультимедийные решения, должна строиться с учетом следующих положений.

1. При разработке всей сетевой архитектуры должны учитываться факторы защиты: при размещении серверов, ресурсов и сетевых элементов защиты. Это должно быть сделано таким образом, чтобы по существу выполнялся первый шаг к построению защищенного решения. Построение защищенной архитектуры базируется на двух основных принципах:

- защищенных зон (далее будет описано подробнее);
- пограничной защиты, то есть защищенных решений, основанных на применении защитных мер в пограничных элементах (защита по периметру).

2. Распределение защитных мер по сети должно производиться так, чтобы оно соответствовало тем угрозам, по отношению к которым они выставляются. Таким образом, размещение должно производиться с учетом их наибольшей эффективности.

Однако, выбор технологии защиты в основном определяется задаваемыми требованиями, хотя также должны учитываться стоимостные показатели. Стоимость защищенного решения должна быть ниже стоимости рисков, которые она устраняет. Также на выбор защищенного решения может повлиять необходимость взаимодействия со смежными доменами.

На рис. 7.3 показана сетевая архитектура мультимедийной сети NGN класса 5 вместе с элементами защиты. Защищенное решение в значительной степени зависит от сетевой архитектуры NGN и базируется на концепции защищенных зон, а также может включать может включать ряд дополнительных мер: фильтрация и ограничение скорости на уровне пограничных маршрутизаторов,

системы защиты от вторжения (IDS) на уровне доступа и т.д.

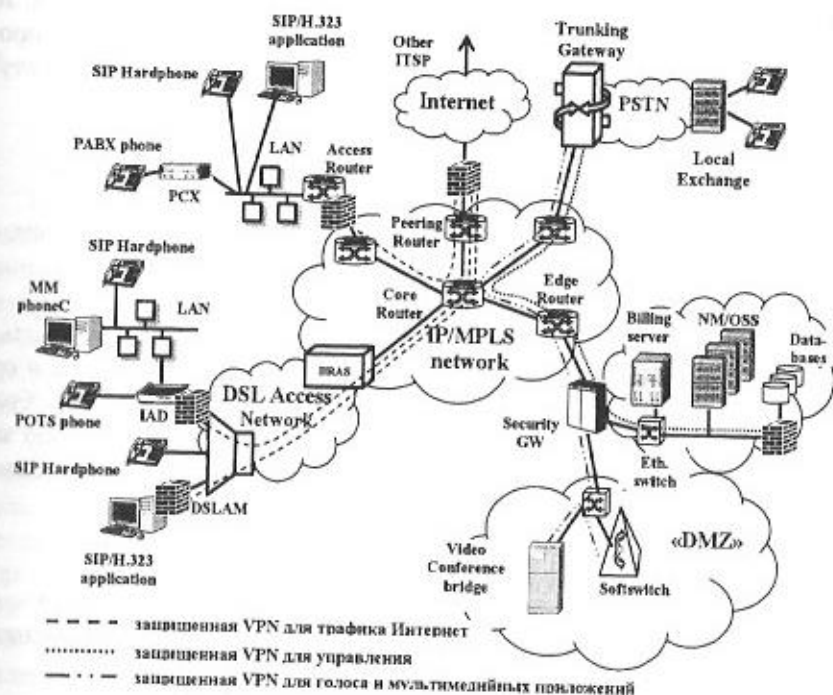


Рисунок 7.3 Структура защищенного решения для мультисервисной сети NGN класса 5

7.4.1 Защищенные зоны

Этот принцип построения архитектуры сети заключается в разделении операторской инфраструктуры на отдельные зоны следующим образом:

- защищенные зоны надежно отделены друг от друга;
- нарушителю трудно перемещаться из зоны в зону;
- в каждой зоне размещаются сетевые элементы, которые требуют одинакового уровня защиты;
- чувствительные к атакам серверы (например, хранилища данных) должны быть отделены от наиболее подверженных атакам элементов;

- защищенные решения могут применяться в разных зонах по-разному, т.е. с индивидуальной настройкой.

В соответствии с приведенными принципами, рекомендуется различать уровни сетевой архитектуры, показанной на рис. 7.3., выделять в разные зоны, то есть уровень предоставления услуг, уровень управления сеансами, уровень управления сетью и уровень среды передачи должны создаваться в виде отдельных защищенных зон. Таким образом, получаются:

- зона транспортной сети IP/MPLS;
- зона серверов приложений и услуг;
- зона управления сетью;
- зона сети доступа;
- очень чувствительная зона серверов данных;
- доступная извне зона, часто называемая демилитаризованной зоной (DMZ, в которой находятся все сервера доступные из Интернет и, поэтому уязвимые для внешних атак).

В рассматриваемой сети (рис. 7.3) транспортная сеть IP/MPLS отделена от сети доступа сервером BRAS, который кроме функций по авторизации и аутентификации, выполняет функции фильтрации и МЭ. Межсетевой экран, установленный между маршрутизатором доступа (Access Router) и опорным маршрутизатором (Core Router), защищает транспортную сеть от проникновений со стороны корпоративной IP-сети. Доступ со стороны сети Интернет защищен МЭ, установленном на пограничном маршрутизаторе (Peering Router). Демилитаризованная зона (DMZ), которая включает наиболее уязвимые сетевые устройства: программный коммутатор Softswitch, сервер управления сетью NM/OSS, сервер тарификации и базу данных, отделена от транспортной сети защитным шлюзом (Security Gateway). Этот шлюз выполняет функции пограничного контроллера сессий SBC, межсетевого экрана, транслятора сетевых адресов NAT и подсистемы предотвращения вторжений IPS.

Разделение на защищенные зоны не надо путать с мерами безопасности, применяемыми между отдельными административными доменами. Защищенные зоны объявляются в пределах одного административного домена.

Для предотвращения роста инфраструктуры межсетевых экранов (МЭ) и оптимизации их стоимостных и функциональных показателей, инфраструктура МЭ может быть частично централизованной и частично децентрализованной, в соответствии с тремя приводимыми схемами, которые могут комбинироваться:

1. размещение функций МЭ в каждом сетевом элементе (т.е. программного обеспечения МЭ);
2. размещение МЭ перед каждым сетевым элементом;
3. размещение МЭ в качестве централизованного элемента между двумя или более защищенными зонами в целях контроля сигнального и управляющего трафика, которым они обмениваются.

Конфигурация МЭ в значительной степени зависит: от конфигурации сети оператора; от размеров сети и размещения на административной границе домена или зоны, содержащей несколько сетевых элементов, требующих защиты. Например, наличие небольшого числа крупных элементов может ограничивать возможности создания большого числа зон.

7.4.2 Защита на границах зон и доменов

Концепция пограничной защиты в основном заключается в размещении защитных мер на границах операторских доменов и защитных зон. Такие защитные меры применяются раздельно к планам транспорта, управления и приложений. Защитные меры, устанавливаемые на границах домена, могут включать окончания защищенных туннелей, подавление вторжений или атак класса «Отказ в обслуживании» (DoS), а также функции аутентификации пользователей.

Защита по периметру обеспечивает следующие преимущества:

- позволяет остановить атаки до того, как они проникли в домен или зону;
- активное участие пограничных средств в аутентификации пользователя позволяет пограничному элементу (proxy server) распознать была ли процедура аутентификации удачной или нет. Это позволяет предотвратить проникновение не аутентифицированного сигнального трафика от пользователя вглубь

домена.

Защитные меры, принимаемые внутри домена или зоны, могут отличаться от мер на границе. Такой двойной подход дает ряд преимуществ:

- разделяет защитные меры используемые на концах соединения (end-to-end) и помогает приводить в замешательство атакующих. Сначала атакующий имеет дело с защитой на входящей границе домена или зоны, прежде чем он получит хотя бы первый байт информации о защитной системе следующей границы;
- облегчает процесс модификации защитных мер в пределах домена или зоны, не оказывая влияния на взаимодействие между доменами и зонами;
- позволяет адаптировать решения, применяемые для доменов с центральными серверами, к решениям для доменов доступа в зависимости от специфики применяемой технологии доступа;
- позволяет передать значительную часть загрузки процессоров защитными задачами от центральных серверов к периферийным.

7.4.3 Технологии защиты

В данном разделе приводятся специальные технологии защиты, которые используются в защищенных решениях. Ниже приведен список технологий защиты, которые могут использоваться:

- Защита потоков протокола SNMP от прослушивания, нелегального проникновения, перегрузки от DoS выполняется за счет дополнительных средств защиты, описанных в SNMP v3 (требующихся, когда SNMP используется для конфигурирования и управления сетью) и отбрасывание трафика SNMP, приходящего извне данного домена, при помощи брандмауэра и использования списков управления доступом (ACL);
- Защита потоков протокола SIP от переполнения, создаваемого оборудованием пользователя, транспортным доменом или из сети Интернет за счет применения входных фильтров, брандмауэров, пакетных фильтров, списков управления доступом, а

также обеспечивая прохождение трафика только от заранее предписанных сетевых элементов;

- Защита трафика протокола HTTP обычно выполняется за счет TLS/SSL (HTTPS). Аутентификация пользователей может выполняться через защищенный TLS/SSL туннель;
- Защита трафика протоколов COPS или H.248 от прослушивания, нелегального проникновения, перегрузки от DoS выполняется при помощи МЭ и пакетных фильтров (списков управления доступом и приемом трафика только от заранее прописанных сетевых элементов);
- Защита потоков протоколов FTP, Telnet, удаленного login, обычно выполняется путем удаления этих служб с сетевого узла и заменой их эквивалентными приложениями на базе SSH;
- Защита транспортных потоков в качестве альтернативы VPN может использовать IPsec или SRTP, последний из которых является менее развитым, но более адаптирован к многоточечной транспортной технологии.

Вопрос об использовании либо IPsec/IKE или TLS для защиты трафика протоколов SIP и H.323 может обсуждаться. Их применение может зависеть от возможности внедрения этих технологий в окончательное оборудование пользователей и сетевых элементов, используемых для передачи сигнальных потоков. IETF рекомендует использовать TLS для защиты потоков SIP с целью обеспечения корректного взаимодействия сетей. Однако, TLS требует использования протокола TCP. IPsec/IKE может работать поверх протокола TCP или UDP. Это является преимуществом для протоколов, которые частично или полностью работают поверх протокола UDP. Например, служба удаленного доступа (RAS), работающей поверх протокола UDP в стеке протоколов H.323. Хотя IPsec/IKE и TLS/SSL обеспечивают схожие функции защиты, между ними существуют значительные различия и они должны рассматриваться как альтернативные решения. В зависимости от конкретной проблемы одно из решений будет иметь преимущество перед другим.

Также целесообразно использовать защитные свойства самих применяемых протоколов (интегрированные защитные приложения), в зависимости от их доступности в установленных сетевых

элементах и взаимодействия с другими сетевыми компонентами. Примерами могут служить внутренняя аутентификация в COPS или сборная аутентификация (Digest) в протоколе SIP. Digest обеспечивает только аутентификацию, но всегда защищает от повторного воспроизведения (anti-replay) и никогда не обеспечивает проверку целостности и шифрование. Защищаются только сообщения SIP: REGISTER и INVITE.

Рассматривая спецификации RFC 3261 можно сделать вывод о необходимости более мощной защиты. В этом случае, должны предусматриваться процедуры аутентификации и проверки целостности на базе либо TLS/SSL, либо IPsec для сообщений протокола SIP (обратите внимание, что шифрование требуется не во всех случаях).

7.4.4 Обнаружение и предотвращение атак

Обнаружение вторжения заключается в обнаружении несанкционированного доступа к сетевому элементу. Например, когда оно было осуществлено или даже лучше когда предпринимаются попытки к его осуществлению. Из-за трудностей в предотвращении распространения атак системы обнаружения вторжений (IDS) в настоящее время имеют тенденцию к превращению в системы предотвращения вторжений (IPS) (по крайней мере, по названию). Система предотвращения вторжений (IPS) может быть определена как система обнаружения вторжений (IDS), совмещенная с МЭ или с пакетным фильтром, таким образом, что IPS может предпринимать действия автономно на основе правил политики безопасности. К таким действиям относятся сброс пакетов, перенаправление пакетов в карантинную сеть или генерация аварийных сообщений. Системы IDS/IPS могут размещаться, например, в доменах сети доступа или в доменах услуг ASP, в доменах управления сетью, в корпоративных доменах и т.д.

В настоящее время система IDS/IPS выполняет значительно более широкие обязанности, чем планировалось в начале. Она часто обеспечивает защиту от вторжений, от атак класса «отказ в обслуживании» (DoS/DDoS), от вирусов, «Троянов», «червей» и других вмешательств. Система IDS/IPS работает на скорости линейного оборудования и ее порты обычно открыты, по сравнению с

МЭ, порты которого обычно закрыты. Поэтому защищенная архитектура обычно включает как систему IDS/IPS, в качестве пограничной защиты, а межсетевой экран размещается сразу за ней (они могут размещаться в одном узле сети).

Для службы передачи голоса VoIP и мультимедийных приложений система IPS должна работать на сетевом и транспортном уровнях (IP/TCP/UDP), а также на 7-ом уровне (SIP, H.323, HTTP, XML, SMTP...). Скорость обработки системы должна быть высокой («на лету»), с малыми задержками. Система должна поддерживать одновременно большое число сессий, обеспечивать высокий уровень доступности и защищенности.

7.4.5 Проблемы прохождения потоков через межсетевые экраны и NAT

Хотя прохождение потоков через МЭ и NAT не является само по себе разделом защиты как таковой, однако при прохождении защищенных потоков через подобные инфраструктуры могут возникать проблемы. Следовательно, это необходимо учитывать. Прохождение пакетов VoIP через инфраструктуру МЭ и NAT является известной проблемой. В тех случаях, когда эти инфраструктуры не рассчитаны на работу с технологией VoIP, МЭ будет блокировать входящие вызовы. При этом, система трансляции адресов NAT будет причиной того, что в сеть оператора будут пересылаться сигнальные сообщения протоколов SIP и H.323, которые будут содержать не уникальные IP-адреса, по которым нельзя произвести их маршрутизацию.

Рассмотрим подробнее процедуру прохождения NAT, которая называется STURN (Simple Traversal of UDP through Network Address Translator).

Как видно из рис. 7.4 пользователь UA1 находится в местной сети и пользуется для взаимодействия в пределах этой сети не уникальным IP-адресом. В том случае, когда пользователю необходимо установить сессию с удаленным абонентом UA2, перед началом установления сессии UA1 обращается к серверу STURN(1), находящемуся вне данной подсети. Получив запрос, который содержит публичный IP-адрес, назначенный NAT для этой пользователю UA1, сервер STURN отвечает пользователю сообщением, в котором содержится назначенный публичный адрес и номер пор-

та(2). Пользователь UA1 устанавливает SIP сессию (3) через два прокси-сервера к пользователю UA2 и передает ему информацию о своем публичном IP-адресе.

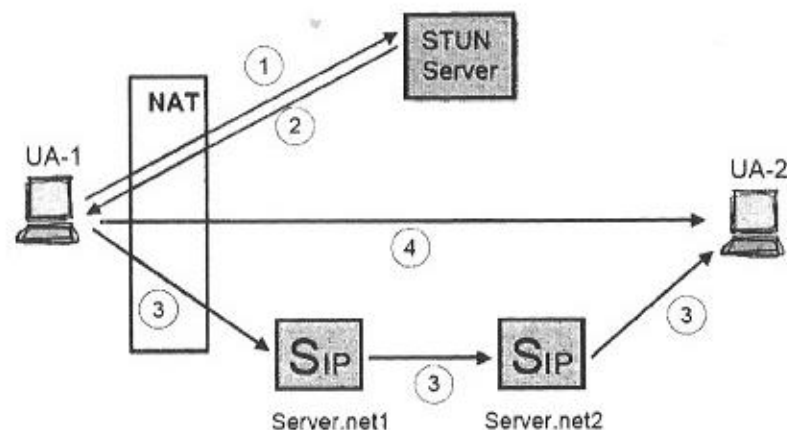


Рисунок 7.4 Процедура прохождения NAT (STURN)

Во всех случаях, когда такое возможно, рекомендуется дополнить инфраструктуру МЭ и системы трансляции адресов (NAT) до уровня шлюза прикладного уровня (ALG), который обеспечивает корректную работу с технологией VoIP. В настоящее время доступны несколько вариантов программного дооборудования МЭ и NAT, реализованных на уровне шлюза ALG. Существуют в той или иной мере стандартизованные решения, такие как: TURN (Traversal Using Relay NAT), ICE (Interactive Connectivity Establishment) корпоративное решение компании Dynamivsoft принятое IETF для группы MMUSIC и UpnP (Universal plug and play) – решение консорциума, поддерживаемое компанией Microsoft.

Например, в решениях по VoIP компания Алкатель-Лусент предусмотрела как взаимодействие с UpnP, так и сетевое преобразование МЭ и NAT. Последнее позволяет выполнять функции ALG для сигнализации SIP и H.323 на сетевом узле для тех абонентов, которым применение других способов невозможно (узел определяет несоответствие в сигнальных сообщениях и автоматически выполняет их коррекцию).

Контрольные вопросы

1. Поясните, почему организация защищенного решения для NGN сложнее, чем в сети ТфОП.
2. Чем отличается угроза от атаки?
3. Поясните, как могут использоваться протоколы сигнализации SIP H.248/MEGACO для организации атаки типа «отказ в обслуживании» (DoS)?
4. Перечислите типы VPN, которые должны быть организованы в мультисервисной сети, обеспечивающей передачу VoIP, VoD, IPTV, доступ в Интернет, доступ в корпоративный Интранет.
5. Каким образом меры по защите информации связаны с прохождением IP-пакетов через NAT?

Глава 8.

ПОДСИСТЕМА МУЛЬТИМЕДИЙНОЙ СВЯЗИ IMS

8.1 Концепция IMS (IP Multimedia Subsystem)

Опыт реализации сетей NGN на базе программных коммутаторов SX показал, что построенные сети хорошо справляются с предоставлением услуг передачи речи и организации видеоконференций, а также достаточно легко соединяются и взаимодействуют с существующими сетями с КК (ТфОП, СПС – 2G).

Дальнейшее расширение номенклатуры услуг востребованных пользователями привело к появлению пакета услуг Triple Play (тройной пакет, включающий голосовые услуги, доступ в Интернет и просмотр телевизионных программ). Для реализации такого пакета услуг необходимо было объединить усилия трех разных компаний: телефонную компанию, провайдера доступа в Интернет и компанию, предоставляющую услуги IPTV (передачи ТВ через IP-сеть). Однако, даже наличие в телефонной компании развитого IP-транспорта и программного коммутатора SX не позволяло использовать ресурсы NGN в качестве основы для предоставления услуг тройного пакета. SX не мог контролировать и тарифицировать доступ в Интернет, а также обеспечивать телевидение в режиме групповой рассылки (Multicast) и передачу видеофильмов по запросу (Unicast). Разница в организации доступа к информации, способах адресации, методах определения стоимости услуги и ее тарификации создавали непреодолимые трудности по координации действий компаний провайдеров, хотя обслуживали они одних и тех же пользователей, которые были вынуждены оплачивать разные счета, обращаться в разные службы поддержки и приобретать разное оконечное оборудование. Эта ситуация усугублялась тем, что, как правило, абоненты использовали единую сеть широкополосного доступа для получения всех трех услуг.

Одновременно с накоплением опыта построения сетей NGN на базе SX в телефонных сетях происходило преобразование мобильных сетей на технологию NGN/SX, связанное как с изменением транспортной структуры сетей 2-го поколения (2G), так и началом построения сетей 3-го поколения (3G), ориентированным на использование пакетного радиointерфейса. Идеологию создания и

развития сетей третьего поколения разрабатывал консорциум 3GPP (3-d Generation Partnership Project). Первая спецификация сетей 3-го поколения была сделана в 1999 году и получила название Release 99. В качестве нового стандарта радиointерфейса была выбрана технология – WCDMA (Wireless Code Division Multiple Access) и определен подход для создания услуг на основе архитектуры OSA (Open Service Architecture). Затем последовал Release 4, в котором был определен IP-транспорт и введены понятия MSC-сервера и транспортных шлюзов MGW. В Release 5 была впервые описана концепция IMS. В Release 6 были добавлены функции взаимодействия с сетями КК и различными сетями доступа.

Взаимодействие 3GPP и ETSI осуществляется в рамках проекта TISPAN, который появился в 2003 году и предназначен для адаптации технологии IMS к требованиям стационарных сетей связи, а также для разработки процесса конвергенции мобильных и стационарных сетей на базе IMS [3].

IMS (IP Multimedia Subsystem) – это спецификация стандартной архитектуры по управлению мультимедийными сеансами для сетей NGN. Система IMS специально разработана как распределенная структура управления сеансами на основе единого протокола сигнализации – SIP, общей базы абонентских данных – HSS (Home Subscriber Server) и ядра системы управления CSCF (Call/Session Control Function).

Система IMS обеспечивает управление сеансами связи для голосовых услуг с возможностью активации мультимедийных приложений (rich voice), видеотелефонии, передачи мультимедийных сообщений, для организации услуг IPTV, услуг определения местонахождения абонента и его мобильности. Также IMS должна обеспечивать требования по качеству обслуживания QoS для каждого из приложений, взаимодействовать с другими сетями (ТфОП, мобильными сетями второго 2G (КК) и третьего поколений 3G (КП)), поддерживать инвариантность доступа (включая технологии WiFi, WiMAX, GPRS, xDSL, HFC, PON...), а также гибкую систему тарификации мультимедийных сеансов.

8.2 Архитектура IMS

Архитектура IMS (рис. 8.1) содержит 3 уровня:

1. уровень доступа и транспорта;
2. уровень управления сессиями;
3. уровень приложений.

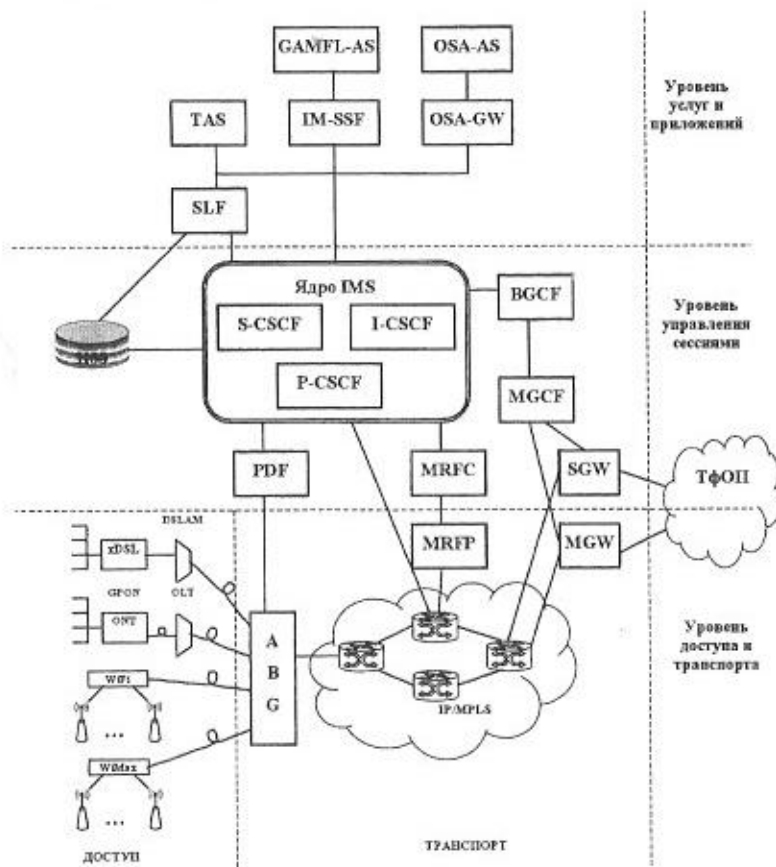


Рисунок 8.1 Архитектура IMS

Уровень доступа и транспорта включает терминальное оборудование, сети доступа с различными технологиями (WiFi, WiMAX, GPRS, xDSL, HFC, PON), единую транспортную IP-сеть и транспортные шлюзы (MGW).

Уровень управления сессиями включает ядро IMS, сервер пользовательских данных HSS (Home Subscriber Server) и сигнальные шлюзы. В IMS определяются не узлы сети, а функции, кото-

рые могут быть реализованы на одной или нескольких аппаратных платформах. Таким образом, в ядре представлена функция управления сеансами CSCF (Common Session Control Function), которая является SIP-сервером, осуществляющим функции: прокси, взаимодействия и обслуживания (Proxy, Interrogating, Service-CSCF).

Уровень приложений представлен серверами приложений AS (Application Server).

Сервер пользовательских данных HSS является централизованным хранилищем данных об абонентах и услугах, замещающей собой сервер HLR (Home Location Register) из архитектуры GSM.

Сервер HSS выполняет следующие функции:

- управляет мобильностью;
- поддерживает аутентификацию и авторизацию;
- поддерживает предоставление услуг и приложений.

В подсистеме IMS может быть один или несколько серверов HSS. Если в сети несколько серверов HSS, то необходима функция SLF (Subscriber Location Function), представляющая собой базу данных о том, какой сервер HSS хранит данные конкретного пользователя.

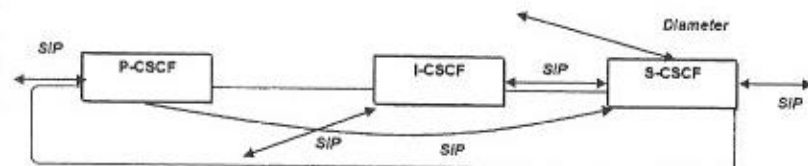


Рисунок 8.2 Функции ядра IMS

Ядро IMS включает 3 типа SIP серверов, выполняющих следующие общие функции по управлению сессиями (CSCF):

1. Proxy-CSCF – прокси-сервер;
2. Interrogating-CSCF – сервер взаимодействия;
3. Service-CSCF – сервер обслуживания.

С точки зрения SIP функция P-CSCF является входящим/исходящим прокси-сервером, через который проходят все запросы от терминала в IMS и обратно.

Терминал прикрепляется к P-CSCF во время регистрации и эта связь сохраняется до отмены регистрации. Основным назначением P-CSCF является маршрутизация запросов и ответов SIP между

терминалом и S-CSCF. P-CSCF обеспечивает аутентификацию пользователей посредством создания защищенных IPsec ассоциаций, что освобождает от повторной аутентификации остальные функции ядра IMS.

P-CSCF производит проверку правильности формирования SIP-сообщений, поступающих от терминала. Подсистема IMS обычно содержит несколько P-CSCF, каждая из которых обслуживает свою группу пользователей.

Основное назначение функции взаимодействия I-CSCF заключается в обращении к HSS по протоколу Diameter с целью получения данных о месте нахождения пользователя и обслуживающей его S-CSCF. Если ни одна сервисная CSCF еще не назначена, то I-CSCF производит ее назначение. Обычно в подсистеме IMS организуются несколько серверов I-CSCF, как правило, расположенных в домашней сети.

Обслуживающий S-CSCF, выполняет функции регистрирующего SIP-сервера, т.е. поддерживает привязку местоположения пользователя (IP-адрес) к его SIP-адресу (PUI – Public User Identity). S-CSCF взаимодействует по протоколу Diameter с сервером HSS с целью получения данных о профиле пользователя, включающих список доступных ему услуг и набор триггерных точек для маршрутизации SIP-запросов к соответствующим серверам приложений. Вся сигнальная информация, передаваемая и принимаемая терминалом, проходит через S-CSCF, которая анализирует каждое сообщение и определяет его последующее назначение. S-CSCF поддерживает сеанс и взаимодействует с функциями начисления оплаты. Для обеспечения масштабируемости в сети могут находиться несколько S-CSCF, которые всегда располагаются в домашней сети.

Функция PDF (Policy Decision Function) отвечает за выработку политики об изменении параметров сеанса. PDF получает информацию о сеансе от P-CSCF. PDF принимает решение о повторной авторизации при изменении параметров сеанса или о запрете передачи данного трафика. PDF иногда интегрируется с P-CSCF, но может быть реализована отдельно.

Функция MRF (Media Resource Function) предназначена для воспроизведения различных объявлений и состоит из:

- контроллера MRFC (Media Resource Function Controller),

- процессора MRFP (Media Resource Function Processor).

Контроллер MRFC находится на сигнальном уровне и взаимодействует с S-CSCF по протоколу SIP. Контроллер MRFC управляет процессором MRFP по протоколу MEGACO/H.248. Процессор MRFP хранит информацию, формирует и посылает объявления. Кроме воспроизведения объявлений, MRF может смешивать медиа-поток, перекодировать информацию разных кодеков, собирать статистические данные и анализировать медиа-информацию. MRF всегда находится в домашней сети.

Для взаимодействия с сетями с КК в IMS (рис. 8.2) выделены следующие элементы:

- о сервер маршрутизации вызовов по телефонному номеру BGCF (Breakout Gateway Control Function);
- о сервер управления транспортными шлюзами MGCF (Media Gateway Control Function);
- о транспортный шлюз MGW (Media Gateway);
- о сигнальный шлюз SGW (Signalling Gateway).

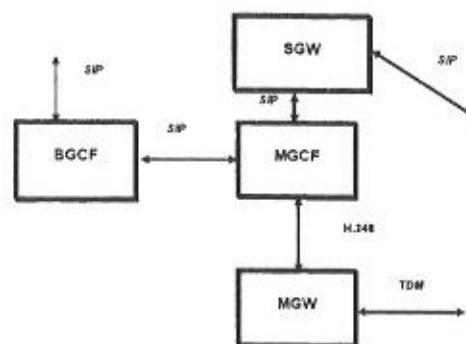


Рисунок 8.3 Функции взаимодействия IMS с сетями с КК (ТфОП, GSM)

BGCF (Breakout Gateway Control Function) – это сервер для маршрутизации вызовов на основе телефонного номера. Сервер BGCF используется только при установлении соединений к сети с КК (ТфОП, GSM). Сервер BGCF производит выбор транспортного шлюза, через который будет осуществляться взаимодействие с сетью с КК. Сервер BGCF выбирает шлюз, если взаимодействие происходит в пределах своей сети или другую IMS когда взаимодействие с нужной сетью КК выполняется в той IMS.

Шлюз сигнализации SGW находится на границе между сетью с КК и IP-сетью. В задачи шлюза сигнализации входит поддержка окончания сигнальных звеньев ОКС №7 на уровне MTP и обеспечение передачи сигнальных сообщений протоколов ISUP, INAP, MAP к серверу MGCF. Для транспортировки этих сигнальных сообщений используется протокол SCTP, который обеспечивает надежную и корректную передачу как в сторону MGCF так и в сторону сети с КК.

Функция контроллера шлюзов MGCF (Media Gateway Control Function) обычно реализуется в виде отдельного сервера. Сервер MGCF принимает сигнальные сообщения от SGW и взаимодействует с транспортными шлюзами MGW по протоколу MEGACO/H.248. MGCF взаимодействует с другими функциями IMS по протоколу SIP.

Реализация MGCF в виде отдельного сервера практически соответствует функционированию программного коммутатора Softswitch в режиме контроллера шлюзов MGC. Поэтому многие компании производители оборудования используют ранее разработанные программные коммутаторы в качестве элементов IMS.

На рисунке 8.4 представлены стеки протоколов в сетевых элементах, обеспечивающих обмен сигнальными сообщениями ОКС №7 при взаимодействии IMS с коммутационными станциями ТфОП (КК) или центрами сетей GSM (MSC – Mobile Switching Center).

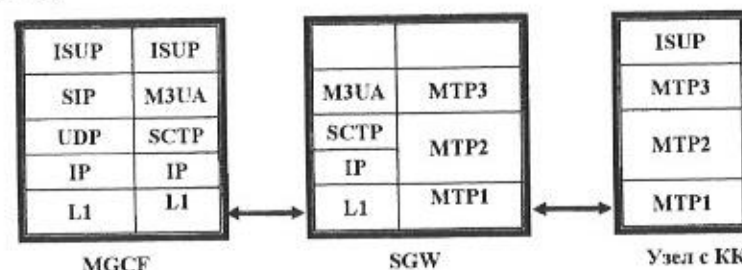


Рисунок 8.4 Стеки протоколов в элементах IMS, обеспечивающих сопряжение с сетью с КК

В коммутационной станции (CS) реализован обычный стек протоколов ОКС №7 с подсистемой пользователя ЦСИС (ISUP). В сигнальном шлюзе SGW реализована версия протокола SIGTRAN

– M3UA. Сигнальные сообщения ISUP передаются в контроллер шлюзов MGCF через процедуру адаптации M3UA по стеку SCTP/IP. Контроллер MGCF взаимодействует с остальными функциями IMS с помощью протокола SIP.

Серверы приложений AS (Application Server) предоставляют услуги посредством взаимодействия с IMS. Сервер обслуживания S-CSCF пересылает запросы к соответствующему серверу приложений AS, который обеспечивает поддержку услуги.

Подсистема IMS обеспечивает взаимодействие с большим количеством различных серверов приложений. Это могут быть как стандартные SIP-сервера, так и сервера построенные на концепции OSA (Open Service Architecture). Кроме того, обеспечивается взаимодействие с серверами CAMEL, которые традиционно входят в структуру мобильных сетей 2G.

В IMS различают следующие типы серверов приложений:

1) серверы поддержки телефонных услуг TAS (Telephone Application Server);

2) серверы взаимодействия с серверами услуг в мобильных сетях IM-SSF (IP Multimedia Service Switching Function);

3) серверы доступа к услугам с открытой сервисной архитектурой OSA-GW (Open Service Access GW).

Серверы приложений работают как промежуточные устройства между обслуживающей S-CSCF со одной стороны и собственно серверами услуг, которые реализуют услуги и построены по различным технологиям. Это могут быть классические серверы приложений, серверы OSA (Open Service Architecture) или стандартные серверы сети GSM использующие протокол CAMEL. Серверы приложений могут взаимодействовать с HSS для получения необходимых пользовательских данных.

Серверы поддержки телефонных услуг TAS эмулируют работу всех видов стандартных телефонных услуг (все виды переадресации вызовов, идентификацию номеров, завершение вызовов к занятому абоненту, конференция и др.).

Серверы взаимодействия с серверами услуг в мобильных сетях IM-SSF обеспечивают абонентам IMS возможность пользоваться стандартным набором услуг, предоставляемым абонентам сетей GSM при помощи протокола CAMEL (роуминг, хэнд-овер и др.).

Серверы доступа к услугам с открытой сервисной архитекту-

рой OSA-GW обеспечивают взаимодействие абонентов IMS с серверами открытой сервисной архитектуры OSA, которые могут принадлежать другим компаниям.

8.3 Сценарий установления сессии

Перед началом установления сессии терминалы должны пройти процедуру регистрации. Процесс регистрации представлен на рис. 8.5.

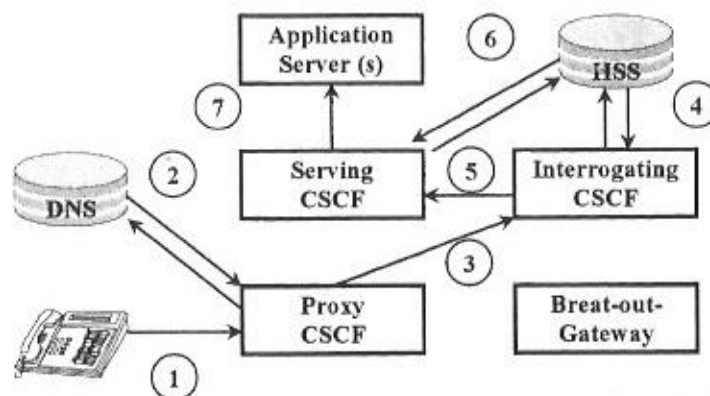
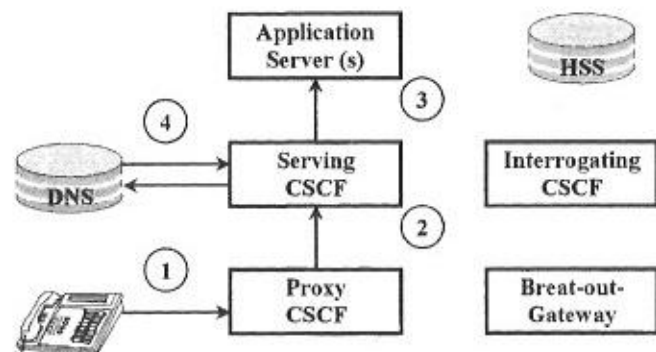


Рисунок 8.5 Процесс регистрации

1. Абонентский терминал UE посылает запрос на регистрацию в P-CSCF.
2. P-CSCF запрашивает в DNS IP-адрес взаимодействующей I-CSCF.
3. P-CSCF пересылает запрос регистрации в I-CSCF.
4. I-CSCF запрашивает в HSS адрес обслуживающей S-CSCF.
5. I-CSCF пересылает запрос регистрации к S-CSCF.
6. S-CSCF получает из HSS профиль пользователя и список прикладных серверов, доступных данному пользователю.
7. Прикладной сервер получает извещение о регистрации пользователя (опционально).

После завершения регистрации пользователь начинает установление сессии. Начало установления сессии на исходящей стороне представлено на рис. 8.6.



Рисунки 8.6 Установление сессии на исходящей стороне

1. Терминал пользователя посылает запрос на установление соединения к P-CSCF.
2. P-CSCF пересылает запрос пользователя к S-CSCF.
3. S-CSCF пересылает запрос прикладному серверу AS.
4. S-CSCF запрашивает в DNS адрес взаимодействующей I-CSCF, обслуживающей вызываемого пользователя (функциональность ENUM).

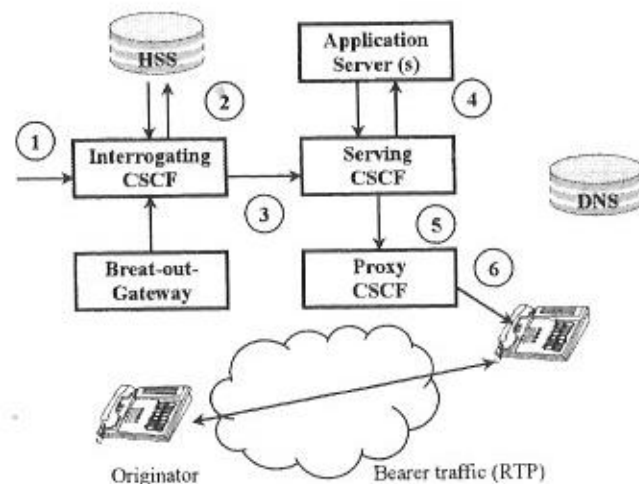
После этого, запрос пересылается к I-CSCF (если вызываемый является терминалом VoIP) или к BGCF (если вызываемый является абонентом телефонной сети).

Допустим, что вызываемый абонент подключен к другой IMS. Продолжение процесса установления сессии показано на рис. 8.7.

1. I-CSCF получает запрос на установление сессии от смежной IMS.
2. I-CSCF обращается к HSS для получения адреса обслуживающей S-CSCF и профиля вызываемого абонента.
3. I-CSCF пересылает запрос на установление сессии к S-CSCF.
4. S-CSCF обращается к прикладному серверу AS, указанному в профиле вызываемого абонента, и получает адрес P-CSCF, обслуживающей вызываемого абонента.
5. S-CSCF пересылает запрос к P-CSCF.
6. P-CSCF пересылает запрос к вызываемому терминалу.

После этого, происходит установление RTP-сессии между вы-

зываемым и вызывающим терминалами.



Рисунки 8.7 Установление сессии на входящей стороне

Если вызываемым или вызывающим пользователем является абонент телефонной сети, то сценарий установления сессии существенно изменяется. Это связано с тем, что после анализа номера вызываемого абонента в BGCF, управление сессией передается к контроллеру шлюзов MGCF, который и обеспечивает взаимодействие сетей через транспортный шлюз (рис. 8.8).

1. Терминал пользователя посылает запрос на установление соединения к P-CSCF.
2. P-CSCF пересылает запрос пользователя к S-CSCF.
3. S-CSCF пересылает запрос прикладному серверу AS.
4. S-CSCF запрашивает в DNS адрес I-CSCF. Поскольку вызываемый абонент не является абонентом IMS, то его адреса нет в DNS сервере.
5. S-CSCF пересылает запрос к BGCF.
6. BGCF пересылает запрос на установление соединения к контроллеру шлюзов MGCF.

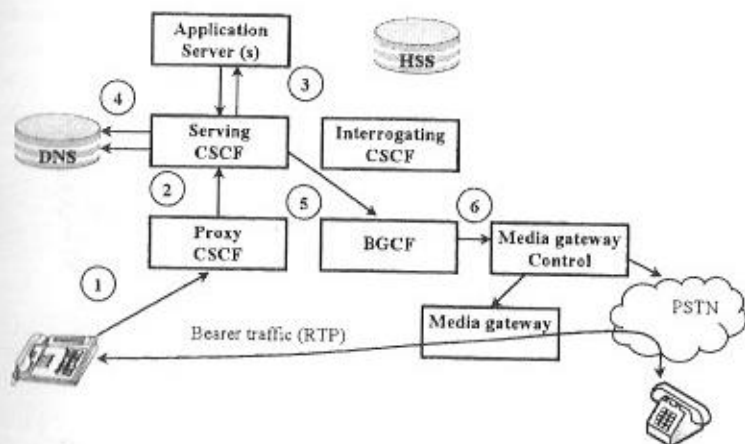


Рисунок 8.8 Установление сессии между абонентом VoIP и абонентом ТфОП

После этого, весь процесс установления соединения выполняется под управлением MGCF. MGCF посылает запрос на установления контекста в транспортном шлюзе MGW.

Затем MGCF посылает сигнальное сообщение IAM в телефонную сеть. После получения ответа вызываемого абонента MGCF устанавливает сессию между вызывающим абонентом VoIP и вызываемым телефонным абонентом.

В заключении рассмотрим более подробно полный процесс установления сессии между абонентами разных IMS (рис. 8.9).

Сценарий установления сессии между абонентами разных IMS состоит из следующих этапов:

1. Абонент А посылает запрос к серверу P-CSCF-1 своей сети.
2. P-CSCF-1 пересылает запрос к серверу S-CSCF-1 своей сети.
3. S-CSCF-1 пересылает запрос прикладному серверу AS-1.
4. AS-1 анализирует запрос и сообщает S-CSCF-1, что вызываемый абонент не принадлежит к данной сети.

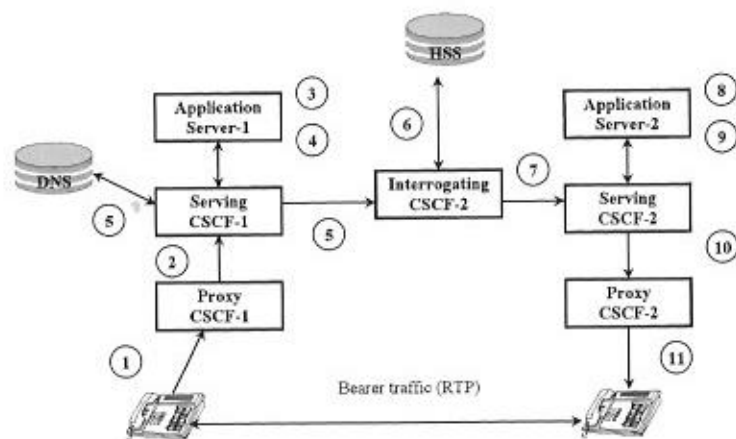


Рисунок 8.9 Установление сессии между абонентами разных IMS

5. Если S-CSCF-1 не находит дополнительного фильтрующего критерия, то S-CSCF-1 обращается к серверу DNS/ENUM для определения взаимодействующей I-CSCF-2.

Если I-CSCF-2 не является частью данной IMS, то S-CSCF-1 проверяет прописан ли адрес I-CSCF-2 в списке взаимодействующих доменов:

- если адрес I-CSCF-2 находится вне списка взаимодействующих доменов, то S-CSCF-1 пересылает сообщение INVITE к I-CSCF-2 через IBCF для выполнения NATP, скрытия внутренней топологии сети и защиты (firewall);
- если адрес I-CSCF-2 найден в списке взаимодействующих доменов, то S-CSCF-1 пересылает сообщение INVITE непосредственно в I-CSCF-2, находящийся в сети назначения.

6. I-CSCF-2 посылает запрос в HSS для поиска адреса S-CSCF-2, обслуживающей вызываемого абонента. HSS сообщает текущий адрес S-CSCF-2, обслуживающей вызываемого абонента.

7. I-CSCF-2 пересылает сообщение INVITE к S-CSCF-2.

8. S-CSCF-2 проверяет сервисный профиль вызываемого абонента (например, транспортный профиль SDP) и оценивает начальный фильтрующий критерий. В нашем примере S-CSCF-1 указывает, что необходимо обращение к прикладному серверу AS-2.

9. Остальные шаги сценария соответствуют процессу установ-

ления входящей сессии.

Рассмотренные сценарии относятся к базовым процессам установления мультимедийных сеансов (передачи голоса, видеоконференции), тогда как предоставление услуг IP TV имеет свои особенности, связанные с организацией широковещательного режима (multicasting).

8.4 Реализация IMS

В настоящее время существует большое число платформ IMS, поставляемых как известными вендорами (Alcatel-Lucent, Ericsson, Huawei...), так и небольшими компаниями. Учитывая, что концепция IMS написана на уровне взаимодействующих функций, то ее реализации отличаются большим разнообразием. В связи с этим, рассмотрим только один типичный пример реализации IMS: 5060 IP Call Server, компании Alcatel-Lucent. Это компактное решение, в котором некоторые функции реализуются на одной и той же аппаратной платформе. Функциональная схема 5060 ICS представлена на рис. 8.10.

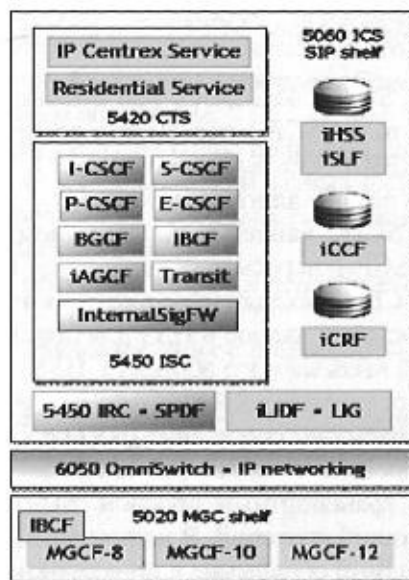


Рисунок 8.10 Функциональная схема 5060 ICS

Основные функции ядра системы выполняются на платформе 5450 ICS (IP Session Control):

1. прокси-функция Proxy-CSCF,
2. функция взаимодействия Interrogate-CSCF,
3. функция обслуживания Service-CSCF,
4. функция обработки вызовов к экстренным службам Emergency-CSCF (E-CSCF),
5. функция маршрутизации телефонных вызовов Breakout Gateway Control Function (BGCF),
6. функция пограничного контроля Interconnection Border Control Function (IBCF),
7. внутренняя функция управления шлюзами доступа Internal Access Gateway Control Function (iAGCF),
8. внутренний брандмауэр Internal Signalling Firewall (Internal-SigFW).

Первые три функции ядра IMS были подробно рассмотрены ранее.

Функция E-CSCF предназначена для обработки вызовов к экстренным службам, что требует обеспечения специальных сценариев обработки этих вызовов, ориентированных на правила принятые в данной стране.

Функции BGCF достаточно полно представлены в приведенных сценариях установления сессии. Однако, рассмотренные сценарии предполагают, что взаимодействующие IMS находятся в сети одного оператора. Если это условие не выполняется, то необходимо принимать меры по защите платформы IMS от внешних атак. Этой цели служит функция контроля пограничного взаимодействия IBCF, задача которой сокрытие внутренней структуры IMS и обеспечение корректного взаимодействия с другими IP-сетями. Для защиты системы сигнализации используется встроенный брандмауэр InternalSigFW. Функция управления шлюзами доступа также реализована iAGCF на платформе 5450 ICS.

Отдельный модуль 5450 IRC (IP Resource Control) выполняет функции PDF (Policy Decision Function), т.е. выработки конкретных политик управления сеансом, ориентированных на реализуемую службу Service-based Policy Decision Function.

Интегрированная функция распределения легального доступа к сеансам связи iLIDF и шлюз для законного прослушивания LIG

(Lawful Intercept Gateway) являются основой для COPM.

Для обеспечения взаимодействия с ТФОП используется оборудование программных коммутаторов MGC (MGC-8, MGC-10, MGC-12).

На физическом уровне взаимодействие отдельных аппаратных платформ обеспечивается Ethernet коммутатором 6850 OmniSwitch.

Поддержка единой абонентской базы данных осуществляется через внутренний iHSS, который также обеспечивает функцию SLF.

Процесс тарификации выполняется двумя функциями:

1. функцией установления тарифа iCRF (internal Charge Rate Function);
2. функцией сбора тарификационных данных iCCF (internal Charging Collection Function).

Функция iCRF собирает тарификационные запросы ACR (Accounting Request) по каждому SIP-сеансу, которые поступают от сервера приложений 5420 CTS. CRF обрабатывает поступающие запросы ACR и на их основе создает детализированные тарификационные записи CDR (Charging Detail Records) в формате ASN.1. Сформированные тарификационные записи пересылаются в iCCF. Программа iCCF обрабатывает тарификационные записи CDR и отправляет их в биллинг-сервер.

Контрольные вопросы и задания

1. Перечислите основные функции ядра IMS?
2. Укажите разницу в функциях BGCF и IBCF. Поясните в каких сценариях используются эти функции.
3. Поясните, каким образом, при входящем вызове I-CSCF получает адрес обслуживающей S-CSCF.
4. В каком случае необходима реализация функции SLF?
5. Какой модуль в IMS 5060 ICS выполняет функции определения политики управления сеансом?

ЛИТЕРАТУРА

1. Аджемов А.С., Кучерявый А.Е. Система сигнализации ОКС №7. – М.: Радио и связь, 2002.
2. Бакланов И.Г. NGN: принципы построения и организации / под ред. Ю.Н. Чернышова. – М.: Эко-Трендз, 2008. – 400 с.
3. Гольдштейн А.Б., Гольдштейн Б.С. Softswitch. СПб.: БХВ – Санкт-Петербург, – 2006. – 386 с.
4. Гольдштейн Б.С., Ехриель И.М., Рерле Р.Д. Стек протоколов ОКС7. Подсистема ISUP. Справочник. – СПб.: БХВ, 2003.
5. ГОСТ Р ИСО/МЭК 15508-1-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Ч.1: Введение и общая модель. Ч.2: Функциональные требования безопасности. Ч.3: Требования доверия к безопасности. М.: ИПК Изд. Стандартов, 2002.
6. Деарт В.Ю. Мультисервисные сети связи. Транспортные сети и сети доступа. – М.: Инсвязьиздат, 2007. – 166с.
7. Запечников С.В., Милославская Н.Г., Толстой А.И., Ушаков Д.В. «Информационная безопасность открытых систем: Учебник для вузов. Том 1 – Угрозы, уязвимости, атаки и подходы к защите. – М.: Горячая линия – Телеком, 2006. – 536с.
8. Кучерявый А.Е., Цуприков А.Л. Сети связи следующего поколения. – М.: ФГУП ЦНИИС, 2006.
9. Летников А.И., Пшеничников А.П., Гайдамака Ю.В., Чукарин А.В. Системы сигнализации в сетях с коммутацией каналов и пакетов. М.: МТУСИ, 2008.
10. Лукацкий А.В. «Практические аспекты защиты корпоративной сети IP-телефонии». Технологии и средства связи. №2, 2005. – С. 112–115.
11. Росляков А.В. Общеканальная система сигнализации №7. – М.: Эко-Трендз, 1999.
12. Росляков А.В. Сети следующего поколения NGN. – М.: Эко-Трендз, 2008. – 424 с.
13. Росляков А.В., Самсонов М.Ю., Шibaева И.В. IP-телефония. – М.: Эко-Трендз, 2001. – 250 с.
14. Randall R. Stewart, Qiaobing Xie. Stream Control Transmission Protocol (SCTP): a reference guide. – Addison Wesley. – 2002.

СПИСОК СОКРАЩЕНИЙ

A

- AAA – Authorisation, Autentication, Accounting – авторизация, аутентификация, тарификация
 ACL – Access Control List – список управления доступом
 ADPCM – адаптивная дифференциальная импульсно-кодовая модуляция
 AGCF – Access Gateway Control Function – функция управления шлюзами доступа
 ALG – Application Layer Gateway – шлюз прикладного уровня
 AMR – Adaptive Multirate – адаптивное многоскоростное кодирование
 ASP – Access Service Provider – провайдер доступа в Интернет

B

- BGCF – Breakout Gateway Control Function – функция маршрутизации телефонных вызовов

C

- CS-ACELP-Conjugate Structure – Algebraic code Excited Linear Prediction – алгоритм сопряженной структуры с управляемым алгебраическим кодом и линейным предсказанием
 CSCF – Call/Session Control Function – функция управления вызовами и сессиями
 CSRC – Contributing SouRCe – содействующий источник

D

- DMZ – DeMilitarized Zone – защищенная (демилитаризованная) зона

E

- E-CSCF – Emergency Call/Session Control Function – функция обработки вызовов к экстренным службам

F

- FW – Firewall – межсетевой экран
 FTP – File transfer Protocol – протокол передачи файлов

G

- GK – Gatekeeper – привратник (контроллер зоны)

H

- HSS – Home Subscriber Server – сервер домашних абонентов (единая абонентская база данных)

I

- IBCF – Interconnection Border Control Function – функция пограничного контроля (IMS)
 ICE – Interactive Connectivity Establishment – интерактивное установление соединений (защита на уровне ALG)
 I-CSCF – Interrogate-Call/Session Control Function – функция взаимодействия (ядро IMS)
 IDS – Intrusion Detection System – система обнаружения вторжений
 IPS – Intrusion Prevention System – система предотвращения вторжений
 IPsec – IP Security – защищенный IP-протокол

J

K

L

- LD-CELP – Low-Delay – Code Excited Linear Prediction – алгоритм малой задержки с управляемым кодом и линейным предсказанием

M

- MIPS – Millions of Interruptions per Second – миллионы операций в секунду
 MP-MLQ-Multi-Pulse – Multi Level Quantization – алгоритм множественной импульсной многоуровневой квантизации

N

- NAT – Network Address Translator- транслятор сетевых адресов

O

- OSA – Open Service Architecture – открытая сервисная архитектура

P

- PDF – Policy Decision Function) – выработка политики об изменении параметров сеанса

Q R

RAS – Remote Access Server – сервер удаленного доступа
RTP – Real-time Transport Protocol – транспортный протокол в реальном времени
RTCP – Real-Time Transfer Control Protocol – протокол контроля передачи в реальном времени

S

SBC – Session Border Controller – пограничный контроллер сессий
S-CSCF – Service – Call/Session Control Function – функция обслуживания (ядро IMS)
SCTP – Session Control Transmission Protocol – транспортный протокол с управлением потоками
SIP – Session Initiation Protocol – протокол инициации сессий
SSRC – Synchronization Source – источник синхронизации

T

Telnet – протокол управления удаленным терминалом
TLS – Transport Layer Security – защита на транспортном уровне

U

UPnP – Universal plug and play – универсальная защита от компании Microsoft
UI – User-to-User Information – информация между пользователями (элемент сообщения Q.931)

V

VAD – Voice Activity Detector – детектор голосовой активности

W

Y

Z

Приложение 1

Сокращенная трассировка процесса установления соединения, передачи речи и разъединения соединения между двумя терминалами H.323 под управлением привратника

Frame 8.

Internet Protocol, Src: 10.16.64.6, Dst: 10.16.64.1
User Datagram Protocol, Src Port: 1039, Dst Port: 1719
H.225.0 RAS
RasMessage : admissionRequest
 requestSeqNum : 13
 callType : PointToPoint
 destinationInfo : dialedDigits :5
 srcInfo : h323-ID : user 6
 dialedDigits : 6
 bandwidth : 1
 callReferenceValue : 4096
 conferenceID : 8dcace-db18-694-..
 callIdentifier : 728598e8-...

Frame 9.

Internet Protocol, Src: 10.16.64.1, Dst: 10.16.64.6
User Datagram Protocol, Src Port: 1719, Dst Port: 1039
H.225.0 RAS
RasMessage : admissionConfirm
 requestSeqNum : 13
 bandwidth : 1280
 callModel : gatekeeperRouted
 destSignalAddress : ipAddress : 10.16.64.1
 port : 1721

Frame 10.

Internet Protocol, Src: 10.16.64.6, Dst: 10.16.64.1
Transmission Control Protocol, Src Port : 1117, Dst Port : 1721 (SYN)

Frame 11.

Internet Protocol, Src: 10.16.64.1, Dst: 10.16.64.6
Transmission Control Protocol, Src Port : 1721, Dst Port : 1117 (SYN/ACK)

Frame 12.

Internet Protocol, Src: 10.16.64.6, Dst: 10.16.64.1
Transmission Control Protocol, Src Port : 1117, Dst Port : 1721 (ACK)

Frame 13.
 Internet Protocol, Src: 10.16.64.6, Dst: 10.16.64.1
 Transmission Control Protocol, Src Port: 1117, Dst Port: 1721 (Seq:1, Ack:1)
 Q.931
 Protocol discriminator: Q.931
 Call reference value length: 2
 Call reference flag: Message sent from originating side
 Call reference value: 1000
 Message type: SETUP
 Bearer capability: Coding standart: ITU-T
 Information transfer capability: Unrestricted digital information
 Transfer mode: Packet mode
 User info layer 1 protocol: H.221 and H.242
 Calling party number: '6'
 Called party number: '5'
 User-User
 Protocol discriminator: X.208 and X.209 coded user information
 H.225.0 CS
 H.323_UserInformation
 H323-message-body: setup
 H245Tunneling: true
 H245Control: request: terminalCapabilitySet
 capabilityTable: 3 items
 Item 0
 receiveAudioCapability: g711Ulaw64k
 Item 1
 receiveAudioCapability: g711Alaw64k
 Item 2
 receiveAudioCapability: gsmFullRate
 H245 request: masterSlaveDetermination
 statusDeterminationNumber: 22981

Frame 14.
 Internet Protocol, Src: 10.16.64.1, Dst: 10.16.64.6
 Transmission Control Protocol, Src Port: 1721, Dst Port: 1117 (Seq:1, Ack:256)
 Q.931
 Protocol discriminator: Q.931
 Call reference value length: 2
 Call reference flag: Message sent to originating side
 Call reference value: 1000

Message type: ALERTING
 User-User
 Protocol discriminator: X.208 and X.209 coded user information
 H.225.0 CS
 H.323_UserInformation
 H323-message-body: alerting
 H245Tunneling: true
 H245Control: request: terminalCapabilitySet
 capabilityTable: 3 items
 Item 0
 receiveAudioCapability: g711Ulaw64k
 Item 1
 receiveAudioCapability: g711Alaw64k
 Item 2
 receiveAudioCapability: gsmFullRate
 H245 request: masterSlaveDetermination
 statusDeterminationNumber: 234
 H245 response: masterslaveDeterminationAck
 Decision: slave

Frame 15.
 Internet Protocol, Src: 10.16.64.6, Dst: 10.16.64.1
 Transmission Control Protocol, Src Port : 1117, Dst Port : 1721 (Seq :256, Ack :208)
 Q.931
 Protocol discriminator : Q.931
 Call reference value length : 2
 Call reference flag: Message sent from originating side
 Call reference value: 1000
 Message type: FACILITY
 User-User
 Protocol discriminator: X.208 and X.209 coded user information
 H.225.0 CS
 H.323_UserInformation
 H323-message-body: facility
 H245Tunneling: true
 H245Control: response: terminalCapabilitySetAck
 H245 response: masterslaveDeterminationAck
 Decision: master

Frame 16.
 Internet Protocol, Src: 10.16.64.1, Dst: 10.16.64.6
 Transmission Control Protocol, Src Port: 1721, Dst Port: 1117 (Seq: 208, Ack:

344)
 Q.931
 Protocol discriminator : Q.931
 Call reference value length : 2
 Call reference flag: Message sent to originating side
 Call reference value: 1000
 Message type: FACILITY
 User-User
 Protocol discriminator: X.208 and X.209 coded user information
 H.225.0 CS
 H.323_UserInformation
 H323-message-body: facility
 conferenceID : 8dcace-db18-694-..
 callIdentifier : 728598e8-..
 H245Tunneling: true
 H245Control: request: openLogicalChannel
 forwardLogicalChannelnumber: 4
 dataType: audioData
 audioData: g711Ulaw64k
 mediaControlChannel: unicastAddress
 iPAddress: 10.16.64.5
 tsapIdentifier: 49157

Frame 17.
 Internet Protocol, Src: 10.16.64.6, Dst: 10.16.64.1
 Transmission Control Protocol, Src Port : 1117, Dst Port : 1721 (Seq :344, Ack :310)
 Q.931
 Protocol discriminator : Q.931
 Call reference value length : 2
 Call reference flag: Message sent from originating side
 Call reference value: 1000
 Message type: FACILITY
 User-User
 Protocol discriminator: X.208 and X.209 coded user information
 H.225.0 CS
 H.323_UserInformation
 H323-message-body: facility
 conferenceID : 8dcace-db18-694-..
 callIdentifier : 728598e8-..
 H245Tunneling: true
 H245Control: response: openLogicalChannelAck

forwardLogicalChannelnumber: 4
 mediaChannel: unicastAddress
 iPAddress: 10.16.64.6
 tsapIdentifier: 49158
 mediaControlChannel: unicastAddress
 iPAddress: 10.16.64.6
 tsapIdentifier: 49159
 H245: request: openLogicalChannel
 forwardLogicalChannelnumber: 4
 dataType: audioData
 audioData: g711Ulaw64k
 mediaControlChannel: unicastAddress
 iPAddress: 10.16.64.6
 tsapIdentifier: 49159

Frame 18.
 Internet Protocol, Src: 10.16.64.1, Dst: 10.16.64.6
 Transmission Control Protocol, Src Port : 1721, Dst Port : 1117 (Seq :310, Ack :470)
 Q.931
 Protocol discriminator : Q.931
 Call reference value length : 2
 Call reference flag: Message sent to originating side
 Call reference value: 1000
 Message type: FACILITY
 User-User
 Protocol discriminator: X.208 and X.209 coded user information
 H.225.0 CS
 H.323_UserInformation
 H323-message-body: facility
 conferenceID : 8dcace-db18-694-..
 callIdentifier : 728598e8-..
 H245Tunneling: true
 H245Control: response: openLogicalChannelAck
 forwardLogicalChannelnumber: 4
 mediaChannel: unicastAddress
 iPAddress: 10.16.64.5
 tsapIdentifier: 49156
 mediaControlChannel: unicastAddress
 iPAddress: 10.16.64.5
 tsapIdentifier: 49157

H323-message-body: facility
H245Tunneling: true

Frame 19.
Internet Protocol, Src: 10.16.64.1, Dst: 10.16.64.6
Transmission Control Protocol, Src Port : 1721, Dst Port : 1117 (Seq :310, Ack :470)
Q.931
Protocol discriminator : Q.931
Call reference value length : 2
Call reference flag: Message sent to originating side
Call reference value: 1000
Message type: CONNECT
User-User

Protocol discriminator: X.208 and X.209 coded user information
H.225.0 CS

H.323_UserInformation
H323-message-body: connect
conferenceID : 8dcace-db18-694-..
callIdentifier : 728598e8-..
H245Tunneling: true

Frame 20.
Internet Protocol, Src: 10.16.64.6, Dst: 10.16.64.5
User Datagram Protocol, Src Port: 49158, Dst Port: 49156
Real - Time Transport Protocol
[Stream setup by H245 (frame 18)]
Payload type: ITU-T G.711 PCMU
Sequence number: 25362
Timestamp:0
Synchronization Source Identifier: 488139190
Payload: FF7FFD,.....

Frame 21.
Internet Protocol, Src: 10.16.64.6, Dst: 10.16.64.5
User Datagram Protocol, Src Port: 49158, Dst Port: 49156
Real - Time Transport Protocol
[Stream setup by H245 (frame 18)]
Payload type: ITU-T G.711 PCMU
Sequence number: 25363
Timestamp:160
Synchronization Source Identifier: 488139190
Payload: 6E787,.....

Frame 22.
Internet Protocol, Src: 10.16.64.5, Dst: 10.16.64.6
User Datagram Protocol, Src Port: 49156, Dst Port: 49158
Real - Time Transport Protocol
[Stream setup by H245 (frame 18)]
Payload type: ITU-T G.711 PCMU
Sequence number: 22606
Timestamp:0
Synchronization Source Identifier: 488139190
Payload: 7EF7FFD,.....

Frame 445.
Internet Protocol, Src: 10.16.64.6, Dst: 10.16.64.1
Transmission Control Protocol, Src Port : 1117, Dst Port : 1721 (Seq :470, Ack :522)
Q.931
Protocol discriminator : Q.931
Call reference value length : 2
Call reference flag: Message sent from originating side
Call reference value: 1000
Message type: FACILITY
User-User

Protocol discriminator: X.208 and X.209 coded user information
H.225.0 CS

H.323_UserInformation
H323-message-body: facility
conferenceID : 8dcace-db18-694-..
callIdentifier : 728598e8-..
H245Tunneling: true
H245Control:

Item 0
request: requestChannelClose
forwardLogicalChannelnumber: 4
Item 1
request: closeLogicalChannel
forwardLogicalChannelnumber: 4
source: user

Frame 546.
Internet Protocol, Src: 10.16.64.1, Dst: 10.16.64.6
Transmission Control Protocol, Src Port : 1721, Dst Port : 1117 (Seq :522, Ack :562)
Q.931

Protocol discriminator : Q.931
Call reference value length : 2
Call reference flag: Message sent to originating side
Call reference value: 1000
Message type: FACILITY
User-User

Protocol discriminator: X.208 and X.209 coded user information
H.225.0 CS

H.323_UserInformation

H323-message-body: facility
conferenceID : 8dcace-db18-694-..
callIdentifier : 728598e8-..
H245Tunneling: true
H245Control:

Item 0

response: requestChannelCloseAck
forwardLogicalChannelnumber: 4

Item 1

request: closeLogicalChannel
forwardLogicalChannelnumber: 4
source: user

Frame 447.
Internet Protocol, Src: 10.16.64.6, Dst: 10.16.64.1
Transmission Control Protocol, Src Port : 1117, Dst Port : 1721 (Seq :562,
Ack :619)
Q.931

Protocol discriminator : Q.931
Call reference value length : 2
Call reference flag: Message sent from originating side
Call reference value: 1000
Message type: FACILITY
User-User

Protocol discriminator: X.208 and X.209 coded user information
H.225.0 CS

H.323_UserInformation

H323-message-body: facility
conferenceID : 8dcace-db18-694-..
callIdentifier : 728598e8-..
H245Tunneling: true
H245Control:

Item 0

response: closeLogicalChannelAck
forwardLogicalChannelnumber: 4
Item 1
endSessionCommand: disconnect

Frame 448.

Internet Protocol, Src: 10.16.64.1, Dst: 10.16.64.6
Transmission Control Protocol, Src Port : 1721, Dst Port : 1117 (Seq :522,
Ack :562)

Q.931

Protocol discriminator : Q.931
Call reference value length : 2
Call reference flag: Message sent to originating side
Call reference value: 1000
Message type: FACILITY
User-User

Protocol discriminator: X.208 and X.209 coded user information
H.225.0 CS

H.323_UserInformation

H323-message-body: facility
conferenceID : 8dcace-db18-694-..
callIdentifier : 728598e8-..
H245Tunneling: true
H245Control:

Item 0

endSessionCommand: disconnect

Frame 449.

Internet Protocol, Src: 10.16.64.6, Dst: 10.16.64.1
Transmission Control Protocol, Src Port : 1117, Dst Port : 1721 (Seq :562,
Ack :619)
Q.931

Protocol discriminator : Q.931
Call reference value length : 2
Call reference flag: Message sent from originating side
Call reference value: 1000
Message type: RELEASE COMPLETE
User-User

Protocol discriminator: X.208 and X.209 coded user information
H.225.0 CS

H.323_UserInformation

H323-message-body: releaseComplete
callIdentifier : 728598e8-..

Frame 450.
Internet Protocol, Src: 10.16.64.6, Dst: 10.16.64.1
User Datagram Protocol, Src Port: 1039, Dst Port: 1719
H.225.0 RAS
RasMessage : disengageRequest
 requestSeqNum : 14
 callReferenceValue : 4096
 disengageReason : normalDrop
 conferenceID : 8dcace-db18-694-..
 callIdentifier : 728598e8-...

Frame 451.
Internet Protocol, Src: 10.16.64.1, Dst: 10.16.64.6
Transmission Control Protocol, Src Port : 1721, Dst Port : 1117 (Seq :703,
Ack :703) (FIN/ACK)

Frame 452.
Internet Protocol, Src: 10.16.64.6, Dst: 10.16.64.1
Transmission Control Protocol, Src Port: 1117, Dst Port: 1721 (Seq: 703, Ack:
704) (ACK)

Frame 453.
Internet Protocol, Src: 10.16.64.6, Dst: 10.16.64.1
Transmission Control Protocol, Src Port : 1117, Dst Port : 1721 (Seq :703,
Ack :704) (FIN/ACK)

Frame 454.
Internet Protocol, Src: 10.16.64.1, Dst: 10.16.64.6
Transmission Control Protocol, Src Port : 1721, Dst Port : 1117 (Seq :704,
Ack :704) (ACK)

Frame 455.
Internet Protocol, Src: 10.16.64.1, Dst: 10.16.64.6
User Datagram Protocol, Src Port: 1719, Dst Port: 1039
H.225.0 RAS
RasMessage : disengageConfirm
 requestSeqNum : 14
[this response to request in frame 450]

Сокращенная трассировка процесса установления соединения, передачи речи и разъединения соединения между двумя терминалами SIP через Proxy сервер

Frame 10.
Internet Protocol, Src: 10.16.64.6, Dst: 10.16.64.1
User Datagram Protocol, Src Port: 5060, Dst Port: 5060
Session Initiation Protocol
Request-Line : INVITE sip :user5@10.16.64.1 SIP/2.0
Message Header
 Contact: <sip:user6@10.16.64.6:5060>
 Call-Id: 3D534AE....@10.16.64.6
 Content-Type: application/sdp
 From: "user6"<sip:user6@10.16.64.1>; tag=20707
 Cseq: 1 INVITE
 To: <sip:user5@10.16.64.1>
 Via: SIP/2.0/udp 10.16.64.1;rport;branch=z9h...
 User-Agent: Siphone/1.50.217d
 Content Length: 333

Message body
Session Description Protocol Version: 0
Owner/Creator, Session ID: - 3406345733 3406345733 IN IP4 10.16.64.6
Session Name: Siphone
Connection Information : IN IP4 10.16.64.64.6
Time Description, active time : 0 0
Session Attribute : direction: active
Media Description, name and address (m) : audio 49162 RTP/AVP 0 8 3
Media Attribute (a) : rtpmap: 0 PCMU/8000
Media Attribute (a) : rtpmap: 8 PCMA/8000
Media Attribute (a) : rtpmap: 3 GSM/8000

Frame 11.
Internet Protocol, Src: 10.16.64.1, Dst: 10.16.64.6
User Datagram Protocol, Src Port: 5060, Dst Port: 5060
Session Initiation Protocol
Status-Line : SIP/2.0 100 Trying:
Message Header
 Call-Id: 3D534AE....@10.16.64.6
 Content-Type: application/sdp

From: "user6"<sip:user6@10.16.65.1>; tag=20707
Cseq: 1 INVITE
To: <sip:user5@10.16.64.1>
Via: SIP/2.0/udp 10.16.64.6 ;rport= 5060;branch=z9h...
Server: Sjphone /1.50.271d
Content Length: 0

Frame 12.

Internet Protocol, Src: 10.16.64.1, Dst: 10.16.64.6
User Datagram Protocol, Src Port: 5060, Dst Port: 5060
Session Initiation Protocol

Status-Line : SIP/2.0 180 Ringing:

Message Header

Call-Id: 3D534AE....@10.16.64.6
Content-Type: application/sdp
From: "user6"<sip:user6@10.16.64.1>; tag=20707
Record-Route: <sip: 10.16.64.1:5060; lr>
Cseq: 1 INVITE
To: <sip:user5@10.16.64.1>
Via: SIP/2.0/udp 10.16.64.6 ;rport= 5060;branch=z9h...
Server: Sjphone /1.50.271d
Content Length: 0

Frame 13.

Internet Protocol, Src: 10.16.64.1, Dst: 10.16.64.6
User Datagram Protocol, Src Port: 5060, Dst Port: 5060
Session Initiation Protocol

Status-Line : SIP/2.0 200 OK

Message Header

Contact: <sip:user5@10.16.64.1:5060>
Call-Id: 3D534AE....@10.16.64.6
Content-Type: application/sdp
From: "user6"<sip:user6@10.16.64.1>; tag=20707
Record-Route: <sip: 10.16.64.1:5060; lr>
Cseq: 1 INVITE
To: "user5"<sip:user5@10.16.64.1>; tag=2060
Via: SIP/2.0/udp 10.16.64.6 ;rport= 5060;branch=z9h...
Server: Sjphone /1.50.271d
Content Length: 215

Message body

Session Description Protocol Version: 0
Owner/Creator, Session ID: - 3406345733 3406345733 IN IP4 10.16.64.5
Session Name: Sjphone

Connection Information : IN IP4 10.16.64.64.5
Time Description, active time : 0 0
Session Attribute : direction: active
Media Description, name and address (m) : audio 49160 RTP/AVP 0 8
Media Attribute (a) : rtpmap: 0 PCMU/8000
Media Attribute (a) : rtpmap: 8 PCMA/8000

Frame 14.

Internet Protocol, Src: 10.16.64.6, Dst: 10.16.64.1
User Datagram Protocol, Src Port: 5060, Dst Port: 5060
Session Initiation Protocol

Request-Line : ACK sip :user5@10.16.64.1 SIP/2.0

Message Header

Contact: <sip:user6@10.16.64.6:5060>
Call-Id: 3D534AE....@10.16.64.6
Max-Forwards: 70
From: "user6"<sip:user6@10.16.64.1>; tag=20707
Cseq: 1 ACK
To: <sip:user5@10.16.64.1>
Via: SIP/2.0/udp 10.16.64; rport;branch=z9h...
User-Agent: Sjphone/1.50.217d
Content Length: 0

Frame 15.

Internet Protocol, Src: 10.16.64.6, Dst: 10.16.64.5
User Datagram Protocol, Src Port: 49162, Dst Port: 49160
Real-Time Transport Protocol

(Stream setup by SDP frame 13)

Payload Type : ITU-T G.711 PCMU (0)
Sequence Number : 2630
Timestamp : 0
Synchronization Source Identifier : 0x03c19884
Payload : 6A6B6E6E.....

Frame 16.

Internet Protocol, Src: 10.16.64.6, Dst: 10.16.64.5
User Datagram Protocol, Src Port: 49162, Dst Port: 49160
Real-Time Transport Protocol

(Stream setup by SDP frame 13)

Payload Type : ITU-T G.711 PCMU (0)
Sequence Number : 2631
Timestamp : 160
Synchronization Source Identifier : 0x03c19884

Payload : 7C75746C6A6B6E6E.....

Frame 17.

Internet Protocol, Src: 10.16.64.5, Dst: 10.16.64.6
User Datagram Protocol, Src Port: 49160, Dst Port: 49162
Real-Time Transport Protocol
(Stream setup by SDP frame 13)
Payload Type : ITU-T G.711 PCMU (0)
Sequence Number : 29993
Timestamp : 0
Synchronization Source Identifier : 0x03c19884
Payload : FFFD76A6B6E6E.....

Frame 18.

Internet Protocol, Src: 10.16.64.5, Dst: 10.16.64.6
User Datagram Protocol, Src Port: 49160, Dst Port: 49162
Real-Time Transport Protocol
(Stream setup by SDP frame 13)
Payload Type: ITU-T G.711 PCMU (0)
Sequence Number: 29994
Timestamp: 160
Synchronization Source Identifier : 0x03c19884
Payload : FFFD76A6B6E6E.....

Frame 190.

Internet Protocol, Src: 10.16.64.6, Dst: 10.16.64.1
User Datagram Protocol, Src Port: 5060, Dst Port: 5060
Session Initiation Protocol
Request-Line : BYE sip:user5@10.16.64.1:5060 SIP/2.0
Message Header
Contact: <sip:user6@10.16.64.6:5060>
Call-Id: 3D534AE.....@10.16.64.6
Max-Forwards: 70
From: "user6" <sip:user6@10.16.65.1>; tag=20707
Cseq: 2 BYE
To: <sip:user5@10.16.64.1>
Via: SIP/2.0/udp 10.16.64; rport; branch=z9h...
User-Agent: Siphone/1.50.217d
Content Length: 0

Frame 191.

Internet Protocol, Src: 10.16.64.1, Dst: 10.16.64.6
User Datagram Protocol, Src Port: 5060, Dst Port: 5060

Session Initiation Protocol

Status-Line-Line : SIP/2.0 200 OK

Message Header

Contact: <sip:user5@10.16.64.1:5060>
Call-Id: 3D534AE.....@10.16.64.6
Max-Forwards: 70
From: "user6" <sip:user6@10.16.64.1>; tag=20707
Cseq: 2 BYE
To: "user5" sip:user5@10.16.64.1; tag=2060
Via: SIP/2.0/udp 10.16.64.6; rport= 5060; branch=z9h...
Server: Siphone/1.50.217d
Content Length: 0

Приложение 3

Сокращенная трассировка процесса установления соединения, передачи речи и разъединения соединения между исходящим шлюзом А 7505 MG и входящим шлюзом А7515 MG под управлением контроллера шлюзов А5020 MGC

No.	Time	Source	Destination	Protocol Info
1	0.00000	149.204.67.216	172.23.94.2	ISUP (ITU) IAM (CIC 70) Internet Protocol, Src Addr: 149.204.67.216 (149.204.67.216), Dst Addr: 172.23.94.2 (172.23.94.2) Stream Control Transmission Protocol Source port: 2904 Destination port: 2904 Verification tag: 0x1b374ee0 Checksum: 0x12a935f7 (correct CRC32C) DATA chunk(ordered, complete segment, TSN: 2463531566, SID: 1, SSN: 297, PPID: 2, payload length: 60 bytes) MTP 2 User Adaptation Layer Version: Release 1 (1) Reserved: 0x00 Message class: MTP2 user adaptation messages (6) Message type: DATA (DATA) (1) Message length: 60 Message Transfer Part Level 3 Service information octet 10.. = Network indicator: National network (0x02) ..00 = Spare: 0x00 0101 = Service indicator: ISUP (0x05) Routing label 11 0111 1001 0001 = DPC: 11300 1010 0000 0111 01.. = OPC: 10269 0110 = Signalling Link Selector: 6 ISDN User Part CIC: 70 Message type: Initial address (1) Nature of Connection Indicators: 0x0 Calling Party's category: 0xa (ordinary calling subscriber) Transmission medium requirement: 0 (speech) Called Party Number: 965711

No.	Time	Source	Destination	Protocol Info
2	0.078815	172.23.94.2	149.204.67.216	MEGACO/SDP 184 Request, with session description Internet Protocol, Src Addr: 172.23.94.2 (172.23.94.2), Dst Addr: 149.204.67.216 (149.204.67.216) User Datagram Protocol, Src Port: 2944 (2944), Dst Port: 5000 (5000) MEGACO Version: 1 MediagatewayID: [172.23.94.2] Transaction: Request Transaction ID: 184 Context: Choose one Command line: A=tdm/1/7 Command: Add Termination ID: tdm/1/7 Media Descriptor M{O{M Local Control Descriptor: MO=SR Mode: SR Command line: A=\$ Command: Add Termination ID: WildCard any Media Descriptor M{L{\n Local Descriptor: v=0\r\no=bell 53655 53655 IN IP4 128.3.4.6\r\nnc=IN IP4 \$ \r\nm=audio \$ RTP/AVP 8\r Local Control Descriptor: MO=RC Mode: RC

No.	Time	Source	Destination	Protocol Info
3	0.377003	149.204.67.216	172.23.94.2	MEGACO/SDP 184 Reply, with session description Internet Protocol, Src Addr: 149.204.67.216 (149.204.67.216), Dst Addr: 172.23.94.2 (172.23.94.2) User Datagram Protocol, Src Port: 5000 (5000), Dst Port: 2944 (2944) MEGACO Version: 1 MediagatewayID: [149.204.67.216] Transaction: Reply

Transaction ID: 184
Context: 18
Command line: A=tdm/1/7
Command: Add
Termination ID: tdm/1/7
Media Descriptor
Media Descriptor
M{O{M
Local Control Descriptor: MO=SR
Mode: SR
Command line: A=rtp/4
Command: Add
Termination ID: WildCard any
Media Descriptor
M{L{\n
Local Descriptor: v=0\r\no=bell 53655 53655 IN IP4 128.3.4.6\r\nnc=IN
IP4 100.100.105.216\r\nm=audio 30512 RTP/AVP 8\r
P=184{C=18{A=tdm/1/7,A=rtp/4{M{L{v=0..c=IN IP4 100.100.105.216
m=audio 30512 RTP/AVP 8..}}}}}

No.	Time	Source	Destination	Protocol Info
4	0.430271	172.23.94.2	149.204.67.133	MEGACO/SDP/SDP

185 Request, with session description, with session description

Internet Protocol, Src Addr: 172.23.94.2 (172.23.94.2), Dst Addr:
149.204.67.133 (149.204.67.133)

User Datagram Protocol, Src Port: 2944 (2944), Dst Port: 5000 (5000)
MEGACO

Version: 1

MediagatewayID: [172.23.94.2]

Transaction: Request

Transaction ID: 185

Context: Choose one

Command line: A=tdm/5/4

Command: Add

Termination ID: tdm/5/4

Media Descriptor

M{O{M

Local Control Descriptor: MO=SR

Mode: SR

Events Descriptor: E=11{ctyp/dtone}

RequestID: 11

pkgdName: ctyp/dtone

Command line: A=\$
Command: Add
Termination ID: WildCard any
Media Descriptor

M{L{\n

Local Descriptor: v=0\r\no=bell 53655 53655 IN IP4 128.3.4.6\r\nnc=IN
IP4 \$r\nm=audio \$ RTP/AVP 8\r

Remote Descriptor: v=0\r\no=bell 865833 865833 IN IP4
149.204.67.216\r\ns=SDP from Megacopi\r\nnc=IN IP4 100.100.105.216\r\nnt=0
0\r\nm=audio 30512 RTP/AVP 8\r},O{MO=SR}}}}}\n
- K{183}\n

No.	Time	Source	Destination	Protocol Info
5	0.5539	149.204.67.133	172.23.94.2	MEGACO/SDP

185 Reply, with session description, with session description

Internet Protocol, Src Addr: 149.204.67.133 (149.204.67.133), Dst Addr:
172.23.94.2 (172.23.94.2)

User Datagram Protocol, Src Port: 5000 (5000), Dst Port: 2944 (2944)
MEGACO

Version: 1

MediagatewayID: [149.204.67.133]

Transaction: Reply

Transaction ID: 185

Context: 46

Command line: A=tdm/5/4

Command: Add

Termination ID: tdm/5/4

Media Descriptor

M{O{M

Local Control Descriptor: MO=SR

Mode: SR

Events Descriptor: E=11{ctyp/dtone}

RequestID: 11

pkgdName: ctyp/dtone

Command line: A=rtp/1

Command: Add

Termination ID: WildCard any

Media Descriptor

M{L{\n

Local Descriptor: v=0\r\no=bell 53655 53655 IN IP4 128.3.4.6\r\nnc=IN

IP4 100.100.105.133\r\nm=audio 40014 RTP/AVP 8\r

Remote Descriptor: v=0\r\no=bell 865833 865833 IN IP4
149.204.67.216\r\ns=SDP from Megacopi\r\nnc=IN IP4 100.100.105.216\r\nnt=0
0\r\nm=audio 30512 RTP/AVP 8\r,O{MO=SR}}}}\n
K{183}\n

P=185{C=46{A=tdm/5/4,A=rtp/1/0/40014{M{L{v=0..c= IN IP4
100.100.105.133..m= audio 40014 RTP/AVP 8..a=ptime:20..},R{v=0..c=IN
IP4 100.100.105.216..m=audio 30512 RTP/AVP 8..a=ptime:20..}}}}}

No.	Time	Source	Destination	Protocol Info
6	0.640492	172.23.94.2	149.204.67.133	ISUP (ITU) IAM (CIC 36)
Internet Protocol, Src Addr: 172.23.94.2 (172.23.94.2), Dst Addr: 149.204.67.133 (149.204.67.133)				
Stream Control Transmission Protocol				
Source port: 2904				
Destination port: 2904				
Verification tag: 0x92d67dd7				
Checksum: 0x636af452 (correct CRC32C)				
DATA chunk(ordered, complete segment, TSN: 456610579, SID: 19, SSN: 261, PPID: 2, payload length: 68 bytes)				
MTP 2 User Adaptation Layer				
Version: Release 1 (1)				
Reserved: 0x00				
Message class: MTP2 user adaptation messages (6)				
Message type: DATA (DATA) (1)				
Message length: 68				
Message Transfer Part Level 3				
Service information octet				
10.. = Network indicator: National network (0x02)				
..00 = Spare: 0x00				
.... 0101 = Service indicator: ISUP (0x05)				
Routing label				
..... 10 1000 0001 1101 = DPC: 11300				
.... 1101 1110 0100 01.. = OPC: 10269				
0100 = Signalling Link Selector: 4				
ISDN User Part				
CIC: 36				
Message type: Initial address (1)				
Nature of Connection Indicators: 0x10				
Calling Party's category: 0xa (ordinary calling subscriber)				

Mandatory Parameter: 9 (Calling party's category)
Calling Party's category: ordinary calling subscriber (0x0a)
Transmission medium requirement: 0 (speech)
Mandatory Parameter: 2 (Transmission medium requirement)
Transmission medium requirement: speech (0)
Called Party Number: 965711

No.	Time	Source	Destination	Protocol Info
7	0.652016	172.23.94.2	149.204.67.216	MEGACO/SDP 186
Request, with session description				

Internet Protocol, Src Addr: 172.23.94.2 (172.23.94.2), Dst Addr:
149.204.67.216 (149.204.67.216)
User Datagram Protocol, Src Port: 2944 (2944), Dst Port: 5000 (5000)
MEGACO

Version: 1
MediagatewayID: [172.23.94.2]
Transaction: Request
Transaction ID: 186
Context: 18
Command line: MF=rtp/4
Command: Modify
Termination ID: rtp/4
Media Descriptor
M{R{\n

Remote Descriptor: v=0\r\no=bell 865833 865833 IN IP4
149.204.67.133\r\ns=SDP from Megacopi\r\nnc=IN IP4 100.100.105.133\r\nnt=0
0\r\nm=audio 40014 RTP/AVP 8\r\na=ptime:20\r,O{MO=SR}}}}\n
K{184}\n

No.	Time	Source	Destination	Protocol Info
8	0.691509	149.204.67.216	172.23.94.2	MEGACO/SDP 186
Reply, with session description				
Internet Protocol, Src Addr: 149.204.67.216 (149.204.67.216), Dst Addr: 172.23.94.2 (172.23.94.2)				
User Datagram Protocol, Src Port: 5000 (5000), Dst Port: 2944 (2944)				
MEGACO				

Version: 1
MediagatewayID: [149.204.67.216]
Transaction: Reply
Transaction ID: 186
Context: 18

Command line: MF=rtp/4
 Command: Modify
 Termination ID: rtp/4
 P=186{C=18{MF=rtp/4}}

No.	Time	Source	Destination	Protocol Info
9	1.81249	149.204.67.133	172.23.94.2	ISUP (ITU) ACM (CIC 36)
Internet Protocol, Src Addr: 149.204.67.133 (149.204.67.133), Dst Addr: 172.23.94.2 (172.23.94.2)				
Stream Control Transmission Protocol				
Source port: 2904				
Destination port: 2904				
Verification tag: 0x1b374ee0				
Checksum: 0x4851ed57 (correct CRC32C)				
DATA chunk(ordered, complete segment, TSN: 2463531569, SID: 1, SSN: 300, PPID: 2, payload length: 36 bytes)				
MTP 2 User Adaptation Layer				
Version: Release 1 (1)				
Reserved: 0x00				
Message class: MTP2 user adaptation messages (6)				
Message type: DATA (DATA) (1)				
Message length: 36				
Message Transfer Part Level 3				
Service information octet				
10... = Network indicator: National network (0x02)				
..00... = Spare: 0x00				
... 0101 = Service indicator: ISUP (0x05)				
Routing label				
... 11 0111 1001 0001 = DPC: 10269				
... 1010 0000 0111 01... = OPC: 11300				
0100... = Signalling Link Selector: 4				
ISDN User Part				
CIC: 36				
Message type: Address complete (6)				
Backward Call Indicators: 0x1614				
Mandatory Parameter: 17 (Backward call indicators)				
End of optional parameters (0)				

No.	Time	Source	Destination	Protocol Info
10	1.8898	172.23.94.2	149.204.67.133	ISUP (ITU) ACM (CIC 70)
Internet Protocol, Src Addr: 172.23.94.2 (172.23.94.2), Dst Addr: 149.204.67.133 (149.204.67.133)				

Stream Control Transmission Protocol

Source port: 2904

Destination port: 2904

Verification tag: 0x92d67dd7

Checksum: 0x25ca3f1a (correct CRC32C)

DATA chunk(ordered, complete segment, TSN: 456610582, SID: 19, SSN: 264, PPID: 2, payload length: 36 bytes)

MTP 2 User Adaptation Layer

Message Transfer Part Level 3

Service information octet

10... = Network indicator: National network (0x02)

..00... = Spare: 0x00

... 0101 = Service indicator: ISUP (0x05)

Routing label

... 10 1000 0001 1101 = DPC: 10269

... 1101 1110 0100 01... = OPC: 11300

0110... = Signalling Link Selector: 6

ISDN User Part

CIC: 70

Message type: Address complete (6)

Backward Call Indicators: 0x1634

Mandatory Parameter: 17 (Backward call indicators)

End of optional parameters (0)

No.	Time	Source	Destination	Protocol Info
11	3.2771	149.204.67.133	172.23.94.2	ISUP (ITU) ANM (CIC 36)
Internet Protocol, Src Addr: 149.204.67.133 (149.204.67.133), Dst Addr: 172.23.94.2 (172.23.94.2)				
Stream Control Transmission Protocol				
Source port: 2904				
Destination port: 2904				
Verification tag: 0x1b374ee0				
Checksum: 0x9a07ea97 (correct CRC32C)				
DATA chunk(ordered, complete segment, TSN: 2463531570, SID: 1, SSN: 301, PPID: 2, payload length: 40 bytes)				
MTP 2 User Adaptation Layer				
Version: Release 1 (1)				
Reserved: 0x00				
Message class: MTP2 user adaptation messages (6)				
Message type: DATA (DATA) (1)				
Message length: 40				
Message Transfer Part Level 3				

Service information octet

10.. = Network indicator: National network (0x02)
 ..00 = Spare: 0x00
 0101 = Service indicator: ISUP (0x05)

Routing label

.....11 0111 1001 0001 = DPC: 10269
 1010 0000 0111 01.. = OPC: 11300
 0100 = Signalling Link Selector: 4

ISDN User Part

CIC: 36

Message type: Answer (9)

Pointer to start of optional part: 1

Access transport (5 bytes length)

Optional Parameter: 3 (Access transport)

Parameter length: 5

Access transport parameter field (-> Q.931)

Low-layer compatibility

End of optional parameters (0)

No.	Time	Source	Destination	Protocol Info
-----	------	--------	-------------	---------------

12	3.348978	172.23.94.2	149.204.67.133	ISUP (ITU) ANM (CIC 70)
----	----------	-------------	----------------	-------------------------

Internet Protocol, Src Addr: 172.23.94.2 (172.23.94.2), Dst Addr:

149.204.67.133 (149.204.67.133)

Stream Control Transmission Protocol

Source port: 2904

Destination port: 2904

Verification tag: 0x92d67dd7

Checksum: 0xfe9c7741 (correct CRC32C)

DATA chunk(ordered, complete segment, TSN: 456610583, SID: 19, SSN:

265, PPID: 2, payload length: 40 bytes)

MTP 2 User Adaptation Layer

Version: Release 1 (1)

Reserved: 0x00

Message class: MTP2 user adaptation messages (6)

Message type: DATA (DATA) (1)

Message length: 40

Message Transfer Part Level 3

Service information octet

10.. = Network indicator: National network (0x02)

..00 = Spare: 0x00

.... 0101 = Service indicator: ISUP (0x05)

Routing label

.....10 1000 0001 1101 = DPC: 10269

.... 1101 1110 0100 01.. = OPC: 11300

0110 = Signalling Link Selector: 6

ISDN User Part

CIC: 70

Message type: Answer (9)

Pointer to start of optional part: 1

Access transport (5 bytes length)

Optional Parameter: 3 (Access transport)

Parameter length: 5

Access transport parameter field (-> Q.931)

Low-layer compatibility

End of optional parameters (0)

No.	Time	Source	Destination	Protocol Info
-----	------	--------	-------------	---------------

13	6.464108	149.204.67.216	172.23.94.2	ISUP (ITU) REL (CIC 70)
----	----------	----------------	-------------	-------------------------

Internet Protocol, Src Addr: 149.204.67.133 (149.204.67.133), Dst Addr:

172.23.94.2 (172.23.94.2)

Stream Control Transmission Protocol

Source port: 2904

Destination port: 2904

Verification tag: 0x1b374ee0

Checksum: 0xc157c628 (correct CRC32C)

DATA chunk(ordered, complete segment, TSN: 2463531572, SID: 1, SSN: 302, PPID: 2, payload length: 36 bytes)

MTP 2 User Adaptation Layer

Message Transfer Part Level 3

Service information octet

10.. = Network indicator: National network (0x02)

..00 = Spare: 0x00

.... 0101 = Service indicator: ISUP (0x05)

Routing label

.....11 0111 1001 0001 = DPC: 11300

.... 1010 0000 0111 01.. = OPC: 10269

0110 = Signalling Link Selector: 6

ISDN User Part

CIC: 70

Message type: Release (12)

Cause indicators, see Q.850 (2 bytes length)

Mandatory Parameter: 18 (Cause indicators)

Pointer to Parameter: 2

Parameter length: 2

Cause indicators (-> Q.850)

.... 0000 = Cause location: User (U) (0)

.00. = Coding standard: ITU-T standardized coding (0x00)

1... = Extension indicator: last octet

.001 0000 = Cause indicator: Normal call clearing (16)

1... = Extension indicator: last octet

No optional parameter present (Pointer: 0)

No.	Time	Source	Destination	Protocol Info
14	6.527459	172.23.94.2	149.204.67.216	MEGACO 187 Request
Internet Protocol, Src Addr: 172.23.94.2 (172.23.94.2), Dst Addr: 149.204.67.216 (149.204.67.216)				
User Datagram Protocol, Src Port: 2944 (2944), Dst Port: 5000 (5000)				
Source port: 2944 (2944)				

MEGACO

Version: 1

MediagatewayID: [172.23.94.2]

Transaction: Request

Transaction ID: 187

Context: 18

Command line: S=*)}\nK

Command: Subtract

Termination ID: WildCard all

T=187{C=18{S=*)}\n

K{186}\n

No.	Time	Source	Destination	Protocol Info
15	6.616041	149.204.67.216	172.23.94.2	MEGACO 187 Reply
Internet Protocol, Src Addr: 149.204.67.216 (149.204.67.216), Dst Addr: 172.23.94.2 (172.23.94.2)				
User Datagram Protocol, Src Port: 5000 (5000), Dst Port: 2944 (2944)				

MEGACO

Version: 1

MediagatewayID: [149.204.67.216]

Transaction: Reply

Transaction ID: 187

Context: 18

Command line: S=*)}\nK

P=187{C=18{S=rtp/4{SA{nt/dur=7000,nt/os=49840,nt/or=6880851,rtp/ps=0,rtp/pr=327680000,rtp/pl=0.000000,rtp/jit=1,rtp/delay=0}},S=tdm/1/7{SA{nt/dur=7000,nt/os=56000,nt/or=56000}}}}

No.	Time	Source	Destination	Protocol Info
16	6.638387	172.23.94.2	149.204.67.133	MEGACO 188 Request
Internet Protocol, Src Addr: 172.23.94.2 (172.23.94.2), Dst Addr: 149.204.67.133 (149.204.67.133)				
User Datagram Protocol, Src Port: 2944 (2944), Dst Port: 5000 (5000)				

MEGACO

Version: 1

MediagatewayID: [172.23.94.2]

Transaction: Request

Transaction ID: 188

Context: 46

Command line: S=*)}\nK

Command: Subtract

Termination ID: WildCard all

T=188{C=46{S=*)}\n

K{185}\n

No.	Time	Source	Destination	Protocol Info
17	6.684741	172.23.94.2	149.204.67.133	ISUP (ITU) RLC (CIC 70)
Internet Protocol, Src Addr: 172.23.94.2 (172.23.94.2), Dst Addr: 149.204.67.133 (149.204.67.133)				
Stream Control Transmission Protocol				
Source port: 2904				
Destination port: 2904				
Verification tag: 0x92d67dd7				
Checksum: 0xfdde37d2 (correct CRC32C)				
DATA chunk(ordered, complete segment, TSN: 456610585, SID: 19, SSN: 266, PPID: 2, payload length: 32 bytes)				

MTP 2 User Adaptation Layer

Version: Release 1 (1)

Reserved: 0x00

Message class: MTP2 user adaptation messages (6)

Message type: DATA (DATA) (1)

Message length: 32

Message Transfer Part Level 3

Service information octet

10.. = Network indicator: National network (0x02)

..00 = Spare: 0x00

.... 0101 = Service indicator: ISUP (0x05)

Routing label

.....10 1000 0001 1101 = DPC: 10269

.... 1101 1110 0100 01.. = OPC: 11300

0110 = Signalling Link Selector: 6

ISDN User Part

CIC: 70

Message type: Release complete (16)

No optional parameter present (Pointer: 0)

No.	Time	Source	Destination	Protocol Info
18	6.773270	149.204.67.133	172.23.94.2	MEGACO/SDP 188 Re- ply Source Internet Protocol, Src Addr: 149.204.67.133 (149.204.67.133), Dst Addr: 172.23.94.2 (172.23.94.2)

MEGACO

Version: 1

MediagatewayID: [172.23.94.2]

Transaction: Reply

Transaction ID: 188

Context: 46

Command line: S=*}}\nK

Command: Subtract

Termination ID: WildCard all

P=188{C=46{S=tdm/5/4{SA{nt/dur=6150,nt/os=48960,nt/or=47040}},S=rtp/
1/0/40014{SA{nt/dur=6200,nt/os=49280,nt/or=47040,rtp/ps=308,rtp/pr=294,r
p/pl=0,rtp/jit=4,rtp/delay=25}}}}

No.	Time	Source	Destination	Protocol Info
19	6.859576	172.23.94.2	149.204.67.133	ISUP (ITU) REL (CIC 36) Internet Protocol, Src Addr: 172.23.94.2 (172.23.94.2), Dst Addr: 149.204.67.133 (149.204.67.133)

Stream Control Transmission Protocol

Source port: 2904

Destination port: 2904

Verification tag: 0x92d67dd7

Checksum: 0xcb3083f5 (correct CRC32C)

DATA chunk(ordered, complete segment, TSN: 456610586, SID: 19, SSN:
267, PPID: 2, payload length: 36 bytes)

MTP 2 User Adaptation Layer

Version: Release 1 (1)

Reserved: 0x00

Message class: MTP2 user adaptation messages (6)

Message type: DATA (DATA) (1)

Message length: 36

Message Transfer Part Level 3

Service information octet

10..... = Network indicator: National network (0x02)

..00 = Spare: 0x00

.... 0101 = Service indicator: ISUP (0x05)

Routing label

.... 10 1000 0001 1101 = DPC: 10269

.... 1101 1110 0100 01.. = OPC: 11300

0100 = Signalling Link Selector: 4

ISDN User Part

CIC: 36

Message type: Release (12)

Cause indicators, see Q.850 (2 bytes length)

Mandatory Parameter: 18 (Cause indicators)

Pointer to Parameter: 2

Parameter length: 2

Cause indicators (-> Q.850)

.... 0000 = Cause location: User (U) (0)

..00. = Coding standard: ITU-T standardized coding (0x00)

1... = Extension indicator: last octet

..001 0000 = Cause indicator: Normal call clearing (16)

1... = Extension indicator: last octet

No optional parameter present (Pointer: 0)

No.	Time	Source	Destination	Protocol Info
20	6.961706	149.204.67.133	172.23.94.2	ISUP (ITU) RLC (CIC 36) Internet Protocol, Src Addr: 149.204.67.133 (149.204.67.133), Dst Addr: 172.23.94.2 (172.23.94.2)

Stream Control Transmission Protocol

Source port: 2904

Destination port: 2904

Verification tag: 0x1b374ee0

Checksum: 0xa1619fb0 (correct CRC32C)

DATA chunk(ordered, complete segment, TSN: 2463531573, SID: 1, SSN:
303, PPID: 2, payload length: 32 bytes)

MTP 2 User Adaptation Layer

Version: Release 1 (1)

Reserved: 0x00

Message class: MTP2 user adaptation messages (6)

Message type: DATA (DATA) (1)

Message length: 32

Message Transfer Part Level 3

Service information octet

10... = Network indicator: National network (0x02)

..00 ... = Spare: 0x00

... 0101 = Service indicator: ISUP (0x05)

Routing label

.... 11 0111 1001 0001 = DPC: 10269

.... 1010 0000 0111 01... = OPC: 11300

0100 ... = Signalling Link Selector: 4

ISDN User Part

CIC: 36

Message type: Release complete (16)

No optional parameter present (Pointer: 0)

В.Ю. Деарт
Мультисервисные сети связи
Протоколы и системы управления сеансами
(Softswitch/TMS)

Учебное пособие

ISBN 978-5-905376-01-6

Подписано в печать 29.03.2011.
Формат 60×84 1/16. Объем 12,5 п.л.
Тираж 600 экз. Заказ № 126.

Оперативная полиграфия «Брис – М»
111024, г. Москва, ул.Авиамоторная, д.8



Владимир Юрьевич Деарт родился в 1951 году в Москве. В 1973 году с отличием закончил факультет МЭС Московского электротехнического института связи. По окончании аспирантуры работал на кафедре ПДИ и Т. В 1984 году защитил кандидатскую диссертацию по специальности «Сети и системы связи».

Доцент, автор 63 печатных работ, которые включают два популярных учебника.

С 1993 года работает в Учебном центре Алкатель-Лусент, отвечает за постановку курсов по новым телекоммуникационным технологиям.

Успешно совмещает работу в центре с преподавательской деятельностью в МТУСИ.