

**А.Б. ГОЛЬДШТЕЙН
Б.С. ГОЛЬДШТЕЙН**



SOFTSWITCH

А. Б. Гольдштейн, Б. С. Гольдштейн

SOFTSWITCH



«БХВ — Санкт-Петербург»
2006

УДК 621.395.34

C59

ББК 32.881

Гольдштейн А. Б., Гольдштейн Б. С.

SOFTSWITCH

СПб.: БХВ — Санкт-Петербург, 2006. — 368 с.: ил.

ISBN 5-8206-0117-3

Один из основных элементов сети связи следующего поколения NGN – гибкий коммутатор Softswitch – уже составил хорошую альтернативу системам управления обслуживанием вызовов в традиционных АТС как по цене и функциональным возможностям, так и по масштабируемости, качеству обслуживания, габаритам, энергопотреблению и стоимости технической эксплуатации. Но основная причина успеха Softswitch на рынке – его умение согласовывать разные протоколы сигнализации как сетей одного типа, например, при сопряжении сетей H.323 и SIP, так и при взаимодействии сетей коммутации каналов (протоколы OKC7) с IP-сетями (протоколы SIP, MGCP, Megaco/H.248, BICC, H.323), которое рассматривается в книге в контексте технологии Sigtran, поддерживающей подсистемы OKC7 средствами IP-протоколов. Обсуждаются неоднозначность определения Softswitch, особенности его архитектуры и принципы работы. В последних главах книги делается попытка заглянуть немного вперед и рассмотреть сотрудничающие с Softswitch в сетях NGN и, возможно, конкурирующие с ним там архитектуры IMS (IP Multimedia SubSystem) и пограничные контроллеры SBC (Session Border Controller), а также представить себе, какими будут сети следующего поколения.

Предназначена для инженеров Операторских компаний, научно-исследовательских, проектных и производственных организаций, занимающихся NGN, студентов и аспирантов, обучающихся специальностям 210400 – Телекоммуникации, а также для всех, кто интересуется современными инфокоммуникациями

Научно-техническое издание

ISBN 5-8206-0117-3

© Гольдштейн А. Б., Гольдштейн Б. С., 2006

Alexander Goldstein, Boris Goldstein.

SOFTSWITCH — BHV-St. Petersburg, 2006. — 368 p.

One of the basic NGN elements, Softswitch, has already formed a good alternative to the call control systems used in traditional switches, concerning not only its price and functionality, but also its scalability, QoS, dimensions, power consumption and operating expenses. But the main source of the Softswitch' market success is its capability to couple different signaling protocols, both of the same type networks (for example, when the H.323 and SIP networks interwork) and of the different type ones – the channel switching (SS7 protocols) and IP networks (SIP, MGCP, Megaco/H.248, BICC, H.323 protocols), which is examined in the Sigtran technology context that supports the SS7 subsystems by means of IP protocols. An ambiguity of the Softswitch definition is discussed, as well as peculiarities of its architecture, and its working principles. In final chapters of the book, an attempt is undertaken to look a little in the future, and examine the IMS (IP Multimedia SubSystem) architecture and the Session Border Controller SBC, both of which will co-operate (and, possible, compete) with Softswitch in NGNs, and imagine what the networks they will be.

The book is intended for engineers of operation companies, of enterprises involved in research, planning and manufacturing works related to the Next Generation Networks, for college students and post-graduates studying in these areas, for all those who are interested in modern infocommunications technologies.

Technical edition

Copyright © A. Goldstein, B. Goldstein 2006

Содержание

Введение.....	9
Глава 1. Идеология Softswitch.....	13
1.1. Основные понятия и функции	13
1.2. Системы сигнализации	15
1.3. Процессы конвергенции в ЕСЭ РФ	18
1.4. Масштабируемость Softswitch	19
1.5. Обслуживание операторского класса	21
1.6. Декомпозиция АТС и Softswitch	23
Глава 2. Архитектура Softswitch.....	25
2.1. Консорциум IPCC	25
2.2. Функциональные плоскости эталонной архитектуры Softswitch	27
2.2.1. Транспортная плоскость	28
2.2.2. Плоскость управления обслуживанием вызовов и сигнализации	29
2.2.3. Плоскость услуг и приложений	29
2.2.4. Плоскость эксплуатационного управления	29
2.3. Функциональные объекты	30
2.4. Модуль контроллера медиашлюзов.....	35
Глава 3. IP-телефония	39
3.1. Этапы развития	39
3.2. Протокол RTP	41
3.3. Кодеки VoIP	44
3.4. Сценарии IP-телефонии	47
3.4.1. Сети H.323.	47
3.4.2. SIP-сеть	49
3.4.3. Управление шлюзами MGCP и MEGACO	50
3.4.4. Общекабельная сигнализация.....	53
3.5. Сравнение протоколов	56

Глава 4. Протокол инициирования сеансов	59
связи	59
4.1. Основы протокола SIP	59
4.2. Архитектура сети SIP	64
4.3. Структура сообщений.....	68
4.4. Команды (запросы)	71
4.5. Ответы	73
4.6. Сценарии сеансов связи	77
4.6.1. Алгоритм установления соединения с участием сервера перенаправления	77
4.6.2. Алгоритм установления соединения с участием прокси- сервера.....	79
4.7. Дополнительные услуги	80
4.8. SIP в NGN	82
Глава 5. Протоколы H.323	85
5.1. H.323 в процессе эволюции IP-телефонии	85
5.2. Адресация в сетях H.323.....	86
5.2.1. Сетевой адрес	86
5.2.2. Идентификатор TSAP	86
5.2.3. Alias адрес	86
5.2.4. Схема H.323 URL	87
5.3. Архитектура и основные устройства сети H.323.....	87
5.3.1. Терминал H.323	87
5.3.2. Шлюз H.323	89
5.3.3. Привратник	91
5.3.4. Устройство управления конференциями	92
5.4. Протоколы H.323	93
5.4.1. Протоколы RAS	94
5.4.2. Сигнальный канал H.225.0.....	99
5.4.3. Управляющий канал H.245	102
5.5. Алгоритмы установления, поддержания и разрушения соединения	108
5.5.1. Базовое соединение	108
5.5.2. Туннелирование управляющих сообщений.....	112
5.5.3. Процедура быстрого установления соединения.....	113

Глава 6. Управление транспортными шлюзами 115

6.1. Еще раз о декомпозиции шлюза	115
6.2. Эволюция протоколов управления шлюзами	118
6.3. Протокол MGCP	119
6.3.1. Модель соединения	119
6.3.2. Команды протокола MGCP	123
6.3.3. Ответы на команды	128
6.3.4. Описание сеансов связи SDP	130
6.4. Протокол Megaco/H.248	131
6.4.1. Особенности Megaco/H.248	131
6.4.2. Модель обслуживания вызова	132
6.4.3. Окончания	133
6.4.4. Контекст	134
6.4.5. Команды	135
6.4.6. Дескрипторы	136
6.4.7. Транзакции	143
6.4.8. Сообщения	144
6.4.9. Наборы сигналов и событий	144
6.5. Расширения Megaco/H.248	149
6.5.1. Развитие H.248	149
6.5.2. Усовершенствования Megaco/H.248	150
6.6. Сценарий установления соединения между шлюзами	150
6.7. Сравнение протоколов VoIP	162
6.7.1. Megaco/H.248 и MGCP	162
6.7.2. Megaco/H.248 и SIP	162
6.7.3. Megaco/H.248 и H.323	162

Глава 7. Группа Sigtran 163

7.1. Система общеканальной сигнализации №7 в IP-сети	163
7.2. Архитектура Sigtran	165
7.3. Транспортный протокол с управлением потоками	168
7.3.1. Основные функциональные возможности SCTP	168
7.3.2. Множественная адресация	169
7.3.3. Соединения для нескольких потоков	171
7.3.4. Фрагменты	172
7.3.5. Фрагмент полезной нагрузки DATA	177
7.3.6. Установление соединения	179

7.4. Протокол M3UA	181
7.4.1. Функции M3UA	181
7.4.2. Терминология	181
7.4.3. Код пункта сигнализации	183
7.4.4. Примитивы	183
7.4.5. Сообщения M3UA	184
7.5. Протокол M2UA	187
7.6. Протокол M2PA	189
7.7. Протокол SUA	191
7.8. Протокол IUA	196
7.9. Протокол V5UA	196

Глава 8. Протокол BICC 197

8.1. Стандартизация BICC	197
8.2. Архитектура протокола BICC	199
8.3. Capability Set 1	203
8.4. Система транспорта сигнализации	207
8.5. Capability Set 2	214
8.6. Протокол IPBCP	221
8.7. Обслуживание вызова в BICC	222
8.8. Сценарии взаимодействия Softswitch	223
8.8.1. Сценарий соединения DSS1 – BICC – SIP	226
8.8.2. Сценарий соединения SIP – BICC – DSS1	230
8.9. Quo vadis?	230

Глава 9. Сети NGN 233

9.1. Примеры сетевых конфигураций	233
9.2. Взаимодействие Softswitch и OKC7	237
9.2.1. Инкапсуляция ISUP в SIP	237
9.2.2. Взаимодействие H.323 и OKC7	240
9.3. Эталонная архитектура MSF	242
9.4. Услуги NGN	245
9.5. COPM	250

9.5.1. Понятие СОРМ	250
9.5.2. Законный перехват сообщений	251
9.5.3. Международные стандарты	252
9.5.4. Механизмы организации СОРМ в концепции ETSI	254
9.5.5. Интерфейсы законного перехвата ETSI	255
9.5.6. СОРМ в сетях NGN	258
9.5.7. Посредник СОРМ	259
9.6. Мультисервисный абонентский доступ	264
9.7. Пограничный контроллер сессий	265
9.7.1. Session Border Controller	265
9.7.2. Архитектура построения SBC	268
9.7.3. Функции безопасности	270
9.7.4. Преодоление NAT и Firewall	271
9.7.5. Поддержка QoS и SLA	272
9.7.6. Сопряжение сетей	273
9.7.7. Сервисные функции для Оператора	274
9.7.8. Сервисные функции для управления	275
9.7.9. Взаимодействие SBC и других элементов сети	276

Глава 10. Реализация SOFTSWITCH 279

10.1. Программно-аппаратные средства Softswitch	279
10.2. Импортные платформы Softswitch	283
10.3. Отечественные платформы Softswitch	308
10.4. Тестирование Softswitch	312
10.5. Варианты реализации СОРМ	314
10.6. Реализации пограничных контроллеров SBC	316

Глава 11. Подсистема мультимедийной связи IMS 317

11.1. Softswitch в сетях подвижной связи	317
11.2. Стандартизация IMS	318
11.2.1. Роль 3GPP/3GPP2	318
11.2.2. От GSM к 3G	318
11.2.3. Взаимодействие стандартизирующих организаций	320
11.3. Функциональные возможности IMS	321
11.3.1. Мультимедийные IP-сеансы	322
11.3.2. Качество обслуживания	323
11.3.3. Взаимодействие с другими сетями	323

11.3.4. Инвариантность доступа	324
11.3.5. Создание услуг и управление услугами	324
11.3.6. Роуминг	324
11.3.7. Безопасность	325
11.3.8. Начисление платы	325
11.4. Архитектура IMS	325
11.4.1. Уровни IMS	325
11.4.2. Абонентские базы HSS и SLF	326
11.4.3. Функция SIP-сервера	327
11.4.4. PDF	330
11.4.5. Серверы приложений	330
11.4.6. MRF	331
11.4.7. BGCF	332
11.4.8. Шлюз PSTN/CS	332
11.4.9. Шлюз безопасности SEG	333
11.4.10. Модули GPRS	334
11.5. Идентификация в IMS	335
11.6. IMS в стационарных сетях	337
11.7. Вместо заключения	343
Литература	344
Глоссарий	352
Предметный указатель	365

Введение

Обнаружение иррационального числа $\sqrt{2}$ при попытке вычислить длину гипотенузы равнобедренного прямоугольного треугольника с длиной катета, равной единице, стало в пифагорейской школе скандальным открытием. Столкнувшись с тем фактом, что в мире существуют величины, не выражающиеся рациональными числами, пифагорейцы были настолько обескуражены, что увидели в нем «руку злого демона». Они решили держать свое открытие в строжайшей тайне, а когда Гиппас Метапонтский раскрыл эту тайну широкой общественности, его учитель Пифагор воззвал к богам с мольбой покарать преступника, и вскоре непокорный ученик погиб в кораблекрушении.

Схожий эффект произвела идея *гибкого коммутатора Softswitch*, неожиданно возникшая на фоне постепенной эволюции традиционных коммутаторов каналов (ручных и автоматических, электромеханических, квазиэлектронных, электронных и цифровых, с сигнализацией по трехпроводным соединительным линиям, по выделенным сигнальным каналам, по ОКЧ7 и V5, с централизованным и распределенным программным управлением, с аналоговыми абонентскими линиями и линиями ISDN). Неизвестно, к кому и кого покарать взывали с мольбой операторы традиционной телефонии, вложившие гигантские средства в совсем недавно казавшиеся безальтернативными дорогостоящие и громоздкие АТС с коммутацией каналов. Да и не совсем понятно, как точно было устроено кораблекрушение 2001 года, утопившее при обвале NASDAQ многие тысячи только что созданных телекоммуникационных компаний. Началом конца телекоммуникационного бума и падения биржевого индекса NASDAQ стала ситуация, в которой новые участники рынка – альтернативные местные телефонные компании *CLEC (Competitive Local Exchange Carriers)*, не смогли успешно соперничать с традиционными местными телефонными компаниями *ILEC (Incumbent Local Exchange Carriers)*. Неудача компаний CLEC привела к потере триллионов долларов инвестиций в телекоммуникации, неблагоприятно сказалась на фондовом рынке и подавила всю экономику в странах, имеющих более развитые, чем в России, телекоммуникации. Одной из причин таких потерь и главными расходами новых

телекоммуникационных компаний были покупка и эксплуатация одной или нескольких АТС, стоящих миллионы долларов, имевших весьма большие габариты и требовавших значительных площадей для размещения и затрат на электропитание. Слишком поздно для CLEC, пострадавших в результате телекоммуникационного кризиса 2001-го года, на рынке появилась новая технология, описываемая в этой книге, – технология гибких коммутаторов Softswitch.

Эти Softswitch составили хорошую альтернативу АТС с коммутацией каналов, как по цене и функциональным возможностям, так и по масштабируемости, качеству обслуживания, протоколам сигнализации, габаритам, энергопотреблению, стоимости техобслуживания. При этом *масштабируемость*, с точки зрения перехода на новые технологии, является ключевым моментом. Чтобы конкурировать с традиционными АТС, новые коммутаторы должны не только поддерживать наращивание емкости до 100000 портов по 64 Кбит/с, что Softswitch, кстати, сегодня реализует в одной стойке вместо десятков статов АТС. Масштабируемость имеет две стороны, и принципы построения и архитектура Softswitch, которые излагаются в главах 1 и 2 книги, позволяют экономично управлять даже четырехпортовыми транспортными шлюзами, обеспечивая таким образом гибкую нижнюю границу эффективности, немыслимую в узлах коммутации каналов.

Ранние приложения передачи речи поверх IP (IP-телефонии) вызывали сомнение с точки зрения качества обслуживания (QoS). Первое, созданное в 1995 году израильской компанией VocalТес промышленное оборудование IP-телефонии передавало речевые пакеты, в основном, непосредственно по сети общего пользования Интернет, из-за чего увеличивались потери вызовов, да и качество речи было весьма невысоким. Многочисленные усовершенствования IP-сетей на протяжении последних 10 лет, связанные, в частности, с развитием технологии MPLS [3], сейчас обеспечивают качество обслуживания не хуже, чем системы коммутации каналов в ТФОП. Основы IP-телефонии и ее эволюции к IP-коммуникациям рассматриваются в главе 3 книги.

Важнейшим стимулом рыночного успеха Softswitch явилась его способность преобразовывать разные *протоколы сигнализации* как сетей одного типа, например, при сопряжении сетей H.323 и SIP, так и разнотипных сетей, например, при сопряжении сетей с коммутацией каналов (протоколы стека ОКС7) и IP-сетей (протоколы SIP, MGCP, MEGACO/H.248, H.323). Эта же способность Softswitch сохраняется при организации совместной работы транспортных шлюзов разных поставщиков.

Несмотря на существенный прогресс в стандартизации SIP и H.323, рассматриваемых в главах 4 и 5, взаимодействие разнород-

ного сетевого оборудования все еще остается трудно достижимым. То же справедливо и в отношении протоколов управления транспортными шлюзами *MGCP*, *MEGACO/H.248*, которым посвящена глава 6.

Применение Softswitch позволяет преодолеть проблемы взаимодействия между собой транспортных шлюзов с разными системами сигнализации. Основной такой системой при сегодняшней конвергенции сетей и услуг связи является система общеканальной сигнализации №7 (*OKC7*), рассматриваемая в контексте Softswitch в главе 7 книги. Взаимосвязь сетей *OKC7* и *IP*, которая нужна при прохождении вызовов как через сеть ТфОП, так и через сеть *IP*, является важной проблемой. В этом вопросе достигнут большой успех, в частности, благодаря новой технологии, предназначенной для работы с сетями *IP* и известной как технология *Sigtran*. Эта технология эмулирует *OKC7* средствами *IP*-протоколов. Другой, весьма близкий к *ISUP OKC7* и поддерживаемый Softswitch протокол сигнализации – независимый от несущего канала протокол управления обслуживанием вызовов *BICC* (*Bearer Independent Call Control*) – рассматривается в главе 8. Более того, *BICC* непосредственно основан на протоколе сигнализации *ISUP* и обеспечивает поддержку услуг узкополосной *ISDN* в широкополосной опорной сети без изменения ее интерфейсов с существующей узкополосной *ISDN* (*N-ISDN*). В заключительном параграфе главы 8 авторы позволили себе весьма пессимистические рассуждения о дальнейших перспективах *BICC*, хотя сама эта глава стала одной из самых объемистых в книге. Это противоречие объясняется практически полным отсутствием публикаций о *BICC*, что отнюдь не является справедливым по отношению к этому весьма интересному протоколу, успешно работающему, например, в известной платформе *ENGINE* компании *Ericsson*. Поэтому авторы постарались более подробно рассмотреть здесь основные идеи *BICC*, приняв во внимание, что у читателя есть возможность обратиться к многостраничным справочникам серии «Телекоммуникационные протоколы» по *SIP* [10] и по *H.248*, которые отсутствуют для *H.323* и *BICC*.

Глава 9 с несколько громким названием «Сети *NGN*» посвящена примерам построения сетей связи следующего поколения *NGN* (*Next Generation Network*) на базе Softswitch. Важной тенденцией, рассматриваемой в этой главе, является смещение акцентов межоператорского взаимодействия со схемы *IP-TDM-IP* на прямые соединения сетей *IP-IP*. Для поддержки таких соединений в состав *NGN*, наряду с Softswitch, включается новый элемент *SBC* (*Session Border Controller*), которому посвящен отдельный параграф главы 9. Сегодня разделение функций между системами Softswitch и *SBC* крайне размыто, и, как правило, Softswitch берет на себя большинство функций межсетевого взаимодействия не только

в схеме IP-TDM-IP, но и в схеме IP-IP, оставляя SBC, в основном, функцию нормализации трафика, т.е. согласования кодеков, сигналов DTMF и т.п. Сами по себе, варианты разделения функций между Softswitch, SBC, шлюзами сигнализации и медиашлюзами зависят от реализаций Softswitch, рассматриваемых в главе 10. Там же обсуждаются вопросы централизованной и распределенной архитектуры Softswitch, варианты построения сетей NGN разными отечественными и зарубежными Операторами, а также перечень сертифицированных для ЕСЭ РФ гибких коммутаторов, среди которых имеется и отечественный мультисервисный коммутатор МКД, применяемый в сетях традиционных и альтернативных Операторов в качестве Softswitch класса 5.

Заключительная глава 11, в которой по традиции авторы пытаются отвечать на вопрос «Quo Vadis?», в этой книге целиком посвящена архитектуре *IMS (IP Multimedia SubSystem)*, предусматривающей развитие рассмотренных в предыдущих главах концептуальных принципов Softswitch в сторону SIP-сетей и мобильных сетей 3G. Однако материал главы 11 существенно шире просто особенностей mobile Softswitch, скорее, речь идет о mobile NGN в том виде, как она представлена в работах 3GPP и 3GPP2.

Первыми слушателями изложенных во всех 11 главах материалов стали слушатели факультета повышения квалификации, аспиранты и студенты старших курсов кафедры систем коммутации СПбГУТ им. проф. М. А. Бонч-Бруевича (www.skri.sut.ru), чья любознательность и разнообразные вопросы помогли подготовить эту книгу. В ее написании непосредственную помощь авторам оказали преподаватели кафедры – доцент, к.т.н. Антон Зарубин и ассистент Александр Атчик. Весьма полезны были также стимулирующие дискуссии с коллегами – научными сотрудниками ЛОНИИС, НТЦ ПРОТЕЙ и ГК ЭКРАН, опыт реальных установок оборудования NGN в операторских компаниях Уралсвязь, Комстар-ОТС, СЗТ, ЮТК, Дальсвязь, сотрудничество с ведущими зарубежными компаниями Siemens, Lucent, Alcatel, Teledata, Ericsson, Avaya, Italtel, Strom, Nortel в различных проектах NGN, которые частично описаны в этой книге и про которые читатели могут прочитать в реальном времени на сайте www.niits.ru.

Глава 1

Идеология

Softswitch

Лучший способ предвидеть будущее – изобрести его
Алан Кей, фирма Apple

1.1. Основные понятия и функции

Термин Softswitch был придуман Айком Элиотом при разработке интерфейса между интерактивной речевой системой (IVR) и АТС с коммутацией каналов в операторской компании MCI. Перейдя в 1997 году из MCI в компанию Level3 Communications, он, вместе с Эндрю Дуганом и Маурицио Аронго, придумал понятия *Call Agent* и *Media Gateway*. Ими же была начата разработка контроллера транспортного шлюза MGC (*Media Gateway Controller*), функции которого, как и функции *Call Agent*, собственно говоря, и выполняет Softswitch. В апреле 1998 года Level3 купила компанию Xcom, создавшую к тому времени технологию управления модемным пулом Интернет-провайдера, на базе которой был разработан *Internet Protocol Device Control (IPDC)*. Тогда же Кристиан Хюйтема из компании Bellcore придумал протокол управления шлюзами сигнализации SGCP (*Signaling Gateway Control Protocol*). На базе этих разработок и совместными усилиями этих специалистов в IETF была создана первая спецификация протокола управления шлюзами MGCP (*Media Gateway Control Protocol*). Это одна ветвь родословной Softswitch.

Другим предшественником Softswitch является привратник GK (*Gatekeeper*). Более того, названия *контроллер MGC* и *привратник GK* являются терминами, адекватными ранним формам Softswitch. Понятие привратник зародилось в технологии H.323, рассматриваемой в главе 5. В задачи привратника входит преобразование адресов (имени или адреса электронной почты – для терминала

или шлюза – и транспортного адреса) и управление доступом (авторизация доступа в сеть). Согласно принципам рекомендации H.323 привратник должен управлять действиями в определенной зоне сети, представляющей собой совокупность одного или нескольких шлюзов и управляющего ими единственного привратника. При этом привратник рассматривается как логическая функция, а не как физический объект.

Тогда же, в 2000 – 2001 г.г. стали появляться первые технические решения Softswitch операторского класса компаний Lucent Technologies, Sonus Networks (система Insignus), Level3 (система Viper), MetaSwitch (система VP3000) и др. Более подробно эти и появившиеся позднее платформы Softswitch рассматриваются в главе 10, посвященной аспектам реализации трехгранной пирамиды. Здесь же отметим лишь характерную для революционных изменений в инфокоммуникационных технологиях последних лет ситуацию, когда разработки (и даже промышленные образцы) опережают появление не только стандартизованных спецификаций, но и устоявшейся терминологии. В полной мере это относится и к рассматриваемой в книге области.

Попробуем ликвидировать этот пробел и перейти к обсуждению Softswitch в современных условиях конвергенции сетей связи с коммутацией каналов и коммутацией пакетов и перехода к сетям связи следующего поколения NGN (*Next Generation Network*). Прежде всего, сосредоточимся на функциональных возможностях программного коммутатора Softswitch, отложив рассмотрение его архитектуры до следующей главы. Тогда можно предложить следующее общее определение:

Softswitch является носителем интеллектуальных возможностей сети, который координирует управление обслуживанием вызовов, сигнализацию и функции, обеспечивающие установление соединения через одну или несколько сетей.

Подчеркнем, что Softswitch – это не только одно из сетевых устройств. Это также и сетевая архитектура и даже, в определенной степени, – идеология построения сети. Именно поэтому основной упор в приведенном определении сделан на функциональные возможности. При этом, строго говоря, под данное здесь определение не подпадают отдельные устройства с ограниченными функциями – привратники H.323 или SIP-прокси, которые в рекламных целях их продавцы также именовали Softswitch.

В первую очередь, Softswitch управляет обслуживанием вызовов, т.е. установлением и разрушением соединений, выполняя функции *Call Agent*. Точно так, как это имеет место в традиционных АТС с коммутацией каналов [6], если соединение установлено, то эти функции гарантируют, что оно сохранится до тех пор, пока

не даст отбой вызвавший или вызванный абонент. В число функций управления обслуживанием вызова Call Agent входят распознавание и обработка цифр номера для определения пункта назначения вызова; а также распознавание момента ответа вызываемой стороны, момента, когда один из абонентов кладет трубку, и регистрация этих действий для начисления платы. Таким образом, Softswitch фактически остается все тем же привычным коммутационным узлом, только без цифрового коммутационного поля и кросса и т.п. Отметим, что *Softswitch* является более точным термином, чем *Call Agent*, т.к. последний, в большинстве случаев, предполагает некое программное обеспечение обслуживания вызовов, функционирующее на стандартном компьютере. Другой термин – *контроллер транспортного шлюза MGC* – является в большей степени синонимом Softswitch и подчеркивает тот факт, что он управляет транспортными шлюзами и шлюзами доступа по протоколу H.248 и ему подобным, рассматриваемым в главе 6.

Softswitch координирует обмен сигнальными сообщениями между сетями, т.е. поддерживает функции *Signaling Gateway (SG)*. В [4] сигнализация в сети связи уже сравнивалась с системой кровообращения в человеческом организме. Если продолжить эту аналогию, то Softswitch организует это кровообращение и, к тому же, при необходимости, – переливание крови между разными организмами. Иначе говоря, Softswitch координирует действия, обеспечивающие соединение с логическими объектами в разных сетях и преобразует информацию в сообщениях с тем, чтобы они были понятны на обеих сторонах несхожих сетей, что будет несколько подробнее рассмотрено в следующем параграфе.

1.2. Системы сигнализации

Основные типы сигнализации, которые использует Softswitch, – это сигнализация для управления соединениями, сигнализация для взаимодействия разных Softswitch между собой и сигнализация для управления транспортными шлюзами. Основными протоколами сигнализации управления соединениями сегодня являются SIP-T, OKC7 и H.323, причем, по мнению авторов, именно в такой последовательности. В качестве опций используются протокол E-DSS1 первичного доступа ISDN, протокол абонентского доступа через интерфейс V5 (или его Sigtran-версии V5U), а также все еще актуальная иногда в отечественных сетях связи сигнализация по выделенным сигнальным каналам R1.5.

Основными протоколами сигнализации управления транспортными шлюзами являются MGCP и Megaco/H.248, а основными протоколами сигнализации взаимодействия между коммутаторами Softswitch являются SIP-T и BICC.

На рис. 1.1 представлено взаимодействие Softswitch с различными существующими и перспективными элементами сети связи общего пользования (ССОП). Там же видно и разделение функций Softswitch по управлению соединениями в нижележащем уровне транспортных (медиа) шлюзов, а также взаимодействие Softswitch и серверов приложений на верхнем уровне.

Нижний уровень в этом контексте может рассматриваться как транспортная плоскость, в которой физически передается как речевой трафик, так и трафик данных. Такая уровневая структура обеспечивает гибкость выбора аппаратного обеспечения (различных транспортных шлюзов).

Верхний уровень на рис. 1.1 восходит по своей идеологии к узлу управления услугами SCP (Service Control Point) классической Интеллектуальной сети [7], но, будучи на 20 лет моложе последнего, позволяет через прикладные программные интерфейсы API типа JAIN или PARLAY создавать массу новых приложений, которые невозможны в любой архитектуре традиционной телефонии с коммутацией каналов.

В рамках такого «вертикального» подхода на рис. 1.1 показаны, в частности, возможности Softswitch, относящиеся к сбору статистической информации, биллинга, мониторинга вызовов и административных функций, а также взаимодействия с системами эксплуатационного управления OSS (Operation Support System), в связи с чем упомянуты протоколы RADIUS и SNMP.

С точки зрения сети коммутации каналов представленный на рис. 1.1 Softswitch заменяет средства управления обслуживанием вызовов АТС. Он может поддерживать протоколы OKC7, E-DSS1, R1.5, V5, выполняя функции транзитного пункта сигнализации STP или оконечного SP сети сигнализации OKC7, причем делать все это более дешевым, простым и удобным в эксплуатации образом, придуманным рабочей группой Sigtran. Усилиями этой группы, входящей в IETF, разработаны средства транспортировки сообщений OKC7 по IP-сетям. Это протокол передачи информации для управления потоками SCTP (Stream Control Transmission Protocol), поддерживающий перенос сигнальных сообщений между конечными пунктами сигнализации SP в IP-сети, три новых протокола: M2UA, M2PA и M3UA для выполнения функций MTP, а также протокол SUA уровня адаптации для пользователей SCCP, поддерживающий перенос по IP-сети средствами протокола SCTP сигнальных сообщений пользователей SCCP OKC7 (например, TCAP или INAP), чему посвящена глава 7 книги.

ностями, а находящийся в разработке BICC CS-3 даже предусматривает возможность взаимодействия с SIP-T, все же практическое внедрение BICC в оборудовании Softswitch производится обычно из соображений необходимости работы в ATM-сети. В материалах ATM-форума отмечается, что хотя в обозримом будущем протоколы H.323, SIP, H.248 и BICC будут существовать параллельно, дальнейшие усилия ITU и IETF концентрируются сегодня на развитии SIP и H.248 для сетей NGN.

1.3. Процессы конвергенции в ЕСЭ РФ

Время написания этой книги (2005 год) совпало, по мнению авторов, с пиком происходящего с самого начала XXI века процесса *конвергенции сетей и услуг связи*. Помимо всего прочего, произошла конвергенция и двух радикально различавшихся в начале аналитических прогнозов, которые делали, с одной стороны, фанаты немедленного перехода на IP поверх всего и все поверх IP с апокалипсическими предсказаниями немедленного разорения всех традиционных телефонных Операторов, и, с другой стороны, умудренные адепты традиционных сетей с коммутацией каналов, до вчерашнего дня уверенные, что без них все равно последней мили не пройдешь и что все проходит, пройдет и IP. Но не прошло, а в результате конвергенции эйфории фанатов коммутации пакетов и самонадеянности приверженцев коммутации каналов начали проступать контуры *сети связи следующего поколения NGN (Next Generation Network)*. Именно на NGN ориентирован принцип декомпозиции шлюзов, для нее созданы различные межсетевые транспортные шлюзы, устройства управления шлюзами и шлюзы сигнализации, входящие в состав Softswitch.

На рис. 1.2 приведен несколько условный, но представляющий-ся правдоподобным прогноз преобразования существующей ТФОП в сеть следующего поколения NGN. Телефонная связь уже сейчас является только одним из многих приложений, доступных для VoIP. Развертывание технологий широкополосной и беспроводной связи только ускорит эту тенденцию. Это, конечно, еще не конец ТФОП в том виде, в каком мы ее знаем, но использование IP-телефонов в сочетании с Softswitch может иметь для традиционных Операторов разрушительные последствия, поскольку при этом требуется лишь, чтобы у абонента имелся IP-телефон и чтобы в установлении соединения могли участвовать разные провайдеры услуг (IP-доступа, телефонной связи и дополнительных услуг и т.п.).

Ускорить реализацию этого сценария сможет повсеместное доведение широкополосных каналов связи до жилых домов и предприятий. Мультисервисный абонентский доступ и технологии бес-

проводной связи, такие как WiMAX, наряду с интенсивным развитием Softswitch сделают возможным быстрое развертывание сетей доступа к NGN. Более подробный разговор об NGN мы отложим до главы 9.

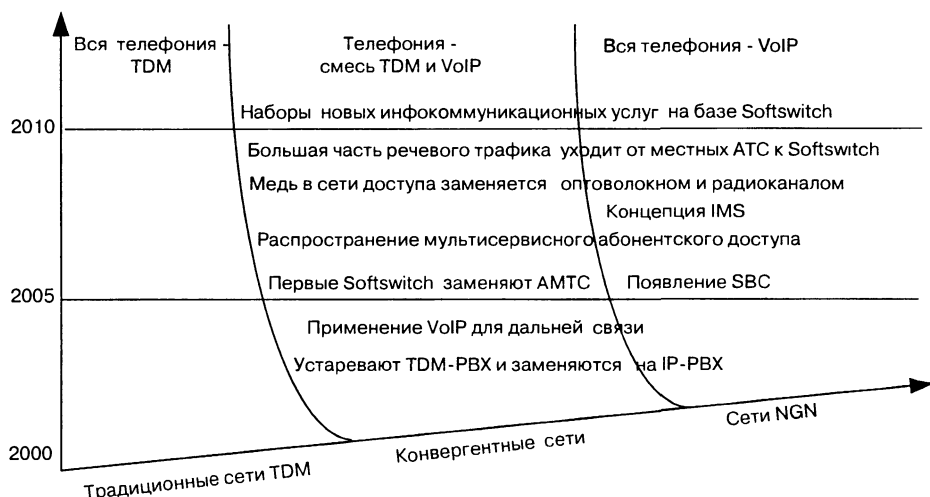


Рис. 1.2. Этапы конвергенции ЕСЭ

1.4. Масштабируемость Softswitch

Одним из упоминавшихся в предисловии многообещающих свойств архитектуры Softswitch является ее масштабируемость, которая и делает возможным целый ряд революционных приложений. Для коммутации каналов понятие «масштабируемость», как правило, связано с вопросом о том, насколько *большой* может быть рассматриваемая система коммутации. Это обусловлено с традиционным мышлением в терминах больших, централизованно расположенных и управляемых коммутационных узлов. А большой узел коммутации очевидным образом приводит к малым удельным затратам Оператора связи в расчете на один порт.

Для Softswitch же масштабируемость определяется в трех измерениях:

- насколько большим может быть общее количество портов,
- насколько малым может быть общее количество портов и
- насколько широкими могут быть при этом возможности обработки вызовов и возможности технического обслуживания.

Индустрия Softswitch, как и индустрия транспортных шлюзов, начинала с малых систем, принимая во внимание, что *точка присутствия PoP (Point of Presence)* альтернативного Оператора могла состоять и из одного четырехпортового транспортного шлюза. Только в последнее время стали внедряться шлюзы с высокой плотностью, которые соизмеримы с коммутационными узлами ТфОП, т.е. масштабируются примерно до 100 000 портов.

Согласно учебникам экономики, новая технология сменяет устаревшую потому, что для решения тех же задач она предоставляет средства, которые *дешевле, проще, меньше и удобней*, чем те, что давала предшествующая технология. Такое определение можно использовать и для оценки коммутаторов Softswitch в сравнении с коммутационными узлами ТфОП, поскольку Softswitch обладает лучшей масштабируемостью.

Появление на рынке IP-телефонов по цене значительно меньше 100 долларов за штуку и 4-портовых транспортных шлюзов, тоже по цене до 100 долларов, ведет к тому, что стоимость Softswitch на порт оказывается существенно меньше, чем у АТС. Немалое значение имеют и гораздо меньшие размеры.

К тому же, появляется все больше и больше приложений, когда пользователь приобретает транспортный шлюз в собственное пользование и избавляет поставщика услуг от расходов на это оборудование.

Если абонент покупает и обслуживает IP-телефон или транспортный шлюз, с поставщика услуг снимаются заботы об их обслуживании, а остается необходимость обслуживать только сеть Softswitch. Примерами таких пользователей становятся небольшие офисы, школы, туристические агентства, банковские отделения, автомобильные дилеры и т.п.

Таким образом, выполняется и последний пункт определения экономических предпосылок смены технологий, поскольку IP-телефоны и транспортные шлюзы удобней в использовании для провайдера услуг, если абонент покупает и обслуживает их сам, а Оператор освобождается от обременительного и дорогостоящего обслуживания АТС. Освободившись от этих расходов, Операторы, установившие Softswitch, могут существенно снизить цены по сравнению с Операторами традиционной телефонии, которые должны по-прежнему обслуживать унаследованную сеть коммутаторов каналов.

1.5. Обслуживание операторского класса

Лучший способ осознать понятие услуг связи операторского класса – это вспомнить момент, когда вы сняли телефонную трубку телефона и не услышали гудок сигнала готовности к приему номера. Вряд ли большинство читателей сможет сразу вспомнить такую ситуацию. Количественно это определялось одной из старейших норм, существовавших еще в Технических условиях (ТУ) на декадно-шаговые АТС, а оттуда перекочевавшей в другие ТУ на следующие поколения узлов коммутации: 2 часа простоя за 20 лет. В этом показателе сроки амортизации АТС сократились с первоначально назначенных 40 лет до 20, но надежность показатели коммутационной техники операторского класса во все времена являлись основой телекоммуникационных сетей общего пользования и составляли все те же «пять девяток», т.е. коэффициент готовности 0.99999, что, кстати, соответствует предельно допустимым 5 минутам простоя в год – еще одной «пятерке» к вышеупомянутым «пяти девяткам». Представляется полезным привести следующую таблицу надежностных показателей.

Таблица 1.1. Показатели надежности оборудования коммутации

Коэффициент готовности	Средний период простоя
0.9 (одна девятка)	36 дней за год
0.99 (две девятки)	89 часов за год
0.999 (три девятки)	9 часов за год
0.9999 (четыре девятки)	53 минуты за год
0.99999 (пять девяток)	5 минут за год

Практическая же трактовка последней строки таблицы сводится к весьма простому, но не всегда, к сожалению, соблюдаемым правилам, что когда вы набираете номер, то соединение устанавливается в соответствии с этим набранным номером. Что когда вы завершаете набор номера, телефон на противоположной стороне начинает звонить, а вы начинаете слушать гудки «Контроля посылки вызова» (или, в худшем случае, гудки зуммера «Занято») не позже чем через 2 – 3 секунды после завершения набора номера. Что в состоявшемся после ответа вызываемого абонента разговоре качество и разборчивость речи будут соответствовать нормам Международного союза электросвязи (ITU) без прослушивания эха, ощутимых задержек и посторонних шумов.

Разумеется, для всего вышесказанного существуют многочисленные нормы, стандарты, рекомендации, методики расчетов и измерений, а в современных условиях конвергенции услуг и сетей связи – не менее многочисленные нерешенные вопросы

определения критериев и оценок QoS, открытые для исследователей. Не вдаваясь более глубоко в чрезвычайно интересную проблематику качества обслуживания при конвергенции сетей и услуг связи, заслуживающую отдельной книги, отметим лишь, что далее и для АТС, и для Softswitch рассматриваются исключительно *услуги операторского класса*, оставляя все другие услуги уровня «...первым 100 дозвонившимся...» на совести контент-провайдеров и за пределами данной книги.

С этих позиций системы Softswitch потенциально более надежны, чем традиционные междугородные и местные АТС, которые гордятся своими «пятью девятками» надежности. Дело в том, что этот показатель традиционно относится только к самим узлам коммутации, а не к сети в целом. ТфОП как сеть никогда не достигнет уровня «пяти девяток», поскольку, к примеру, каждая ее АТС представляет собой уязвимое звено, отказ которого может привести к отказу всей сети. Это на собственном опыте поняли сотни тысяч американских абонентов во время событий 11 сентября 2001 года.

В то же время, технология передачи речевой информации с помощью IP-сетей (VoIP) подразумевает передачу речевого трафика по распределенным сетям передачи данных.

Существует много сетей передачи данных, имеющих показатель готовности на уровне «пяти девяток». И этот показатель относится к сети в целом, а не к отдельному сетевому элементу, в данном случае – к узлу коммутации.

Точно так же в плане обеспечиваемого качества обслуживания QoS возможности Softswitch соответствуют местным и междугородным АТС общего пользования (или даже превосходят их). Главное, что волнует поставщиков услуг и абонентов новых сетей, – иметь то качество телефонной связи, к которому они привыкли в ТфОП и которое выражается баллом 4.0 при оценке качества передачи речи методом *MOS (Mean Opinion Score)* по пятибалльной шкале. Некоторые построенные на базе Softswitch сети обеспечивают MOS и выше 4.0.

Для обеспечения адекватного QoS в IP-сети могут использоваться разные механизмы, в том числе система дифференцированного обслуживания трафика разных классов *DiffServ*, протокол резервирования ресурсов *RSVP (Resource Reservation Protocol)* [8] и технология многопротокольной коммутации по меткам *MPLS (Multiprotocol Label Switching)* [3].

И, наконец, дополнительные услуги, традиционно предоставляемые местными АТС с программным управлением непосредственно или с помощью узла управления услугами SCP (Service Control Point) Интеллектуальной сети. Развивая подход Интеллектуальной сети, в Softswitch используются открытые интерфейсы,

позволяющие быстро создавать и предоставлять новые услуги производителем Softswitch, или Оператором связи самостоятельно, или ими совместно, или ими вместе со сторонним провайдером услуги. Оператора также интересует проблема взаимодействия IP-сети и ТФОП, особенно, в отношении обмена сигнальной информацией между этими сетями.

Чтобы обеспечить предоставление услуг абонентам, необходимо использовать систему сигнализации ОКС7. Сообщения ОКС7 могут передаваться по IP-сетям с помощью рассматриваемого в главе 7 протокола Sigtran и других механизмов. Возможно, что на смену ОКС7 придет более простое и эффективное средство сигнализации, такое как протокол инициирования сеансов связи SIP, которому посвящены глава 4 и книга [10].

1.6. Декомпозиция АТС и Softswitch

В завершение первой главы авторам представляется полезным ненадолго отвлечься от спецификаций протоколов VoIP, от численных характеристик масштабируемости и надежности Softswitch и попробовать на идейном уровне показать эволюцию архитектуры систем с коммутацией каналов [6] к Softswitch.

Дорогостоящие традиционные АТС в единой структуре объединяют функции коммутации, функции управления обслуживанием вызовов, услуги и приложения, а также функции биллинга. Такая АТС представляет собой монолитную, закрытую системную структуру, как правило, не допускающую расширения или модернизации на базе оборудования других производителей.

Определенные попытки разрушить этот монолит предпринимались как снизу, через сеть доступа, с помощью универсального интерфейса V5 [5], так и сверху, через Интеллектуальную сеть, с помощью протокола INAP [7]. И не были безуспешными, но все же разрабатываемому таким образом оборудованию и программному обеспечению были свойственны высокая стоимость и длительное время их внедрения.

РевOLUTIONное изменение ситуации принес Softswitch. Он в корне изменил традиционную закрытую структуру систем коммутации, используя принципы компонентного построения сети и открытые стандартные интерфейсы между тремя основными функциями: коммутации, управления обслуживанием вызовов, услуг и приложений. В такой открытой, распределенной структуре могут свободно использоваться функциональные компоненты разных производителей.

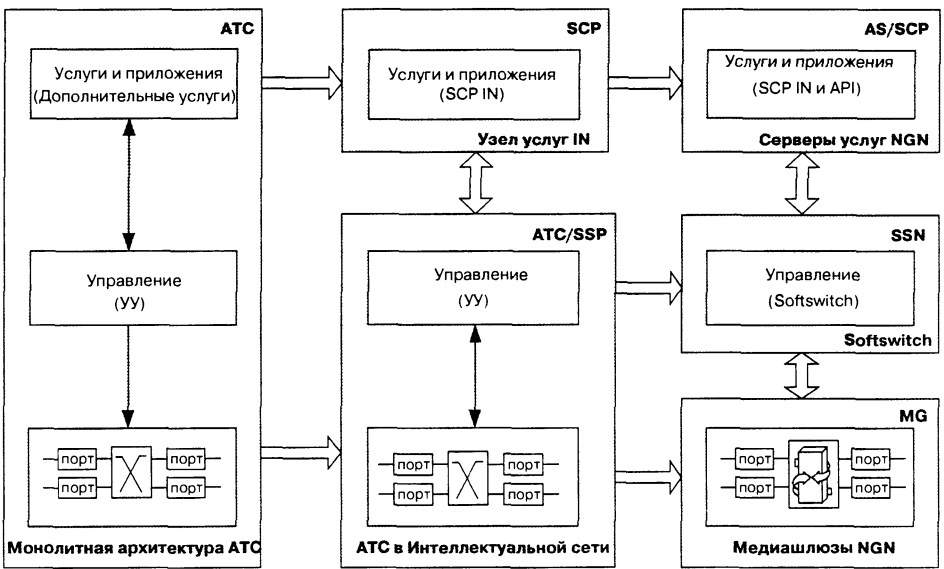


Рис. 1.3. Декомпозиция ATC и Softswitch

Узлам и станциям с коммутацией каналов для сетей TDM посвящена книга [6], а некоторые аналогии рассматриваемых в ней ATC с составляющим предмет этой книги Softswitch представлены на рис. 1.3.

Нам показалось уместным привести эти тезисы именно здесь, прежде, чем мы перейдем к более строгому обсуждению архитектуры Softswitch в следующей главе, являющейся, по сути, углубленным анализом принципа декомпозиции шлюзов, основную идею которого как раз и иллюстрирует рис. 1.3.

Глава 2

Архитектура Softswitch

*Совершенство дилижанс можно создать первоклассный дилижанс,
но первоклассный автомобиль — едва ли.*
Эдуард де Бано, Кембридж

2.1. Консорциум IPCC

Именно по приведенной в эпиграфе причине архитектура Softswitch с самого начала создавалась в структурах, далеких от официальных международных организаций традиционной телефонии. Первым был Международный Softswitch-консорциум *ISC* (*International Softswitch Consortium*), переименованный позже в *IPCC* (*International Packet Communication Consortium*) и занимающийся продвижением соответствующих стандартов Softswitch и обеспечением функциональной совместимости различных технологий Softswitch. В состав IPCC вошли представленные в табл. 2.1 рабочие группы (РГ), в которых и обсуждались архитектура, услуги, протоколы, а также вопросы маркетинга Softswitch.

В следующем параграфе рассматривается предложенная IPCC эталонная архитектура Softswitch. При этом IPCC не является органом стандартизации. Он только продвигает стандарты путем проведения тестов функциональной совместимости, выработки спецификаций и типовых реализаций для компаний, желающих разработать приложения на основе стандартов, установленных ITU, ETSI и IETF, которые как раз и являются органами стандартизации. В свою очередь, IPCC организует также проведение тестов функциональной совместимости, проводит учебные конференции и учреждает отраслевые рабочие группы по тем или иным важным направлениям.

Таблица 2.1. Рабочие группы в составе консорциума IPCC

Рабочая группа	Направление	Сфера деятельности
Applications WG	РГ по услугам	Ввод новых услуг, сочетающих речевую связь, доступ в Интернет, универсальную почту и др. Применение API и прикладных протоколов для взаимодействия с оборудованием разных производителей
Architecture WG	РГ по архитектуре	Архитектурная стратегия, технические требования
SIP WG	РГ по SIP	Вопросы взаимодействия различных Softswitch при создании и разрушении соединений по протоколу SIP
Device Control WG	РГ по управлению	Обеспечение функциональной совместимости устройств Softswitch, разработанных независимо
Network Boundary Functionalities WG	РГ по сетевым функциям	Документирование, представление в виде обзоров и анализ требований операторов связи
Legal Intercept WG	РГ по COPM	Координация работы с правоохранительными органами
Marketing WG	РГ по маркетингу	Формулировка цели ISC, содействие принятию и реализации предложенных ISC архитектуры и стандартов

Деятельность этих рабочих групп заслуживает самого пристального внимания. Как и любая другая отрасль, индустрия Softswitch нуждается в стандартизации. Содержимое следующего параграфа книги базируется на документе IPCC, озаглавленном «Эталонная архитектура» и определяющем сетевые уровни, стандартные интерфейсы и термины, используемые при описании компонентов Softswitch.

Справедливости ради следует отметить, что работы по построению NGN на базе Softswitch отнюдь не ограничиваются деятельностью одного IPCC. Как будет показано в следующих главах, активную работу ведут и сектор стандартизации телекоммуникаций Международного союза электросвязи ITU-T, IETF, Европейский институт стандартизации телекоммуникаций ETSI, BCD-форум (Broadband Content Delivery Forum), MSF, альянс EFMA (Ethernet in the First Mile Alliance), MPLS – форум (Multiprotocol Label Switching Forum), форум MEF (Metro Ethernet Forum), SIP – форум (Session Initiation Protocol Forum) и др.

2.2. Функциональные плоскости эталонной архитектуры Softswitch

Согласно эталонной архитектуре Softswitch, разработанной консорциумом IPCC, в ней предусматриваются четыре представленные на рис. 2.1 функциональные плоскости:

- транспортная,
- управления обслуживанием вызова и сигнализации,
- услуг и приложений,
- эксплуатационного управления.

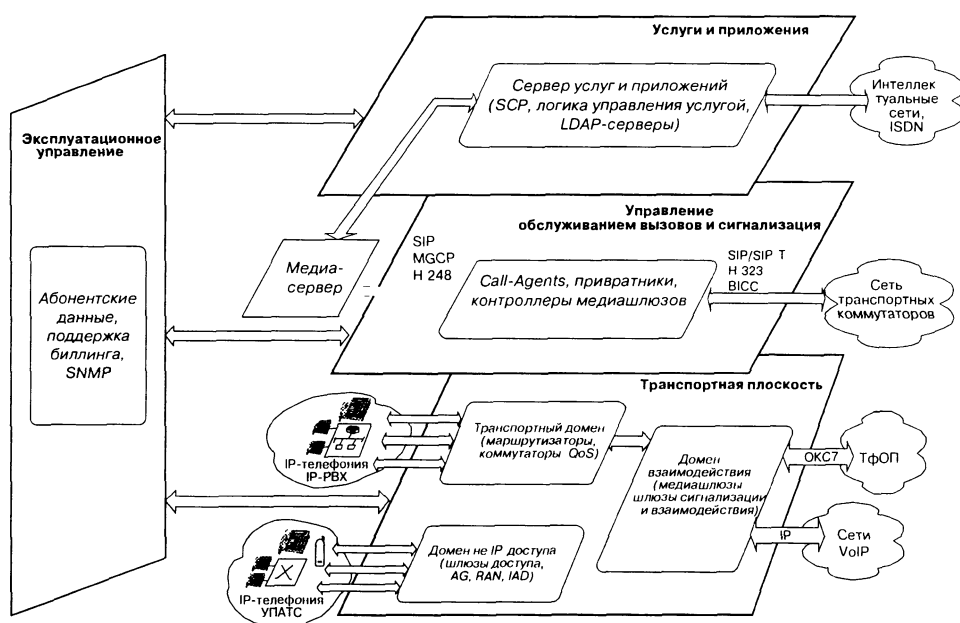


Рис. 2.1. Функциональные плоскости эталонной архитектуры Softswitch

2.2.1. Транспортная плоскость

Транспортная плоскость (Transport Plane) отвечает за транспортировку сообщений по сети связи. Этими сообщениями могут быть сообщения сигнализации, сообщения маршрутизации для организации тракта передачи информации, или непосредственно пользовательские речь и данные. Расположенный под этой плоскостью физический уровень переноса этих сообщений может базироваться на любой технологии, которая соответствует требованиям к пропускной способности для переноса трафика этого типа. Транспортная плоскость обеспечивает также доступ к сети IP-телефонии

сигнальной и/или пользовательской информации, поступающей со стороны других сетей или терминалов.

Как правило, устройствами и функциями транспортной плоскости управляют функции *плоскости управления обслуживанием вызова и сигнализации*, рассматриваемой в следующем подразделе. Сама транспортная плоскость делится на три домена:

- домен транспортировки по протоколу IP,
- домен взаимодействия и
- домен доступа, отличного от IP.

Домен транспортировки по протоколу IP (IP Transport Domain) поддерживает магистральную сеть и маршрутизацию для транспортировки пакетов через сеть IP-телефонии. К этому домену относятся такие устройства, как *коммутаторы*, *маршрутизаторы*, а также средства обеспечения качества обслуживания QoS (Quality of Service).

Домен взаимодействия (Interworking Domain) включает в себя устройства преобразования сигнальной или пользовательской информации, поступающей со стороны внешних сетей, в вид, пригодный для передачи по сети IP-телефонии, а также обратное преобразование. В этот домен входят такие устройства, как *шлюзы сигнализации (Signaling Gateways)*, обеспечивающие преобразование сигнальной информации между разными транспортными уровнями, транспортные шлюзы или *медиашлюзы (Media Gateways)*, выполняющие функции преобразования пользовательской информации между разными транспортными сетями и/или разными типами мультимедийных данных, и *шлюзы взаимодействия (Interworking Gateways)*, обеспечивающие взаимодействие различных протоколов сигнализации на одном транспортном уровне.

Домен доступа, отличного от IP (Non-IP Access Domain), предназначен для организации доступа к сети IP-телефонии различных IP-несовместимых терминалов. Он состоит из *шлюзов Access Gateways* для подключения учреждений ATC, аналоговых кабельных модемов, линий xDSL, транспортных шлюзов для мобильной сети радиодоступа стандарта GSM/3G, а также устройств *интегрированного абонентского доступа IAD (Integrated Access Devices)* и других устройств доступа. Что же касается IP-терминалов, например, SIP-телефонов, то они непосредственно подключаются к домену транспортировки по протоколу IP без участия Access Gateway.

2.2.2. Плоскость управления обслуживанием вызова и сигнализации

Плоскость управления обслуживанием вызова и сигнализации (Call Control & Signaling Plane) управляет основными элементами сети IP-телефонии и, в первую очередь, теми, которые принадлежат транспортной плоскости. В этой плоскости ведётся управление обслуживанием вызова на основе сигнальных сообщений, поступающих из транспортной плоскости, устанавливаются и разрушаются соединения, используемые для передачи пользовательской информации по сети. Плоскость управления обслуживанием вызова и сигнализации включает в себя такие устройства, как *контролер медиашлюзов MGC (Media Gateway Controller)*, *сервер управления обслуживанием вызова Call Agent*, *привратник Gatekeeper* и *LDAP-сервер*.

2.2.3. Плоскость услуг и приложений

Плоскость услуг и приложений (Service & Application Plane) реализует управление услугами и/или приложениями в сети IP-телефонии, их логику и выполнение. Устройства в этой плоскости содержат логику услуг и управляют этими услугами путем взаимодействия с устройствами, находящимися в плоскости управления обслуживанием вызова и сигнализации. Плоскость услуг и приложений состоит из таких устройств, как *серверы приложений Application Servers* и *серверы дополнительных услуг Feature Servers*. Плоскость услуг и приложений может также управлять специализированными компонентами передачи пользовательской информации, например, медиасerverами, которые выполняют функции конференцсвязи, IVR и т. п.

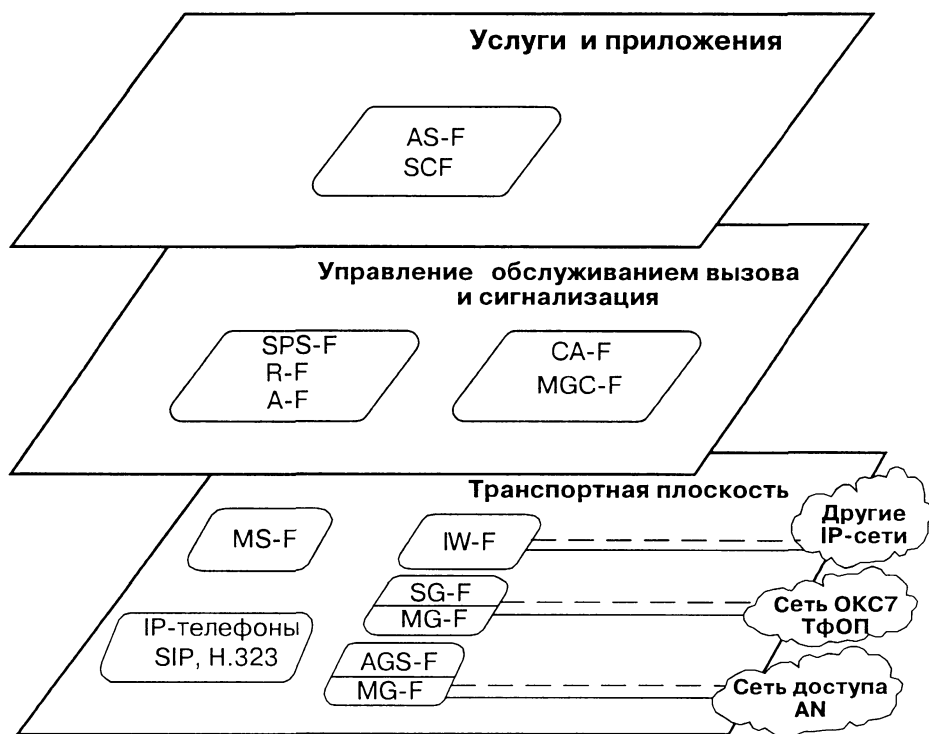
2.2.4. Плоскость эксплуатационного управления

На плоскости эксплуатационного управления (Management Plane) поддерживаются функции активизации абонентов и услуг, техобслуживания, биллинга и другие функции эксплуатационного управления сетью. Плоскость эксплуатационного управления может взаимодействовать с некоторыми или со всеми другими тремя плоскостями либо по стандартному протоколу (например, по протоколу SNMP), либо по внутренним протоколам и интерфейсам API.

2.3. Функциональные объекты

Функциональными объектами рассмотренной в предыдущем параграфе эталонной архитектуры Softswitch являются логические объекты сети IP-телефонии. В предложенном Консорциумом подходе выделяются 12 основных функциональных объектов,

относительно которых следует прежде всего подчеркнуть, что это суть функции, а не физические продукты. Последнее означает, что разные функциональные объекты могут физически располагаться в разных автономных устройствах или многофункциональных платформах, т.е. что существует практически неограниченное число способов отображения функциональных объектов в физические объекты. Перерисуем рис. 2.1 таким образом, чтобы разместить эти 12 автономных функциональных объектов (ФО) на плоскостях эталонной архитектуры Softswitch (рис. 2.2).



AS-F – ФО сервера приложений, SC-F – ФО управления услугами, CA-F – ФО устройства управления шлюзом, MGC-F – ФО контроллера медиашлюзов, SPS-F – ФО прокси-сервера SIP, R-F – ФО маршрутизации вызова, A-F – ФО учета, авторизации, аутентификации, MS-F – ФО транспортного сервера, SG-F – ФО шлюза сигнализации, MG-F – ФО медиашлюза, IW-F – ФО взаимодействия, AGS-F – ФО сигнализации шлюза доступа

Рис. 2.2. Функциональные объекты эталонной архитектуры Softswitch

ФО контроллера медиашлюзов **MGC-F** (*Media Gateway Controller Function*) представляет собой конечный автомат логики управления обслуживанием вызова и сигнализацией для одного или более транспортных шлюзов. MGC-F определяет состояние процесса

обработки каждого вызова в медиашлюзе и состояния информационных каналов для интерфейсов MG-F, передает информационные сообщения пользователя между двумя MG-F, а также между IP-телефонами или терминалами, отправляет и принимает сигнальные сообщения от портов, от других MGC-F и от внешних сетей, взаимодействует с AS-F для предоставления услуг пользователю, имеет возможность управлять некоторыми сетевыми ресурсами (например, портами MG-F, полосой пропускания и т. д.), имеет возможность устанавливать правила для портов пользователя, взаимодействует с R-F и A-F для обеспечения маршрутизации вызова, аутентификации и учета, а также может участвовать в задачах эксплуатационного управления в мобильной среде (т.к. управление мобильностью обычно является частью CA-F). Функциональный объект MGC-F обычно использует протоколы H. 248 и MGCP.

*ФО устройства управления шлюзом **CA-F** (Call Agent Function) и функциональный объект взаимодействия **IW-F** (Interworking Function) являются подмножествами MGC-F.*

Первый из них, CA-F, существует, когда MGC-F управляет обработкой вызова и определяет состояние процесса его обслуживания. Протоколами этого функционального объекта могут являться SIP, SIP-T, BICC, H. 323, Q. 931, Q. SIG, INAP, ISUP, TCAP, BSSAP, RANAP, MAP и CAP [4, 5], а в качестве интерфейсов API используются любые открытые API типа JAIN или Parlay [9].

Второй функциональный объект, IW-F, существует, когда MGC-F обеспечивает взаимодействие между разными сетями сигнализации, например, IP и ATM, OKC7 и SIP/H.323 и т. п.

*ФО маршрутизации и учета стоимости **R-F** и **A-F** (Call Routing and Accounting Functions) работают следующим образом. Функциональный объект R-F предоставляет информацию о маршрутизации вызова функциональному объекту MGC-F. Функциональный объект A-F собирает учетную информацию о вызовах для целей биллинга, а также может выполнять более широкий спектр функций AAA, т. е. обеспечивать аутентификацию, идентификацию и учет в удаленных сетях.*

Основная роль обоих функциональных объектов – реагировать на запросы, поступающие от одного или более MGC-F, направляя вызов или учетную информацию о нем к входящим портам (другим MGC-F) или услугам (AS-F). Функциональный объект R-F/A-F обеспечивает функцию маршрутизации для локальных и межсетевых вызовов (R-F), фиксирует детали каждого сеанса связи для целей биллинга и планирования (A-F), обеспечивает управление сеансом и управление мобильностью, может узнавать о маршрутной информации от внешних источников, может взаимодействовать

с AS-F для предоставления услуги пользователю, может функционировать прозрачно для других элементов в тракте сигнализации. Здесь R-F и A-F могут сцепляться друг с другом последовательно или иерархически, и к тому же R-F/A-F часто объединяется с MGC-F, причем объединенный R-F/A-F/MGC-F может также запрашивать услуги внешнего R-F/A-F. Сам A-F собирает и передает учетную информацию о каждом вызове, а AS-F передает учетную информацию о предоставлении дополнительных услуг, таких как конференцсвязь или платные информационные услуги.

Функция маршрутизации для локальных и межсетевых вызовов R-F может использовать протоколы *ENUM* и *TRIP*, а функция учета стоимости A-F может использовать протокол *RADIUS* и *AuC* (для сетей подвижной связи).

ФО SIP-прокси-сервера **SPS-F** (*SIP Proxy Server Function*) выделен в отдельный функциональный объект по той причине, что чаще всего R-F и A-F конструктивно оформляются в виде прокси-сервера SIP.

ФО шлюза сигнализации **SG-F** (*Signaling Gateway Function*) поддерживает шлюз для обмена сигнальной информацией между сетью IP-телефонии и ТфОП, которая может передаваться на базе ОКС7/TDM или, например, ВСС/АТМ. Для беспроводных сетей подвижной связи SG-F поддерживает также шлюз для обмена сигнальной информацией между транзитной пакетной IP-сетью и сетью сотовой подвижной связи (СПС) с коммутацией каналов на базе стека ОКС7. Основная роль SG-F заключается в пакетировании и транспортировке протоколов сигнализации ОКС7 в ТфОП (ISUP или INAP) или в СПС (MAP или CAP) по сети с коммутацией пакетов IP. Для этого функциональный объект SG-F пакетирует и транспортирует протоколы сигнализации ОКС7 к MGC-F или другому SG-F, используя методы Sigtran. Один SG-F может обслуживать много MGC-F, а интерфейсом между SG-F и другими функциональными объектами является протоколы Sigtran типов TUA, SUA и M3UA over SCTP, за исключением ситуаций, когда SG-F и MGC-F или другой SG-F объединены в одном месте.

ФО сигнализации шлюза доступа **AGS-F** (*Access Gateway Signaling Function*) поддерживает шлюз для обмена сигнальной информацией между сетью IP-телефонии и сетью доступа с коммутацией каналов на базе интерфейса V5.1/V5.2 [11] или ISDN [5].

Для беспроводных сетей подвижной связи AGS-F поддерживает также шлюз для обмена сигнальной информацией между транзитной сетью подвижной связи с коммутацией пакетов и сетью СПС на базе TDM или АТМ. Основная роль AGS-F заключается в пакетировании и транспортировке протоколов сигнализации интерфейсов V5 или ISDN (для проводных сетей), или BSSAP или

RANAP (для беспроводных сетей) по сети с коммутацией пакетов IP. AGS-F пакетирует и транспортирует к MGC-F протоколы сигнализации V5, ISDN или OKC7, используя протоколы Sigtran типов M3UA, IUA и V5UA over SCTP.

*ФО сервера приложений **AS-F** (Application Server Function)* поддерживает логику и выполнение услуг для одного или более приложений. AS-F может запрашивать у MGC-F прекращение вызовов или сеансов связи для определенных приложений (например, речевой почты или конференцсвязи), может запрашивать у MGC-F повторное инициирование услуг связи (например, сопровождающего вызова или вызовов по предоплаченной телефонной карте), может изменять описания потоков пользовательских данных, участвующих в сеансе, используя протокол SDP, может управлять MS-F для обслуживания потоков пользовательской информации, может komponоваться с Web-приложениями или иметь Web-интерфейсы, может использовать открытые API типа JAIN или Parlay для создания услуг, может иметь внутренние интерфейсы алгоритма распределения ресурсов, биллинга и регистрации сеансов, может взаимодействовать с функциональными объектами MGC-F или MS-F, может вызывать другой AS-F для предоставления дополнительных услуг или для построения составных, ориентированных на компоненты приложений, может использовать функциональные возможности MGC-F для управления внешними ресурсами. Для всех этих целей используются протоколы SIP, MGCP, H. 248, LDAP, HTTP, CPL и XML. Совместное использование функциональных объектов AS-F и MGC-F обеспечивает поддержку составных услуг для пользователей, таких как сетевые записанные объявления, трехсторонняя связь, уведомление о поступлении нового вызова и т. д. В ситуациях, когда AS-F и MGC-F реализованы в одной системе, вместо подключения AS-F к MGC-F по одному из вышеуказанных протоколов производители часто используют API типа JAIN или Parlay. При такой организации, AS-F называют сервером дополнительных услуг (Feature Server).

*ФО управления услугами **SC-F** (Service Control Function)* существует, когда AS-F управляет логикой услуг. SC-F использует протоколы INAP, CAP и MAP, а также открытые API типа JAIN и Parlay.

*ФО медиашлюза **MG-F** (Media Gateway Function)* обеспечивает сопряжение IP-сети с портом доступа, с соединительной линией или с совокупностью портов и/или соединительных линий, служа, тем самым, шлюзом между пакетной сетью и внешними сетями с коммутацией каналов, такими как ТфОП, СПС или АТМ. Его основная роль состоит в преобразовании пользовательской информации из одного формата передачи в другой, чаще всего – из канального вида в пакетный и обратно, из ячеек АТМ в пакеты IP и обратно.

MG-F имеет следующие характеристики:

- всегда состоит в отношениях ведущий/ведомый с MGC-F с использованием протокола управления MGCP или MEGACO/H.248;
- может выполнять функции обработки пользовательской информации, такие как кодирование, пакетирование, эхокомпенсацию, управление буферами, устранение джиттера, корректирующие действия при потерях пакетов и др.;
- может выполнять функции обслуживания пользовательских соединений, такие как генерирование акустических сигналов, генерирование сигналов DTMF, генерирование комфортного шума и др., а также выполнять анализ цифр на базе таблицы, загружаемой от MGC-F;
- может выполнять функции сигнализации и обнаружения событий передачи пользовательской информации, такие как обнаружение сигналов DTMF, обнаружение состояний отбоя/ответа абонента, детектирование наличия речевых сигналов и др.

Таким образом, MG-F поддерживает механизм, позволяющий MGC-F контролировать состояние и функциональные возможности портов, а самому ему не требуется знать состояния процессов обслуживания вызовов, проходящих через него; он поддерживает только сами соединения. Используемые протоколы и технологии: RTP/RTCP, TDM, H. 248 и MGCP. Кстати, SIP-телефон или шлюз с поддержкой SIP с этой функциональной точки зрения представляет собой MG-F и MGC-F в одном блоке.

ФО медиасервера **MS-F** (*Media Server Function*) обеспечивает управление обработкой пользовательского пакетного трафика от любых приложений. В основном, он функционирует в качестве сервера, обслуживающего запросы от AS-F или MGC-F касательно выполнения обработки пользовательской информации в пакетированных потоках мультимедиа. MS-F поддерживает различные кодеки и схемы кодирования, может управляться AS-F или MGC-F непосредственно (управление ресурсами) или косвенно (вызов функции) с использованием протоколов SIP, MGCP и H. 248. Функциональный объект MA-F может параллельно поддерживать обнаружение набираемых цифр, генерирование и передачу акустических сигналов и записанных сообщений, регистрацию и запись мультимедийных потоков, распознавание речи, речевое воспроизведение текста, микширование для конференцсвязи, обработку факсимильных сообщений, определение наличия речевых сигналов и передачу информации о громкости.

2.4. Модуль контроллера медиашлюзов

Теперь вернемся от функциональных объектов к реальным физическим объектам и, прежде всего, – к контроллеру медиашлюзов MGC, являющемуся одним из ключевых элементов сети IP-телефонии. Имеется множество различных реализаций MGC, в связи с чем он известен под разными именами: *Softswitch*, *Call Agent*, *Call Controller*, *Telephone Server* и др. На рис. 2.3 представлены только некоторые из множества возможностей функциональной компоновки MGC согласно рассматриваемой в этой главе эталонной архитектуре ISC.

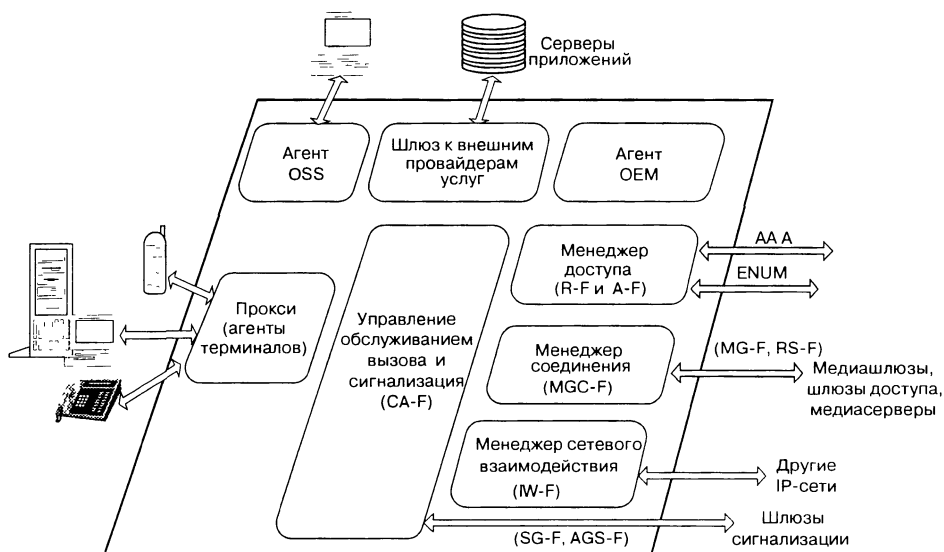


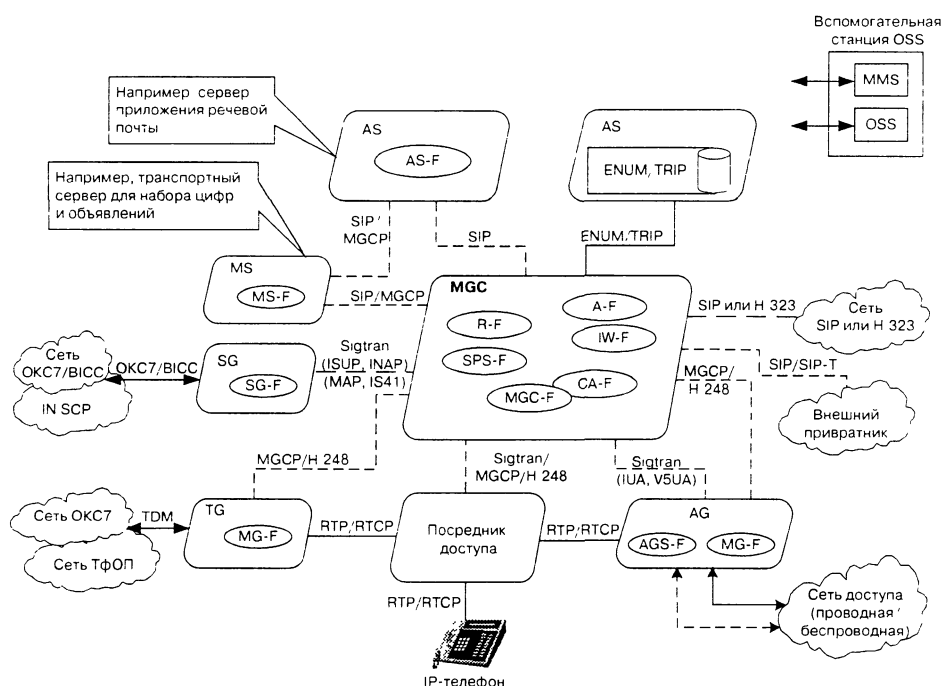
Рис. 2.3. Модули контроллера транспортных шлюзов в эталонной архитектуре ISC

Как видно на рис. 2.3, в большинстве современных контроллеров медиашлюзов MGC, помимо MGC-F, реализованы и другие функциональные объекты. В частности, в представленный на рисунке контроллер MGC входят функциональные блоки:

- менеджера сеансов соединения Connection Session Manager (MGC-F),
- управления обслуживанием вызова и сигнализацией (CA-F),
- менеджера взаимодействия Interworking/Border Connection Manager (IW-F),
- менеджера сеансов доступа Access Session Manager (R-F/A-F),
- шлюз доступа к открытым услугам Open Service Access Gateway,
- модули-посредники приложений (Proxies),

- агенты системы эксплуатационной поддержки OSS и OEM, которые подключаются к внешним менеджерам OSS/OEM, расположенным в центре эксплуатационной поддержки, для обеспечения функций сетевого управления, подготовки к работе услуг и сети, техобслуживания и т. д.

Все упомянутые на рис. 2.3 функциональные объекты CA-F, IW-F, R-F и A-F могут совмещаться в одной физической платформе или распределяться по разным устройствам, которые в совокупности дают итоговое техническое решение MGC. В свою очередь, из соображений надежности и/или распределения нагрузки MGC может быть реализован на параллельно работающих устройствах со всеми перечисленными функциями в каждом.



ПРИМЕЧАНИЕ. Пунктирные линии представляют реализацию информационных потоков, полученную в результате выбора протокола и интерфейсов в соответствии с требованиями к обслуживанию этого рисунка и соответствующий выбор протоколов приводятся только в информационных целях

Рис. 2.4. Реализация контроллера транспортных шлюзов в эталонной архитектуре IPCC

Для иллюстрации вышеизложенного рассмотрим пример реализации функций Softswitch (рис. 2.4).

В этом примере Softswitch управляет шлюзами между сетью ТФОП/IN и IP-сетью, транспортными шлюзами и транспортными серверами посредством своего функционального объекта MGC-F, используя соответствующие протоколы управления шлюзами.

Кроме того, MGC обменивается сигнальными сообщениями с портами, другими Softswitch и внешними сетями. Эту функцию выполняет модуль управления обслуживанием вызова и сигнализации (CA-F), который также сохраняет данные о состоянии процесса обслуживания каждого вызова.

В представленной на рис. 2.4 схеме Softswitch реализованы и другие функциональные объекты, а именно: маршрутизации и учета стоимости вызовов (R-F/A-F), прокси-сервера SIP (SPS-F) и менеджера пограничных соединений (IW-F). Кроме того, Softswitch взаимодействует через модуль шлюза открытых услуг Open Service Gateway Block с серверами приложений для поддержки услуг, которые не являются «родными» для Softswitch, а подключаются посредством различных протоколов управления услугами и API, таких как SIP, JAIN и Parlay.

Обобщая пример на рис. 2.4, перечислим в заключение этой главы функциональные элементы Softswitch и соответствующие им протоколы и/или интерфейсы API.

AS-F (Application Server Function):

- SIP, MGCP, H. 248, LDAP
- HTTP, CPL, XML
- Open APIs (JAIN, PARLAY и т.д.)

SC-F (Service Control Function)

- INAP, CAP, MAP
- Open APIs (JAIN, PARLAY и т.д.)

MS-F (Media Server Function)

- SIP, MGCP, H. 248

SG-F (Signaling Gateway Function)

- Sigtran (TUA, SUA, M3UA over SCTP)

IW-F (Interworking Function) Protocols

- H.323/SIP, IP/ATM

MG-F (Media Gateway Function)

- RTP/RTCP, TDM
- H.248, MGCP

ASG-F (Access Signaling Gateway Function)

- Sigtran (M3UA, IUA, V5UA over SCTP)

CA-F (Call Agent Function)

- SIP, SIP-T, BICC, H. 323
- Q. 931, Q. SIG, INAP, ISUP, TCAP

- (Mobile) BSSAP, RANAP, MAP, CAP
- Open APIs (JAIN, PARLAY и т.д.)

SPS-F (SIP Proxy Server Function)

- SIP

MGC-F (Media Gateway Controller Function)

- H.248, MGCP

A-F (Authentication, Authorization, Accounting Function)

- RADIUS
- AuC для мобильных сетей

R-F (Routing Function)

- ENUM, TRIP

В следующих главах, начиная с главы 4, мы последовательно рассмотрим приведенные в правой колонке протоколы, но сначала посвятим одну главу тому, что по традиции назовем IP-телефонией, хотя сегодня более точно было бы именовать эту технологию IP-коммуникациями в силу характера обсуживаемого трафика, ставшего по своей структуре не просто телефонным, а действительно мультимедийным.

Глава 3

IP-телефония

Мы считаем эти истины очевидными...
Декларация о независимости

3.1. Этапы развития

Приведенными в эпиграфе словами начинается Декларация о независимости США, содержащая отнюдь не очевидные, а весьма революционные для тогдашнего устройства человеческого общества идеи. Та же степень неочевидности и революционности с точки зрения Операторов сетей связи и всей связистской общественности была присуща и IP-телефонии [8], перевернувшей казавшиеся незыблемыми принципы построения всепланетной сети связи.

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

Докоммерческий этап характеризовался научно-исследовательской деятельностью в разных университетах и исследовательских организациях сообщества Интернет. Первая в истории попытка испробовать IP-телефонию была произведена в 1983 году в Кембридже, Массачусетс. В состав оборудования рабочих станций разных исследовательских проектов была включена так называемая «речевая воронка», выполнявшая функции цифровизации речи, ее пакетирования и передачи через Интернет между офисами BBN (Bolt, Beranek, Newman) на Восточном и Западном побережьях США. Немногочисленные энтузиасты IP-телефонии первого поколения должны были заранее находиться в режиме подключения к системе к моменту вызова, использовать на обоих концах одно самодельное программное обеспечение и тратить во время разговора значительные усилия на регулировку компрессии и попытки компенсации эха. Качество речи портили и длинные паузы, вызванные случайными задержками при прохождении пакетов по Интернет,

«рваная» речь, получавшаяся в результате потерь пакетов, эхо из-за близкого расположения динамика компьютера и микрофона. И все же, именно в то время были созданы две рабочие группы IETF: AVT (*Audio/Video Transport*) – группа транспортировки аудио/видео, которая создала транспортный протокол реального времени RTP, и MMUSIC (*Multiparty Multimedia Session Control*) – группа управления мультимедийным сеансом, спроектировавшая семейство протоколов для мультимедийной конференцсвязи через Интернет, включая самый удачный протокол IP-телефонии – протокол SIP [10], – который рассматривается в следующей главе.

Компьютерный этап был начат израильской компанией VocalTec, сумевшей к 1995 году собрать воедино достижения в областях процессоров цифровой обработки сигналов (DSP), кодеков, компьютеров, протоколов маршрутизации и увеличившей свой доход с 46 тысяч долларов во втором квартале 1995 года до 181 миллиона долларов во втором квартале 1996 года (из-за чего, собственно, предшествовавший этому этап развития IP-телефонии и назван до-коммерческим). Первоначально продукты VocalTec допускали только соединения PC – PC. Все функции сигнализации и управления реализовались непосредственно в этих PC, а программное обеспечение сеансов связи все еще ориентировалось на нестандартные протоколы разных компаний-производителей. Но уже в июне 1996 года 16-я Исследовательская комиссия Международного союза электросвязи (ITU-T) согласовала версию 1 протокола H.323, названную стандартом для видеоконференцсвязи с негарантированным качеством обслуживания через локальную вычислительную сеть. Этот первый «зонтичный» стандарт IP-телефонии появился в нужное время и открыл тем самым следующий этап инфокоммуникационных услуг. Стек протоколов H.323 рассматривается в главе 5 книги.

Инфокоммуникационный этап IP-телефонии знаменуется тем, что услуга передачи речи через IP-сети, которая первоначально не воспринималась как угроза существующим телекоммуникационным Операторам, оказалась с успехом востребована почти всеми сторонами в отрасли как инновационное средство, реально способное выполнить обещания мультимедийных коммуникаций, которые однажды уже были даны B-ISDN, но не оправдались.

Да и по мере развития первых сетей IP-телефонии стали проявляться недостатки и ограничения H.323. Весьма важным ограничением стало то, что шлюз H.323 обрабатывает сигнализацию, выполняет управление обслуживанием вызова и транскодирование транспортных потоков в едином блоке, что создает проблему масштабируемости при росте трафика. Кроме того, H.323 не обеспечивает также возможности подключения к OKC7, что препятствует его «бесшовной» интеграции с существующей телефонной сетью общего пользования. Для того чтобы справиться с этими проблемами,

и была разработана концепция декомпозиции шлюза, при которой управление обслуживанием вызова сосредоточено в одном блоке, называемом Softswitch или контроллером транспортного шлюза *MGC (Media Gateway Controller)*, а элементы преобразования транспортных потоков находятся в другом блоке, называемом транспортным шлюзом *MG (Media Gateway)*, что подробно обсуждалось в двух предыдущих главах. Тогда же, в 1998 году, был создан протокол управления шлюзами MGCP (*Media Gateway Control Protocol*), а после еще двух лет напряженной работы Исследовательской комиссии 16 ITU-T и IETF в июне 2000 появился стандарт управления транспортным шлюзом, названный H.248 или MEGACO. Этим протоколам посвящена глава 6. Сам же мультимедийный трафик переносится по IP-сети, как правило, протоколом RTP. Поскольку этот протокол в Softswitch не обрабатывается, в книге он подробно не рассматривается. Тем не менее, краткое описание RTP полезно для понимания архитектуры сети NGN, и оно приводится в следующем параграфе.

3.2. Протокол RTP

Основным транспортным протоколом для мультимедийных приложений стал *протокол реального времени RTP (Real-Time Protocol)*, предназначенный для организации передачи пакетов с кодированными речевыми сигналами по IP-сети. Передача пакетов RTP ведется поверх протокола UDP, работающего, в свою очередь, поверх IP (рис. 3.1).

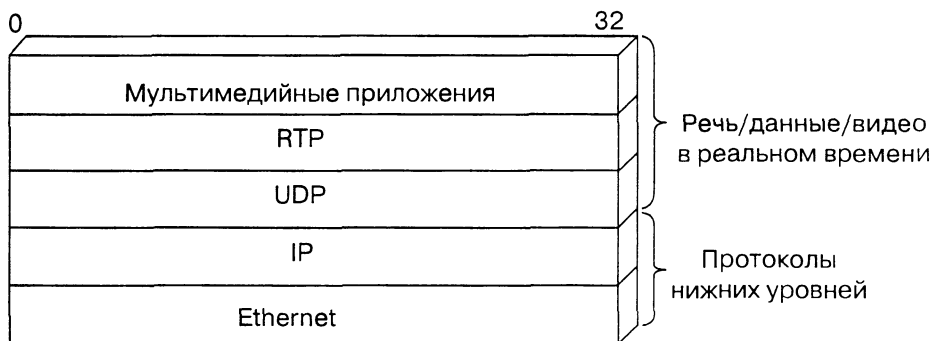


Рис. 3.1. Уровни протоколов RTP/UDP/IP

На самом деле уровень, к которому относится RTP, не определяется настолько однозначно, как это показано на рис. 3.1 и как это обычно описывается в литературе. С одной стороны, протокол действительно работает поверх UDP, реализуется прикладными программами и, по всем признакам, является прикладным протоколом. Но в то же время, как сказано в начале этого параграфа,

RTP предоставляет транспортные услуги независимо от мультимедийных приложений и является, с этой точки зрения, просто транспортным протоколом. Наиболее удачное определение RTP дано Э. Таненбаумом в [25]: *RTP — это транспортный протокол, реализованный на прикладном уровне.*

Для передачи речевого (мультимедийного) трафика RTP использует пакеты, структура которых показана на рис. 3.2.

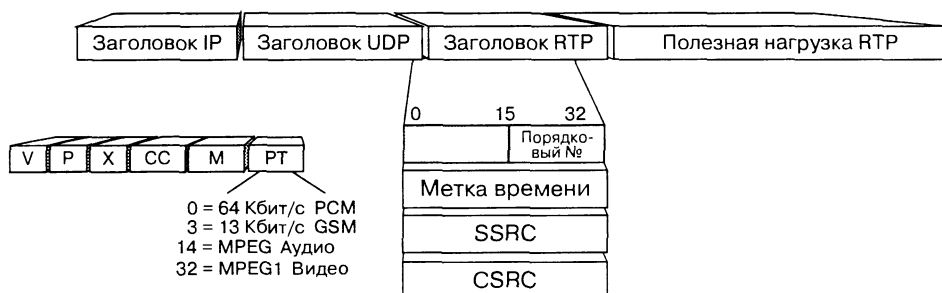


Рис. 3.2. Заголовок VoIP

Пакет RTP состоит, как минимум, из 12 байтов. В двух первых битах RTP-заголовка (поле бита версии, V) указывается версия протокола RTP (в настоящее время это версия 2). Ясно, что при такой структуре заголовка возможна максимум еще только одна версия RTP. Следующее за ними поле содержит два бита: бит P, который указывает, были ли добавлены в конце поля с полезной нагрузкой символы-наполнители (они обычно добавляются, если транспортный протокол или алгоритм кодирования требует использования блоков фиксированного размера), и бит X, который указывает, используется ли расширенный заголовок. Если он используется, то первое слово расширенного заголовка содержит общую длину расширения.

Далее, четыре бита CC определяют число CSRC-полей в конце RTP-заголовка, т.е. число источников, формирующих поток. Маркерный бит M позволяет отмечать то, что стандарт определяет как *существенные события*, например, начало видеокadra, начало слова в аудиоканале и т.п. За ним следует поле типа данных PT (7 битов), где указывается код типа полезной нагрузки, определяющий содержимое поля полезной нагрузки – *данные приложения (Application Data)*, например, несжатое 8-битовое аудио MP3 и т.п. По этому коду приложение может узнать, что нужно делать, чтобы декодировать данные. Остальная часть заголовка фиксированной длины состоит из поля *порядкового номера (SequenceNumber)*, поля *метки времени (Time Stamp)* для записи момента создания первого слова пакета и поля *источника синхронизации SSRC*, которое идентифицирует этот источник. В последнем поле можно

указывать единственное устройство, имеющее только один сетевой адрес, множественные источники, которые могут представить различные мультимедийные среды (аудио, видео и т.д.), или разные потоки одной и той же среды. Так как источники могут быть на разных устройствах, SSRC-идентификатор выбирается случайным образом, чтобы шанс получить данные сразу от двух источников во время RTP-сеанса был минимальным. Однако определен также и механизм решения конфликтов, если они возникают. За фиксированной частью RTP-заголовка могут следовать еще до 15 отдельных 32-разрядных CSRC-полей, которые идентифицируют источники данных.

RTP поддерживается *протоколом управления транспортировкой в реальном времени RTCP (Real-Time Transport Control Protocol)*, который формирует дополнительные отчеты, содержащие информацию о сеансах связи RTP. Напомним, что ни UDP, ни RTP не занимаются обеспечением качества обслуживания QoS (*Quality of Service*). Протокол RTCP обеспечивает обратную связь с отправителями, а получателям потоков он предоставляет некоторые возможности повышения QoS, информацию о пакетах (потери, задержки, джиттер) и о пользователе (приложении, потоке). Для управления потоком существуют отчеты двух типов – генерируемые отправителями и генерируемые получателями. Например, информация о доле потерянных пакетов и абсолютном количестве потерь позволяет отправителю при получении отчета обнаруживать, что перегрузка канала может заставить получателей не принимать потоки пакетов, которые они ожидали. В этом случае отправитель имеет возможность понизить скорость кодирования, чтобы уменьшить перегрузку и улучшить прием. Отчет отправителя содержит информацию о том, когда был генерирован последний RTP-пакет (она включает в себя как внутреннюю метку, так и реальное время). Эта информация позволяет получателю координировать и синхронизировать множественные потоки, например, видео и аудио. Если поток направляется нескольким получателям, то организуются потоки RTCP-пакетов от каждого из них. При этом будут предприняты шаги для ограничения ширины полосы – обратно пропорционально скорости, с которой генерируются RTCP-отчеты, и числу получателей.

Следует заметить, что хотя RTCP работает отдельно от RTP, но уже и сама цепочка RTP/UDP/IP приводит к существенным накладным расходам (в виде их заголовков). Как будет отмечено в следующем параграфе, кодек G.729 генерирует пакеты размером в 10 байтов (80 битов каждые 10 мс). Один RTP-заголовок, размером в 12 байтов, больше, чем весь этот пакет. К нему, кроме того, должен быть добавлен 8-байтовый UDP-заголовок и 20-байтовый IP-заголовок (в версии Ipv4), что создает заголовок, в четыре раза превосходящий по размеру передаваемые данные. Чуть подробнее мы рассмотрим это в следующем параграфе.

3.3. Кодеки VoIP

С момента первого телефонного соединения между Беллом и Ватсоном речевую информацию стали преобразовывать в формат аналогового электрического сигнала. При переходе к цифровым телефонным сетям эти речевые сигналы перед отправкой в сеть начали подвергать *дискретизации* (формированию дискретных во времени отсчетов амплитуды сигнала), *квантованию* (определению амплитуды полученного отсчета числом с конечной точностью – дискретизации по амплитуде) и *кодированию*. Стандартной для традиционной телефонии стала примитивная с сегодняшней точки зрения схема ИКМ-кодирования речевого сигнала, хотя никогда не прекращались поиски более сложных и эффективных алгоритмов, позволяющих снизить требования к полосе пропускания.

Революционным толчком, позволившим прийти к передаче речи средствами IP-телефонии, стало появление процессоров цифровой обработки сигналов *DSP (Digital Signal Processor)*, архитектура которых оптимизирована для выполнения операций, характерных для типичных алгоритмов обработки сигналов, например, умножение с накоплением или выборку операндов с бит-инверсной адресацией для выполнения быстрого преобразования Фурье. Физически DSP выполняются в виде интегральных микросхем, содержащих в одном кристалле ядро процессора, память и периферийные устройства для обмена информацией. Наличие встроенной памяти обеспечивает быстрый доступ ядра к ее содержимому для получения максимальной производительности. Функционально на DSP реализуются кодеки для использования в приложениях VoIP.

Различаются эти кодеки, в частности, по *требуемой полосе пропускания канала*. Для узкополосных кодеков скорость передачи информации лежит в пределах 1.2 – 64 Кбит/с, что определяет качество передачи речи. Существует несколько подходов к проблеме определения качества, наиболее популярным из которых является *оценка MOS (Mean Opinion Score)*, которая определяется как среднее значение оценок качества по пятибалльной шкале, данных большой группой слушателей. Экспертам предъявляются для прослушивания разные звуковые фрагменты – речь, музыка, речь на фоне того или иного шума и т.д. Оценки интерпретируют следующим образом: 4-5 – высокое качество, которое аналогично или выше качества передачи речи при разговоре по сети ISDN; 3.5-4 – качество ТфОП (toll quality), обеспечиваемое при большинстве телефонных связей через ТфОП, а мобильные сети обеспечивают качество чуть ниже toll quality; 3-3.5 – качество речи по-прежнему удовлетворительное, однако его ухудшение хорошо заметно на слух; 2.5-3 – речь разборчива, однако для ее понимания требуется концентрация внимания

Кроме того, еще одной функцией кодеков в шлюзах VoIP является *подавление периодов молчания (VAD, CNG, DTX)*, позволяющее уменьшить объем информации, передаваемой в течение таких периодов, и освободить на это время занимаемую полосу пропускания. В двустороннем разговоре такие меры позволяют сократить объем передаваемой информации до 50%, а в децентрализованных многоадресных конференциях за счет большего числа говорящих – и более. Технология подавления молчания имеет три важных составляющих: *детектор речевой активности VAD (Voice Activity Detector)* определяет моменты времени, когда пользователь говорит, оценивает энергию входного сигнала и активизирует передачу, если она выше некоторого порога; *прерывистая передача DTX (Discontinuous Transmission)* вынуждает кодек прекратить передачу пакетов в то время, когда VAD обнаружил период молчания (а возобновляет ее снова VAD); *генератор комфортного шума CNG (Comfort Noise Generator)*, создающий у говорящего ощущение присутствия собеседника на другом конце при отключенной передаче. Совершенные кодеки, например, G.723.1 Annex A или G.729 Annex B имеют возможность предоставлять удаленному декодеру информацию для восстановления шума с близкими к исходному параметрами.

Большинство кодеков обрабатывает речевую информацию блоками, называемыми кадрами. Выбор размера кадра (*frame*) важен, так как минимальная теоретически достижимая задержка передачи информации (т.н. алгоритмическая задержка) определяется суммой этого параметра и длины буфера предварительного анализа.

Как было показано в предыдущем параграфе, к кадру, сгенерированному кодеком, добавляется необходимая дополнительная информация: заголовки IP (20 байтов), UDP (8 байтов) и RTP (12 байтов), поэтому большинство реализаций VoIP использует пересылку нескольких кадров в пакете. Число таких кадров ограничено максимально допустимой задержкой. В большинстве случаев в одном пакете передается до 120 мс речевой информации.

Еще одним фактором работы шлюзов VoIP является чувствительность к потерям кадров, являющимся неотъемлемым атрибутом IP-сетей. Применяются коды с исправлением ошибок, позволяющие снизить количество потерь кадров при данном числе потерянных пакетов. Некоторая избыточная информация распределяется между несколькими пакетами так, что при потерях некоторого числа пакетов кадры могут быть восстановлены. Но положительный эффект при введении избыточности для борьбы с потерями кадров не столь легко достижим, так как потери в IP-сетях происходят пачками, т.е. значительно более вероятно, что будут наблюдаться потери сразу нескольких пакетов подряд, чем потери всего одного из нескольких последовательно передаваемых пакетов. Так что, если применить простые схемы введения

избыточности, например, повторяя посылку каждого кадра два раза в соседних пакетах, то это, скорее всего, окажется в реальных условиях бесполезным, приводя лишь к передаче значительного объема избыточной информации. Кроме того, введение избыточности отрицательно сказывается на задержке воспроизведения сигнала. Например, если мы повторяем один и тот же кадр в четырех следующих один за другим пакетах, для того чтобы обеспечить возможность восстановления информации при потере трех подряд идущих пакетов, декодер вынужден поддерживать буфер из четырех пакетов, а это вносит значительную дополнительную задержку. Влияние потерь кадров на качество воспроизводимой речи зависит от используемого кодека. Если потерян кадр, состоящий из N отсчетов кодека G.711, то на приемном конце будет отмечен пропуск звукового фрагмента длительностью $N \cdot 125$ мкс. Если используется более совершенный узкополосный кодек, то потеря кадра может сказываться на воспроизведении нескольких последующих, так как декодеру потребуется время для того, чтобы достичь синхронизации с кодером – потеря кадра длительностью 20 мс может привести к слышимому эффекту длительностью 150 мс и более. Кодеры типа G.723.1 разрабатывались так, что они функционируют без существенного ухудшения качества в условиях некоррелированных потерь до 3% кадров, однако при превышении этого порога качество ухудшается катастрофически.

Отметим, что G.711 – наиболее известный, часто называемый просто ИКМ, цифровой кодек речевых сигналов, поддерживаемый всеми шлюзами VoIP, был стандартизован ITU-T в 1965 году, его типичная оценка MOS составляет 4.3.

Рекомендация G.723.1 утверждена ITU-T в ноябре 1995 года. Кодек G.723.1 имеет длительность кадра 30 мс с длительностью предварительного анализа 7.5 мс и два режима работы: 6.3 Кбит/с (кадр имеет размер 189 битов, выровненных до 24 байтов) и 5.3 Кбит/с (кадр имеет размер 158 битов, выровненных до 20 байтов). G.723.1 обеспечивает оценку MOS 3.7 в режиме 6.3 Кбит/с и 3.9 в режиме 5.3 Кбит/с, имеет детектор речевой активности и обеспечивает генерацию комфортного шума на удаленном конце в период молчания.

ADPCM кодек G.726 (рекомендация принята в 1990 г.) обеспечивает кодирование цифрового потока G.711 со скоростью 40, 32, 24 или 16 Кбит/с, поддерживая оценки MOS на уровне 4.3 (32 Кбит/с), что часто принимается за эталон уровня качества телефонной связи (toll quality). В приложениях VoIP этот кодек практически не используется, так как он не обеспечивает достаточной устойчивости к потере информации.

Кодек G.728 использует оригинальную технологию линейного предсказания с малой задержкой LD-CELP (low delay code excited

linear prediction) и обеспечивают оценки MOS, аналогичные G.726 при скорости передачи только 16 Кбит/с.

Кодек G.729 очень популярен в сетях Frame Relay, использует технологию CS-ASELP (Conjugate Structure, Algebraic Code Excited Linear Prediction) и обеспечивает скорость передачи 8 Кбит/с. В рамках спецификаций G.729 определены алгоритмы VAD, CNG и DTX.

Еще одной задачей шлюзов VoIP является передача сигналов *многочастотного набора номера DTMF*. Узкополосные кодеки, чтобы достичь низких скоростей передачи информации, опираются на тот факт, что сигнал, который они кодируют, представляет собой именно речь, а сигналы DTMF при прохождении через такие кодеки искажаются и не могут быть успешно опознаны соответствующим приемником на удаленном конце. В ряде случаев, а именно, когда пользователь ТФОП вынужден ввести какую-то дополнительную информацию в удаленную систему при уже установленном соединении (например, номер дебитной карты или номер пункта меню автоинформатора), необходимо обеспечить возможность надежной передачи DTMF-сигналов через сеть VoIP. Существуют две процедуры передачи DTMF-информации по сетям VoIP:

- обязательный метод, в соответствии с которым специальное сообщение протокола H.245 (Userinputindication) может содержать символы цифр и знаки «*» и «#». Используется надежное TCP-соединение, так что информация не может быть потеряна, однако из-за особенностей TCP могут иметь место значительные задержки;
- нестандартный метод, предложенный VoIP форумом, может быть использован в терминалах H.323v2 при использовании процедуры fastStart и отсутствии канала H.245. В этом случае для передачи DTMF открывается специальный RTP-сеанс, в котором передаются кодированные значения принятых цифр, а также амплитуды и длительности сигналов. Использование RTP позволяет четко привязать сигналы DTMF к реальному времени, что является важным преимуществом этого метода.

3.4. Сценарии IP-телефонии

3.4.1. Сети H.323

Первый в истории подход к построению сетей IP-телефонии на стандартизированной основе предложен Международным союзом электросвязи (ITU) в рекомендации H.323. Сети на базе протоколов H.323 ориентировались на интеграцию с телефонными сетями и вначале рассматривались как сети ISDN, наложенные на IP-сети.

В частности, процедура установления соединения в сетях IP-телефонии по H.323 базировалась на рекомендации Q.931 и аналогична процедуре, используемой в ISDN.

Протокол H.323 подробно рассматривается в главе 5 книги, а здесь отметим, что рекомендация H.323 включает в себя довольно сложный набор протоколов, который предназначен не просто для передачи речевой информации по IP-сетям с коммутацией пакетов, а обеспечивает работу мультимедийных приложений в сетях с не гарантированным качеством обслуживания. Речевой трафик – это только одно из приложений H.323, наряду с видео и данными. *Протокол RAS (Registration, Admission, Status)*, входящий в семейство протоколов H.323, обеспечивает контроль использования сетевых ресурсов и поддерживает аутентификацию пользователей и начисление платы за услуги. Основными устройствами сети H.323 являются: *терминал (Terminal)*, *шлюз (Gateway)*, *привратник (Gatekeeper)* и *устройство управления конференциями (Multipoint Control Unit)*, которые также рассматриваются в главе 5.

В контексте Softswitch целесообразно заметить, что рекомендациями предусмотрен еще один элемент сети H.323 – *прокси-сервер H.323*. Этот сервер функционирует на прикладном уровне и может проверять пакеты с информацией, которой обмениваются два приложения. Прокси-сервер может определять, с каким приложением (H.323 или другим) ассоциирован вызов, и производить нужное соединение.

Входящий в состав H.323 *протокол H.225.0 (Q.931)* специфицирует процедуры установления, поддержания и разрушения соединения, а в качестве транспортного протокола использует протокол TCP. По *протоколу H.245* происходит обмен между участниками соединения информацией, которая необходима для создания логических каналов. По этим каналам передается речевая информация, упакованная в пакеты RTP/UDP/IP, которые рассмотрены выше и представлены на рис. 3.1.

В этом же параграфе была упомянута еще одна важная проблема – качество обслуживания в сетях H.323. Оконечное устройство, запрашивающее у привратника разрешение на доступ, может, используя поле *transportQoS* в сообщении ARQ протокола RAS, сообщить о своей способности резервировать сетевые ресурсы. Рекомендация H.323 определяет протокол резервирования ресурсов (RSVP) как средство обеспечения гарантированного качества обслуживания, что предъявляет к терминалам требование поддержки *протокола RSVP*. К сожалению, этот протокол используется отнюдь не повсеместно, что оставляет сети H.323 без основного механизма обеспечения гарантированного качества обслуживания. Это – общая проблема сетей IP-телефонии, характерная не только для сетей H.323.

Как отмечалось в параграфе 3.2, мониторинг качества обслуживания может выполняться протоколом RTCP, однако обмен информацией RTCP происходит только между окончательными устройствами, участвующими в соединении.

3.4.2. SIP-сеть

Более популярный сегодня подход к построению сетей IP-телефонии был предложен рабочей группой IETF с музыкальным названием MMUSIC в документе RFC 2543. Положенный в его основу протокол SIP (Session Initiation Protocol) рассматривается в следующей главе книги и является частью разработанной IETF глобальной архитектуры мультимедиа. Эта архитектура включает в себя также *протокол резервирования ресурсов RSVP (Resource Reservation Protocol)*, рассмотренные выше в этой главе транспортный протокол реального времени RTP (Real-Time Transport Protocol; RFC 1889) и протокол передачи потоков в реальном времени RTSP (Real-Time Streaming Protocol; RFC 2326), рассматриваемый вместе с SIP в главе 4 *протокол описания параметров связи SDP (Session Description Protocol; RFC 2327)*, а также *протокол уведомления о связи SAP (Session Announcement Protocol)*. Сразу же подчеркнем, что функции протокола SIP не зависят ни от одного из этих протоколов.

Сообщения SIP могут переноситься как протоколом TCP, так и протоколом UDP. Подробнее об этом будет сказано в главе 4. Там же будет показано, как протокол SIP поддерживает услуги Интеллектуальной сети, такие как преобразование (мэппинг) имён, преадресация и маршрутизация [7], что существенно при использовании SIP в Softswitch сети общего пользования, где приоритетной задачей Оператора является предоставление широкого спектра телефонных услуг. Другой важной особенностью протокола SIP является поддержка мобильности пользователя, т.е. его способности получать доступ к заказанным услугам в любом месте и с любого терминала, а также способности сети идентифицировать и аутентифицировать пользователя при его перемещении из одного места в другое.

Сеть SIP содержит основные элементы трех видов: агенты пользователя, прокси-серверы и серверы преадресации. *Агенты пользователя (User Agent или SIP client)* являются приложениями терминального оборудования и включают в себя две составляющие: *агент пользователя – клиент UAC (User Agent Client)* и *агент пользователя – сервер UAS (User Agent Server)*. Клиент UAC инициирует SIP-запросы, т.е. выступает в качестве вызывающей стороны. Сервер UAS принимает запросы и передает обратно ответы, т.е. выступает в качестве вызываемой стороны. Кроме того, существует два типа сетевых серверов SIP: *прокси-серверы* (серверы-посредники) и *серверы преадресации*. Серверы SIP могут работать как

в режиме с сохранением данных о состояниях текущих соединений (statefull), так и в режиме без сохранения таких данных (stateless). Сервер SIP, функционирующий в режиме stateless, может обслужить сколь угодно большое количество пользователей, в отличие от привратника H.323, который может одновременно работать с ограниченным количеством пользователей.

3.4.3. Управление шлюзами MGCP и MEGACO

Третий подход к построению сетей IP-телефонии, основанный на использовании протокола MGCP, также предложен комитетом IETF – его рабочей группой MEGACO – и рассмотрен в главе 6 книги. При разработке этого протокола рабочая группа MEGACO опиралась на сетевую архитектуру, аналогичную рассмотренной в главах 1 и 2 содержащую следующие представленные на рис. 3.3 функциональные блоки:

- *транспортный шлюз MG (Media Gateway)*, выполняющий функции преобразования речевой информации, которая поступает от ТФОП, в вид, пригодный для передачи по сетям с маршрутизацией пакетов IP (кодирование и упаковку речевой информации в пакеты RTP/UDP/IP, а также обратное преобразование);
- *контроллер шлюзов MGC (Media Gateway Controller, Softswitch, Call Agent)*, который выполняет функции управления шлюзами,
- *шлюз сигнализации SG (Signaling Gateway)*, который обеспечивает доставку сигнальной информации, поступающей со стороны ТФОП, к контроллеру шлюзов и перенос сигнальной информации в обратном направлении.

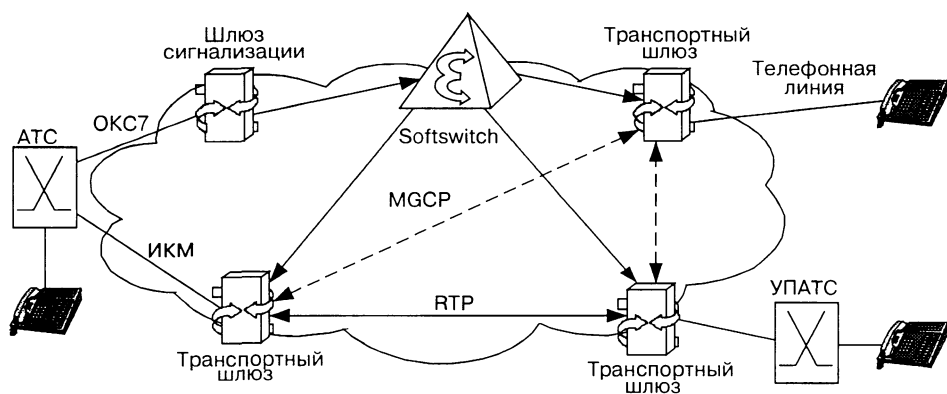


Рис. 3.3. Архитектура VoIP-сети на базе протокола MGCP

Таким образом, весь интеллект функционально распределенного шлюза сосредоточен в Softswitch (MGC, Call Agent), который, к тому же, вместе со шлюзом сигнализации, выполняет функции транзит-

ного STP или окончного SP пункта сети сигнализации ОКС7, к чему мы вернемся в следующем разделе этого параграфа.

Но перед этим, чтобы оправдать само название параграфа, рассмотрим сценарии установления и разрушения соединения с использованием протоколов MGCP и ОКС7 (рис. 3.4).

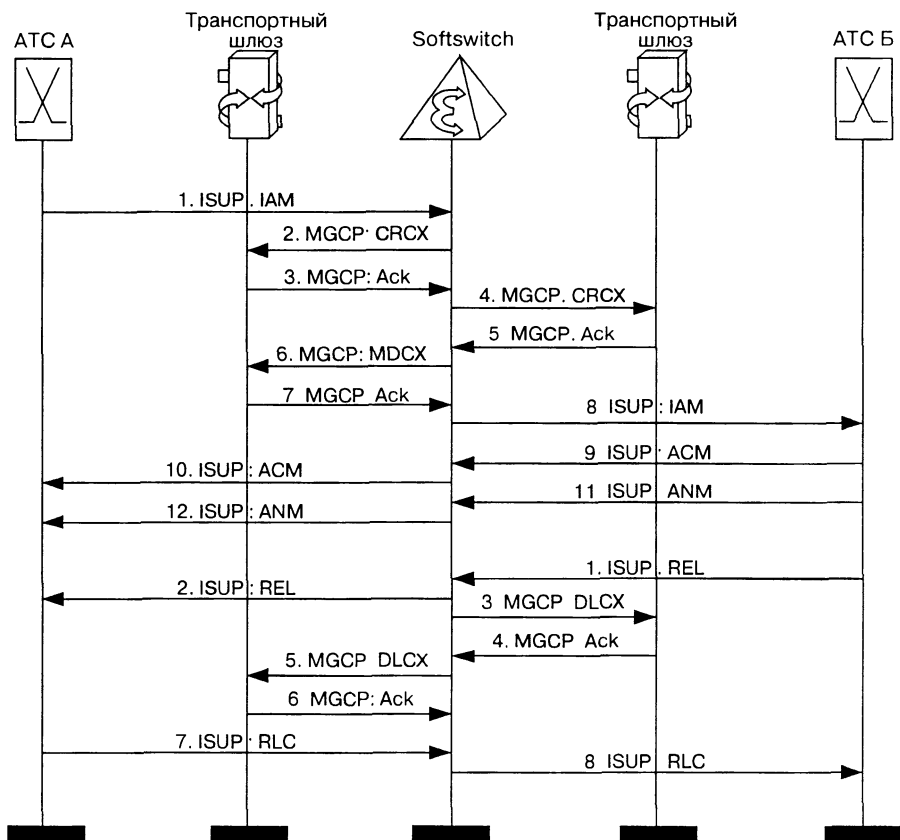


Рис. 3.4. Первый пример установления и разрушения соединения IP-телефонии

Пример на рис. 3.4 охватывает взаимодействие протокола MGCP с протоколом ОКС7. Отметим, что протокол MGCP является master/slave-протоколом, т.е. Softswitch здесь является ведущим, а шлюз – ведомым устройством, которое должно выполнять все команды, поступающие от Softswitch. Благодаря этому шлюзы не должны быть интеллектуальными устройствами, требуют меньшей производительности процессоров и, следовательно, становятся менее дорогими. Кроме того, очень быстро вводятся новые протоколы сигнализации или дополнительные услуги, так как эти изменения затрагивают только Softswitch, а не сами шлюзы.

1. От телефонной станции АТС-А к шлюзу сигнализации SG1 по общему каналу сигнализации поступает запрос соединения в виде сообщения IAM протокола ISUP [12]. Для простоты на рис. 3.4 шлюз сигнализации SG1 совмещен с транспортным шлюзом TGW1. Шлюз SG1 передает сообщение IAM к контроллеру шлюзов, который обрабатывает запрос и определяет, что вызов должен быть направлен к АТС-Б через шлюз TGW2.
2. Далее контроллер резервирует порт шлюза TGW1 (разговорный канал). С этой целью он передает к шлюзу команду CreateConnection. Отметим, что порт шлюза TGW1 может только принимать информацию (режим *recvonly*), так как он еще не осведомлен о том, по какому адресу и каким образом ему следует передавать информацию.
3. В ответе на эту команду шлюз TGW1 передает описание параметров сеанса связи.
4. Приняв ответ шлюза TGW1, контроллер передает команду CRCX второму шлюзу TGW2 с целью резервировать порт в этом шлюзе.
5. Шлюз TGW 2 выбирает порт, который будет участвовать в соединении, и подтверждает прием команды CRCX. При помощи двух команд CRCX создается односторонний разговорный канал для передачи вызываемому абоненту акустических сигналов или речевых подсказок и приглашений. В то же время, порт шлюза TGW 2 уже может не только принимать, но и передавать информацию, так как он получил описание параметров связи от встречного шлюза.
6. Далее контроллер шлюзов передает сообщение IAM к АТС-Б.
7. На сообщение IAM станция АТС-Б отвечает подтверждением ACM, которое немедленно пересылается к станции АТС-А.
8. После того как вызываемый абонент примет вызов, АТС-Б передает к контроллеру шлюзов сообщение ANM.
9. Далее контроллер заменяет в шлюзе TGW1 режим «*recvonly*» на полнодуплексный режим.
10. Шлюз TGW1 выполняет и подтверждает изменение режима.
11. Контроллер передает сообщение ANM к АТС-А, после чего начинается разговорная фаза соединения.
12. Завершение разговорной фазы происходит следующим образом. В нашем случае вызвавший абонент дает отбой первым. АТС-А передает через шлюз сигнализации сообщение REL к контроллеру шлюзов.
13. Приняв сообщение REL, контроллер шлюзов разрушает соединение с вызывавшим абонентом.

14. Шлюз подтверждает разрушение соединения и передает к контроллеру собранные за время соединения статистические данные.
15. Далее контроллер шлюзов передает сообщение RLC к АТС-А с целью подтвердить разъединение.
16. Параллельно контроллер разрушает соединение с вызванной стороной.
17. Шлюз TGW2 подтверждает разрушение соединения и передает к контроллеру собранные за время соединения статистические данные.
18. После приема ответа на команду DLCX контроллер может начинать процедуру разрушения соединения с АТС-Б, которая должна подтвердить разъединение, после чего соединение считается разрушенным.

Отметим, что в приведенном сценарии использован протокол MGCP, что обусловлено следующим. Рабочая группа MEGACO комитета IETF усовершенствовала процедуры управления шлюзами, в результате чего был разработан протокол MEGACO с более широкими, чем у MGCP, функциональными возможностями,.

Параллельно с этим Международный союз электросвязи ITU-T в версии 4 рекомендации H.323 ввел принцип декомпозиции шлюзов, согласно которому управление функциональными блоками распределенного шлюза производится контроллером шлюза MGC при помощи протокола MEGACO, который в рекомендации H.248 назван Gateway Control Protocol.

В технической литературе этот протокол обычно именуется Megaco/H.248 или просто H.248. Сообщения протокола Megaco отличаются от сообщений протокола MGCP, но процедуры установления и разрушения соединений с использованием обоих протоколов идентичны. По этой причине в этом и следующем (рис. 3.5) сценарии использован протокол MGCP, а глава 6 и приведенные в ней сценарии почти полностью посвящены Megaco/H.248.

3.4.4. Общекабельная сигнализация

Шлюз сигнализации должен принимать поступающие из ТфОП пакеты трех нижних уровней системы сигнализации ОКС7 (уровней подсистемы переноса сообщений МТП) и передавать сигнальные сообщения верхнего, пользовательского, уровня к контроллеру шлюзов. Шлюз сигнализации должен также уметь передавать по IP-сети приходящие из ТфОП сигнальные сообщения Q.931.

Для этих целей рабочая группа Sigtran комитета IETF разработала эффективный механизм передачи сигнальной информации

ОКС7 по IP-сетям, рассматриваемый в главе 7. По целому ряду причин пришлось отказаться от использования для этой цели протокола TCP, вместо которого рабочая группа Sigtran разработала *протокол транспортировки информации с управлением потоками SCTP (Stream Control Transport Protocol)*, имеющий ряд преимуществ перед TCP, основным из которых является значительное снижение времени доставки сигнальной информации и, следовательно, времени установления соединения.

В качестве продолжения сценария из предыдущего раздела на рис. 3.5 приведен второй пример, охватывающий взаимодействие протокола MGCP с протоколами ОКС7 и DSS1.

1. С телефонной станции АТС-А к шлюзу сигнализации SG1 по общему каналу сигнализации поступает запрос соединения (сообщение IAM). На рис. 3.5 шлюз сигнализации SG1 также совмещен с транспортным шлюзом TGW1. Шлюз SG1 передает сообщение IAM к контроллеру шлюзов, который обрабатывает запрос и определяет, что вызов должен быть направлен к окончному устройству вызываемого пользователя – терминалу Н.323.
2. Далее контроллер шлюзов резервирует порт шлюза TGW1 (разговорный канал). С этой целью он передает к шлюзу команду CreateConnection. И в этом примере порт шлюза TGW1 может пока только принимать информацию (режим «recvonly»).
3. В ответе на принятую команду шлюз TGW1 передает описание параметров связи.
4. Приняв ответ от шлюза TGW1, контроллер передает к привратнику сети Н.323 сообщение ARQ с alias-адресом вызываемого абонента.
5. В ответ на сообщение ARQ привратник передает сообщение ACF с указанием транспортного адреса своего сигнального канала.
6. Далее контроллер передает запрос соединения SETUP на транспортный адрес сигнального канала привратника, при этом используется процедура Fast Start. Привратник пересылает сообщение SETUP к вызываемому терминалу.
7. Вызываемый терминал передает запрос допуска к ресурсам сети ARQ.
8. В ответ на запрос ARQ привратник передает подтверждение запроса ACF.
9. Вызываемый терминал передает сообщение ALERTING, которое привратник маршрутизирует к контроллеру шлюзов. При этом вызываемому пользователю подается визуальный или акустический сигнал о входящем вызове, а вызывающему пользователю

лю подается индикация того, что вызываемый пользователь не занят и получает сигнал о вызове.

10. Контроллер преобразует сообщение ALERTING в сообщение ACM, которое немедленно пересылается к АТС-А.
11. После того как вызываемый пользователь примет входящий вызов, контроллер получит сообщение CONNECT, которое преобразуется им в сообщение ANM и передается вызывающей стороне.
12. Далее контроллер шлюзов меняет в шлюзе TGW1 режим «tesvonly» на полнодуплексный режим.
13. Шлюз TGW1 выполняет и подтверждает изменение режима соединения.
14. Контроллер передает сообщение ANM к АТС-А, после чего начинается разговорная фаза соединения, в ходе которой оборудование вызвавшего пользователя передает речевую информацию, упакованную в пакеты RTP/UDP/IP, на транспортный адрес RTP-канала терминала вызванного абонента, а тот передает пакетированную речевую информацию на транспортный адрес RTP-канала терминала вызвавшего абонента. При помощи канала RTCP ведется контроль передачи информации по RTP каналу.
15. После окончания разговорной фазы начинается фаза разрушения соединения. Оборудование пользователя, инициирующего разрушение соединения, должно прекратить передачу речевой информации, разрушить логические каналы и передать сообщение RELEASE COMPLETE, после чего сигнальный канал разрушается.
16. Контроллер шлюзов передает сообщение RLC к АТС-А с целью завершения соединения.
17. Кроме того, контроллер передает к шлюзу команду DLCX.
18. Шлюз подтверждает разрушение соединения и передает к контроллеру собранные за время соединения статистические данные.
19. После вышеописанных действий контроллер и окончное оборудование извещают привратник об освобождении занимавшейся полосы пропускания. С этой целью каждый из участников соединения передает привратнику по каналу RAS запрос выхода из соединения DRQ, на который привратник должен передать подтверждение DCF.
20. От АТС-А приходит подтверждение разъединения RLC, после чего соединение считается разрушенным.

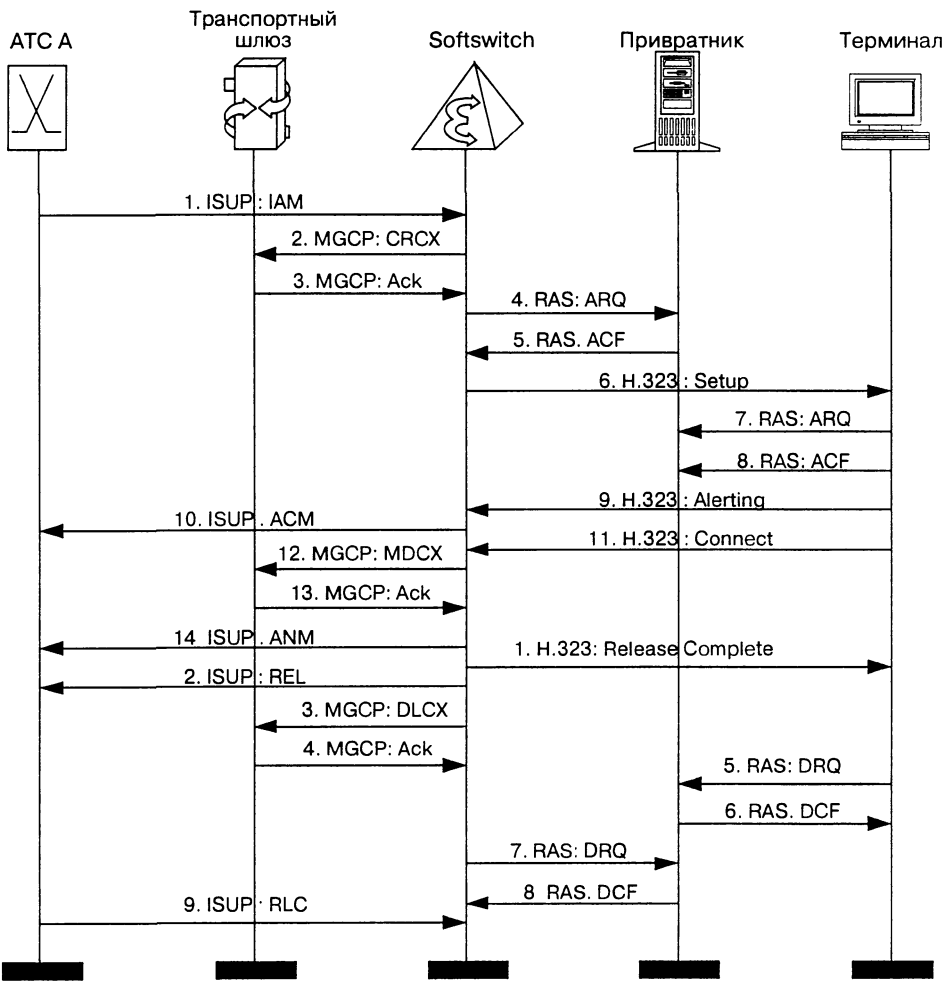


Рис. 3.5. Второй пример установления и разрыва соединения IP-телефонии

Заметим, что алгоритм взаимодействия протоколов SIP и MGCP, например, не сильно отличается от вышеописанного алгоритма.

3.5. Сравнение протоколов

Приведенных в предыдущем параграфе сведений отнюдь не достаточно для окончательных выводов относительно перспектив использования того или другого протокола IP-телефонии, хотя первое впечатление у читателя уже должно было сложиться. В следующих четырех главах авторы постараются представить более глубокие сведения о каждой из упомянутых систем сигнализации,

не навязывая при этом какой-либо одной точки зрения, а предоставляя все необходимое для того, чтобы читатель мог самостоятельно сделать надлежащие выводы. С этой же целью здесь представлена сводная табл. 3.1, содержащая краткие характеристики упомянутых выше протоколов. Практически все строки этой таблицы заслуживают отдельных пояснений, чему и посвящены главы 4 – 7 книги.

Таблица 3.1. Сравнительные характеристики протоколов, рассматриваемых в главах 4-7

Характеристики	SIP (глава 4)	H.323 (глава 5)	MGCP (глава 6)	MEGACO/ H.248 (глава 6)	ISUP (глава 7)
Назначение	Для IP-коммуникаций	Для IP-телефонии	Для управления транспортными шлюзами	Для управления транспортными шлюзами	Для сетей TDM
Архитектура	Peer-to-Peer	Peer-to-Peer	Master-Slave	Master-Slave	Peer-to-Peer
Преемственность	Не пытается воспроизвести ТфОП	Моделирует ТфОП по аналогии с Q.931 [5]	Не пытается воспроизвести ТфОП	Наследует базовые принципы MGCP	Лежит в основе ТфОП по Q.700 [4]
Стандарты	IETF-стандарт RFC	Рекомендации ITU-T	Информационный RFC	Рек. ITU-T и IETF	Рекомендации ITU-T
Версии	Разные	V1 – 1996, V2 – 1998, V3 – 1999 V4 – 2000 V5 – 2003	Единственная версия	V1 – 2000, V2 – 2002, V3 – 2005	Национальные спецификации
Интеллект	Рассредоточен по элементам сети	В ядре сети	В ядре сети	В ядре сети	В ядре сети
Сложность	Еще простой, хотя уже содержит 13 сообщений	Сложный. H.225 RAS содержит 30 сообщений, H.245–72 сообщения, H.255.0 – 13 сообщений	Простой	Простой	Сложный. Содержит 44 сообщения и 60 информационных элементов
Масштабируемость	Высокая степень масштабируемости	Масштабируемый	—	—	Масштабируемый
Передача информации	Речь, данные и видео	Речь, данные и видео	Управление передачей речи, данных	Управление передачей речи, данных	Речь и данные

Окончание табл. 3.1

Характеристики	SIP (глава 4)	H.323 (глава 5)	MGCP (глава 6)	MEGACO/ H.248 (глава 6)	ISUP (глава 7)
Описание функциональных возможностей оконечного оборудования	Использование протокола SDP для обмена данными о функциональных возможностях	Использование H.245 для обмена данными о функциональных возможностях	Использование SDP для обмена данными о функциях транспортных шлюзов	Использование SDP для обмена данными о функциях транспортных шлюзов	Обмен данными о функциональных возможностях с помощью информационных элементов ISUP
Контроль доступа	Контроль доступа поддерживается	Контроль доступа (управление полосой пропускания и ее контроль)	Контроль доступа на уровне IP	Контроль доступа на уровне IP	Контроль доступа посредством процедур перехода на аварийный режим
Качество обслуживания	Процедуры QoS поддерживаются	Поддержка дифференцированного обслуживания (согласование скорости передачи и задержки)	Контроль QoS на уровне IP	Контроль QoS на уровне IP	QoS не требуется (предоставление выделенных некоммутируемых каналов)
Адресация	Поддержка IP-адресов и имен доменов через DNS	Поддержка IP-адресов, мультитизонная, многодоменная поддержка через привратник	Цифровая адресация терминалов пользователей, поддержка IP-адресов и имен доменов для транспортных шлюзов	Цифровая адресация терминалов пользователей, поддержка IP-адресов и имен доменов для транспортных шлюзов	Адреса по Рек.ITU-T E.164, статические
Обнаружение закольцованных маршрутов	С помощью специальных заголовков	С помощью вектора пути	Не используется	Не используется	С помощью таймера, подсчета пересылок и сообщения Loop
Защита информации	Протоколы IPSec, TLS, SSL и HTTP Digest	Протоколы H.235, IPSec и TLS	Протоколы IPSec, TLS, SSL	Протоколы IPSec, TLS, SSL	Физическая защита
Кодирование	Текстовое кодирование	Двоичное кодирование ASN.1	Текстовое кодирование	Текстовое и двоичное кодирование	Двоичное кодирование

Глава 4

Протокол инициирования сеансов связи

*Поэзия – та же добыча радия:
В грамм добыча, в год труды,
Изводишь единого слова ради
Тысячи тонн словесной руды*
В.В. Маяковский

4.1. Основы протокола SIP

Рассматриваемый в этой главе протокол SIP (Session Initiation Protocol) является текст-ориентированным протоколом прикладного уровня и предназначается для организации, модификации и завершения различных сеансов связи, в том числе, мультимедийных конференций, телефонных соединений, широковещательной рассылки мультимедийной информации и соединений пользователей с разными инфокоммуникационными приложениями. С помощью SIP пользователи могут принимать участие в уже существующих сеансах связи, а также приглашать и/или быть приглашенными другими пользователями к участию во вновь создаваемом сеансе.

Тщательный отбор текстовых сообщений для весьма ограниченного словарного запаса SIP (что подчеркивает эпиграф к главе) не помешал ему занять лидирующие позиции в сетях NGN. Недавно вышел справочник по протоколу SIP [10], подробно описывающий все особенности работы SIP, поэтому в этой главе мы рассмотрим лишь общие аспекты.

Первая спецификация протокола SIP, согласно опубликованному IETF в феврале 1996 года документу *draft-ietf-mmusic-sip-00*, содержала единственный текстовый запрос. Да и далее, по мере своего развития в следующих версиях, протокол SIP, базирующийся на HTTP (*Hypertext Transport Protocol*), тоже не стал многословным: по RFC 2543, уже значительно отличающейся от первого варианта, протокол SIP предусматривает всего 6 запросов.

Несколько слов об этом первом варианте. В начале 1996 года в IETF соперничали два протокола установления сеансов связи: протокол *Session Invitation Protocol*, который предложили Марк Хэндлей и Ив Шулер, и протокол *Simple Conference Invitation Protocol (SCIP)*, предложенный Хеннингом Шульцриным.

Session Invitation Protocol обеспечивал только установление сеанса и элементарные возможности согласования сеансов связи, а когда сеанс уже начинался, этот протокол не использовался вовсе [88]. Протокол был рассчитан на работу только поверх протокола *UDP (User Datagram Protocol)* и использовал *SDP* для описания сеанса связи.

Протокол *SCIP*, с другой стороны, был основан на *TCP (Transmission Control Protocol)*. Протокол функционировал и после установления сеанса, включая процедуру завершения сеанса связи. Он использовал также существующие Интернет-протоколы *HTTP* и *SMTP (Simple Mail Transport Protocol)*, но не использовал *SDP* для описания сеансов связи.

В том же 1996 году оба этих протокола были объединены в протокол SIP – *Session Initiation Protocol*, который позаимствовал идеи у каждого из своих прародителей [89]. У *Session Invitation Protocol* протокол SIP перенял его базирование на *UDP* и использование *SDP*, а у *SCIP* протокол SIP взял совместимость с *TCP* и его близость к *SMTP* и *HTTP*. Новый протокол назвали *SIP2.0*, чтобы отличить его от схожей аббревиатуры *SIP/1.0*, которая значила *Session Invitation Protocol*. Комбинированный протокол имел много достоинств. Например, чтобы найти местоположение пользователя, он мог использовать другие имеющиеся в его распоряжении средства; он мог ретранслировать приглашение к сеансу между серверами SIP, переправлять приглашение другим серверам и мог также параллельно или последовательно разветвлять приглашение (повторять приглашение к сеансу по многим ветвям), производить согласование сеанса, поддерживать примитивы для установления и прекращения сеансов, а также запрашивать конечных пользователей об их возможностях.

Кроме использования числовых идентификаторов для представления пользователей SIP позволяет применять удобные для пользователей идентификаторы, аналогичные идентификаторам электронной почты.

Все эти достоинства и простота протокола (текстовая база, парадигма запрос-ответ) привлекали многих сторонников, как из научного мира, так и из промышленности. В марте 1999 года SIP был опубликован в качестве стандарта IETF под номером RFC 2543, а в июне 2002 года его дополнительно пересмотрели и дали ему номер RFC 3621 [114]. Момент выпуска RFC 2543 совпал с описанным в начале предыдущей главы коммерческим этапом IP-телефонии, ее выходом из исследовательских лабораторий университетов и фирм и вторжением на телекоммуникационный рынок. В такой обстановке SIP все больше начинали рассматривать как предпочтительный протокол сигнализации для установления сеансов VoIP по IP-сетям. С самого начала, по сравнению с ближайшим соперником – протоколом H.323, рассматриваемым в следующей главе [78], – у него было много преимуществ, самыми важными из которых были возможность использовать его не только для установления телефонных сеансов, но и для других услуг, таких как транспортировка текущих сообщений и уведомление о присутствии, ну и, конечно, изначальное ориентирование на Интернет. К тому же, рассматриваемая в следующем параграфе схема адресации в SIP и ее расширяемость обеспечили успех за пределами телефонии. Другие протоколы телефонной сигнализации, включая H.323, не располагают *примитивами*, которые можно использовать для реализации таких же услуг, сохраняя ту же структуру сигнализации.

На самом деле, справедливость восторжествовала с небольшим опозданием – значительная часть сетей IP-телефонии оказалась построенной не на SIP, а все плюсы и достоинства этого протокола раскрылись уже после появления SIP-T. Примерно в это же время в телекоммуникационный мир пришло понятие Softswitch и, если можно так выразиться, они нашли друг друга, и SIP-T занял лидирующее место и как протокол взаимодействия для разных Softswitch, без которых уже не представлялись сети IP-телефонии и NGN, и как протокол установления мультимедийной связи.

Вышеизложенного уже достаточно, чтобы оправдать решение авторов начать обсуждение протоколов Softswitch именно с SIP, в отличие, в частности, от написанной 5 лет тому назад книги [8], где все начиналось именно с H.323.

Помимо немногословности в основу протокола SIP были заложены следующие принципы:

- *предоставление услуг независимо от местоположения пользователя*, т.е. персональная мобильность пользователей, основанная на присвоении пользователю уникального идентификатора, который позволяет ему перемещаться в пределах сети и получать связь в любом ее месте, вне зависимости от своего местоположения, путем дистанционной регистрации в Softswitch при помощи специального сообщения REGISTER;

- *определение готовности* пользователей участвовать в сеансе связи, для чего в протоколе SIP определены рассматриваемые ниже специальные коды ответов для предоставления детальной информации о текущей готовности пользователя к связи;
- *масштабируемость сети*, построенной на базе протокола SIP;
- *интеграция* в стек протоколов Интернет, разработанных IETF для передачи мультимедийной информации и включающих в себя *протокол резервирования ресурсов RSVP (Resource ReSerVation Protocol)*, рассмотренные в предыдущей главе протокол реального времени RTP и протокол передачи потоков в реальном времени RTSP, а также протокол описания сеанса связи SDP (Session Description Protocol), рассматриваемый ниже в этой главе;
- *взаимодействие с протоколами сигнализации* H.323, MGCP, MEGACO/H.248, DSS1 и OKC7, включая возможность переносить в сигнальных сообщениях SIP не только специфический SIP-адрес, но и телефонный номер формата E.164 или любого другого формата;
- *расширяемость протокола SIP*, характеризующаяся возможностью дополнять протокол функциями поддержки новых услуг и его адаптации к работе с различными приложениями.

Еще одним важным принципом протокола SIP является его независимость от транспортных технологий. В качестве транспорта могут использоваться протоколы UDP или TCP. Протокол UDP позволяет быстрее, чем TCP, доставлять сигнальную информацию (даже с учетом повторной передачи не подтвержденных сообщений), а также вести параллельный поиск местоположения пользователей и передавать приглашения к участию в сеансе связи в режиме многоадресной рассылки. В свою очередь, протокол TCP упрощает работу с межсетевыми экранами и гарантирует надежную доставку данных. При использовании протокола TCP разные сообщения, относящиеся к одному вызову, либо могут передаваться по одному TCP-соединению, либо для каждого запроса и ответа на него может создаваться отдельное TCP-соединение. На практике обычно используется протокол UDP, который, к тому же, облегчает обработку ситуаций аварийного переключения серверов. Команды передаются на порт 5060 по умолчанию. Команды SIP могут также передаваться на любой другой порт терминала или Softswitch, если номер этого порта заранее сообщен отправителю. Вариант переноса сигнальных сообщений SIP транспортным протоколом с установлением соединения TCP обычно не практикуется. Возможен также перенос запросов и ответов протокола SIP транспортным протоколом SCTP, рассматриваемым в главе 7.

В организуемом с помощью SIP сеансе связи может передаваться мультимедийная информация любого вида: речь, видео и данные,

а также любая их комбинация, в связи с чем необходимо организовать обмен между участниками предполагаемой связи сведениями о характере передаваемой информации. Для этой цели чаще всего SIP дополняется еще одним протоколом – *описания сеанса связи SDP*, – информация которого передается в теле сообщения протокола SIP. Поскольку в течение сеанса связи может производиться его модификация (например, приглашение других пользователей к уже существующему сеансу, – в частности, к конференциям в режиме многоадресной рассылки), – предусмотрена передача сообщений SIP с новыми описаниями сеанса средствами SDP.

Для передачи речевой информации IETF предлагает использовать протокол RTP, рассмотренный в параграфе 3.2 предыдущей главы, но сам протокол SIP не исключает возможность применения для этих целей других протоколов.

Заметим, что в протоколе SIP не реализованы механизмы управления потоками информации и предоставления гарантированного качества обслуживания. Кроме того, SIP не предназначается для передачи пользовательской информации, но, в то же время, он может переносить ограниченные объемы информации в своих сообщениях.

Ранее считалось, что SIP уступает H.323 в организации мультимедийных конференций. Но по мере эволюции в SIP реализованы возможности присоединения новых участников к уже существующему сеансу связи, т.е. двусторонний сеанс связи может перейти в конференцию. В общем случае SIP предусматривает организацию конференций трех видов:

- создаваемых в режиме многоадресной рассылки (*multicasting*), когда информация передается на один multicast-адрес, а затем доставляется сетью конечным адресатам;
- создаваемых при помощи *устройства управления конференцией MCU*, к которому участники конференции передают информацию в режиме точка-точка, а MCU, в свою очередь, обрабатывает ее и рассылает участникам конференции;
- создаваемых путем соединения каждого пользователя с каждым в режиме точка-точка.

И – несколько слов об адресации в сетях SIP. Для организации взаимодействия с существующими приложениями IP-сетей и обеспечения вышеупомянутой мобильности пользователей протокол SIP использует принцип адресации, подобный электронной почте. В качестве адресов используются специальные *универсальные указатели ресурсов URL (Universal Resource Locators)*, называемые *SIP URL*.

Различаются SIP-адреса следующих типов:

- *имя@домен*,
- *имя@хост*,
- *имя@IP-адрес*,
- *№телефона@шлюз*.

SIP-адрес состоит из двух частей. Первая часть адреса – это имя пользователя, зарегистрированного в домене сети или на рабочей станции. Если вторая часть адреса идентифицирует какой-либо шлюз, то в первой указывается телефонный номер абонента.

Во второй части адреса указывается имя домена сети, хоста или шлюза. Для определения IP-адреса устройства необходимо обратиться к *службе доменных имен DNS (Domain Name Service)*. Если же во второй части SIP-адреса размещается IP-адрес, то с рабочей станцией можно связаться непосредственно.

В начале адреса ставятся ключевое слово, например *'sip:'*, указывающее, что это именно SIP URL. Существуют также другие URL (например, *'tel:'*). Ниже приводятся примеры SIP-адресов:

sip: alex@niits.ru

sip: boris@218.10.12.123

tel: +78129998877@sip-gateway.ru

Кроме того, разработан ряд методов совместной работы оборудования SIP с *преобразователями сетевых адресов NAT (Network Address Translator)*. Существует целый ряд таких решений: протокол *STUN (Simple Traversal of UDP Through NAT)*; *TURN (Traversal Using Relay NAT)*; *SIP Application Layer Gateways (ALGs)*; протокол *MIDCOM (Middlebox Communication)*; *SIP Symmetric Response Routing* по RFC 3581; *Firewall Enhancement Protocol* по RFC 3093 и др.

4.2. Архитектура сети SIP

Как уже отмечалось в предыдущем параграфе, SIP – это текстовый протокол, прародителем которого, в известном смысле, является протокол HTTP (Hypertext Transfer Protocol). Протокол SIP унаследовал от него синтаксис и архитектуру и опирается на запросы (команды), передаваемые контроллером (Softswitch), и ответы на них. В оригинальных спецификациях SIP для запросов используется термин *methods*. С того времени, когда были определены упомянутые в предыдущем параграфе шесть первоначальных запросов, были приняты еще несколько запросов, которые используются как внутри оборудования, так и в виде расширений к базовой спецификации протокола, о чем будет сказано ниже в этой главе. В такой системе существует два функциональных элемента: клиент

и сервер (рис. 4.1). Клиент передает запросы, в которых указывает, какого рода услугу он желает получить от сервера. Сервер принимает запросы, обрабатывает их и передает обратно ответ с указанием либо успешного выполнения запроса, либо ошибки, или обеспечивает предоставление услуги, затребованной клиентом.



Рис. 4.1. Архитектура «клиент-сервер»

Таким способом SIP обеспечивает управление соединением и сигнализацию, необходимые для организации мультимедийных сеансов связи, а также обеспечивает предоставление конвергентных услуг по IP-сетям. При организации и завершении мультимедийной связи SIP поддерживает:

- *определение местоположения (User location)* пользователя;
- *определение готовности (User availability)* пользователя, т.е. того, что встречная сторона готова участвовать в сеансе связи;
- *определение функциональных возможностей (User capabilities)* пользователей, т.е. того, какого рода информацией они могут обмениваться, и параметров этой информации;
- *установление сеанса связи (Session setup)*, т.е. назначение параметров сеанса связи как для вызывающей, так и для вызываемой сторон;
- *управление сеансом связи (Session management)*, включая поддержание и завершение сеанса связи, модификацию параметров сеанса и активизацию услуг.

Важно отметить, что протокол SIP является не вертикально интегрированной системой, а, скорее, компонентом, который можно использовать совместно с другими разработанными IETF протоколами Интернет, что делает его гораздо более эффективным при построении законченной мультимедийной архитектуры. Благодаря архитектуре, более эффективной, по сравнению со строительством вертикали, SIP, как правило, используется в сочетании с другими протоколами, но основное множество его функций не зависит ни от одного из этих протоколов. Проще говоря, протокол SIP не определяет услуги, но позволяет пользователям устанавливать сеансы связи и их параметры для ввода потоков пользовательской информации «в услуги» и для вывода ее «из них». SIP позволяет создавать мультимедийные конференции по упрощенному алгоритму и объединять разнородные услуги, например телефонную связь и Web-приложения, что, в частности, дает возможность пользователю, находящемуся на Web-сайте компании, связаться по те-

лефону через Интернет с менеджером этой компании и получить его консультацию. Протокол SIP устанавливает сеансы, согласует требования к передаваемой/принимаемой информации, определяет местоположение пользователей и позволяет предоставлять современные интеллектуальные услуги, такие как переадресация вызова, переключение связи, предоставление идентификационной информации, обеспечение конфиденциальности связи и интерактивные услуги мгновенного обмена сообщениями через Интернет для систем мобильной связи третьего поколения.

В спецификациях протокола SIP определены четыре основных функциональных элемента, которые, в зависимости от конкретных требований, либо могут реализоваться в виде автономных компонентов, либо совмещаться на объединенной платформе.

Агенты пользователей UA (User Agents) – терминалы SIP, которые инициируют запросы, отвечают на запросы и взаимодействуют с другими агентами пользователей для организации и завершения сеансов связи. Агенты пользователей могут взаимодействовать друг с другом непосредственно; однако часто в сеанс связи бывает вовлечен один или более промежуточных серверов: прокси-серверов или серверов переадресации. Клиентская и серверная часть программного обеспечения UA названы, соответственно, *клиентом агента пользователя UAC (User Agent Client)* и *сервером агента пользователя UAS (User Agent Server)*. Заметим, что сервер UAS и клиент UAC могут (но не обязаны), непосредственно взаимодействовать с пользователем, а другие клиенты и серверы SIP этого делать не могут. UAC и UAS могут быть реализованы как непосредственно в терминале пользователя, так и в программном обеспечении универсальных устройств доступа, например, мультисервисных абонентских концентраторов.

Прокси-серверы (Proxy Servers) получили свое название от английского проху – «представитель» и обеспечивают обработку запросов, поступающих от терминалов пользователей, с целью предоставления услуг связи. Порядок обработки запроса и дальнейшие действия прокси-сервера зависят от типа запроса. Это может быть поиск и вызов пользователя, маршрутизация запроса, предоставление услуги и т.д. Как и агент пользователя, прокси-сервер тоже состоит из клиентской и серверной частей, поэтому он может принимать вызовы, инициировать собственные запросы и передавать ответы на запросы. Прокси-сервер может быть реализован совместно с сервером определения местоположения, рассматриваемым ниже, или помещаться отдельно от него, но иметь возможность связываться с ним по LDAP согласно RFC 1777 или по любому другому протоколу. Предусматривается два типа прокси-серверов: с сохранением данных о состояниях *stateful* и без сохранения данных о состояниях *stateless*. Сервер первого типа хранит в памяти ис-

торию процесса обслуживания вызова, в частности, первый поступивший запрос, который является причиной генерации одного или нескольких исходящих запросов, также запоминаемых сервером. Все запросы хранятся в памяти сервера только до окончания транзакции, т.е. до получения соответствующих ответов. Сервер *stateful* позволяет предоставить большее количество услуг и допускает применение упрощенных терминалов пользователей, но требует значительной вычислительной мощности. Прокси-сервер должен работать в режиме *stateful* при использовании для передачи сигнальной информации протокола TCP, при работе в режиме многоадресной рассылки сигнальной информации, или при множественной рассылке запросов, когда один запрос, поступивший на прокси-сервер, передается одновременно по нескольким направлениям. Сервер *stateless* лишь ретранслирует запросы и ответы, которые принимает. Он требует менее быстросуществующей платформы, т.к. ее производительность не тратится на контроль состояний текущих процессов обслуживания вызовов, вследствие чего сервер может обслужить большее количество пользователей. Недостатком такого режима является то, что он позволяет реализовать лишь наиболее простые услуги. Впрочем, прокси-сервер может для одних вызовов функционировать с сохранением данных о состояниях, а для других – без сохранения, но во всех случаях выполняет свои основные функции: – пересылает сообщения к агентам пользователей и предоставляет такие функции, как определение местоположения пользователей, авторизация и учет пользователей. В рассматриваемой в главе 2 эталонной архитектуре IPCC им соответствуют функция маршрутизации и функция учета;

Серверы перенаправления (*Redirect servers*) всегда являются серверами без сохранения данных о состояниях. Сервер перенаправления предназначен для определения текущего IP-адреса терминала вызываемого пользователя. Вызывающий пользователь посылает на сервер сообщение с известным ему адресом вызываемого пользователя, а прокси-сервер перенаправляет вызов на текущий адрес пользователя. Для реализации этой функции сервер перенаправления должен взаимодействовать с сервером определения местоположения. Сервер перенаправления не завершает обслуживание вызовов и не иницирует свои собственные запросы. Он только сообщает адрес вызываемого пользователя или прокси-сервера, и уже по этому адресу инициатор запроса передает новый запрос. Сервер перенаправления не содержит клиентскую часть программного обеспечения. Однако пользователю не обязательно связываться с каким-либо SIP-сервером, он может вызвать другого пользователя непосредственно, но при условии, что знает его точный адрес. Сценарий установления соединения в этом случае будет выглядеть следующим образом: сначала клиент получает от сервера перенаправления адрес вызываемого UA, а затем связывается прямо с ним.

Серверы регистрации местоположения пользователей (**Registrars или Location servers**) позволяют агентам регистрировать свое местоположение, реализуя тем самым услуги мобильности с помощью протокола SIP. О своем местоположении пользователь сообщает специальному серверу с помощью сообщения REGISTER. Возможны два режима регистрации пользователя: он может передать свой новый адрес один раз, а может регистрироваться периодически через определенные промежутки времени. Первый способ подходит для случая, когда терминал включен постоянно, и его пользователь не перемещается по сети, а второй – если терминал пользователя часто перемещается или выключается. Фактически *сервер регистрации местоположения* пользователя представляет собой базу адресной информации. Кроме постоянного адреса пользователя в базе данных указывается один или несколько текущих адресов. Как уже отмечалось, этот сервер может быть реализован совместно с прокси-сервером, в этом случае он называется *registrar*, или отдельно – тогда его называют *location server*, – но с возможностью связываться с прокси. В спецификациях протокола SIP сервер регистрации местоположения представлен как отдельный сетевой элемент, однако принципы его работы не регламентированы.

Резюмируя все вышесказанное, отметим, что в сети SIP присутствуют следующие основные элементы: терминалы, прокси-серверы и серверы перенаправления.

4.3. Структура сообщений

Согласно рассмотренной в предыдущем параграфе архитектуре «клиент-сервер» все сообщения SIP делятся на запросы клиента серверу и ответы сервера клиенту. Так, для инициирования установления соединения вызывающий пользователь должен сообщить серверу ряд обязательных параметров, в том числе, параметры информационных каналов, адрес вызываемого пользователя и другую информацию. Указанные параметры передаются в соответствующем SIP-запросе. От вызываемого пользователя приходит ответ на запрос, также содержащий ряд параметров. Все сообщения протокола SIP – запросы и ответы – представляют собой последовательности текстовых строк, структура и синтаксис которых, как уже упоминалось ранее, соответствуют протоколу HTTP. На рис. 4.2 представлена структура сообщения протокола SIP.

Стартовая строка представляет собой начальную строку любого SIP-сообщения. Если сообщение является запросом, то в стартовой строке указываются *тип запроса*, *текущий узел-адресат* и *номер версии протокола*. Если сообщение является ответом на запрос, то в стартовой строке указываются *номер версии протокола*, *тип ответа* и *короткая расшифровка ответа*, предназначенная

только для обслуживающего персонала и не обрабатываемая клиентом.

Заголовки сообщений несут информацию об отправителе, адресате, пути следования и др., в общем, переносят информацию, необходимую для обслуживания сообщения. В протоколе SIP определено четыре вида заголовков:

- **общие заголовки**, присутствующие в запросах и ответах, к которым относятся, в частности, Call-ID (идентификатор соединения), Contact (контакт), CSeq (порядковый номер запроса/ответа), Date (дата), Encryption (кодирование), From (источник запроса), To (адресат), Via (через), Record-Route (запись маршрута);
- **заголовки содержания** переносят информацию о размере тела сообщения или об источнике запроса, начинаются со слова '**Content**', например, Content-Encoding (кодирование тела сообщения), Content-Length (размер тела сообщения), Content-Type, (тип содержимого);
- **заголовки**, передающие дополнительную информацию о запросе, например, Accept (принимается), Accept-Encoding (кодирование принимается), Accept-Language (язык поддерживается), Authorization (авторизация), Hide (скрыть), Max-Forwards (максимальное количество переадресаций), Organization (организация), Priority (приоритет), Proxy-Authorization (авторизация прокси-сервера), Proxy-Require (требование прокси-сервера), Route (маршрут), Response-Key (ключ кодирования ответа), Subject (тема), User-Agent (агент пользователя);
- **заголовки ответов**, передающие дополнительную информацию об ответе, например Allow (разрешение), Proxy-Authenticate (подтверждение подлинности прокси-сервера), Retry-After (повторить через некоторое время), Server (сервер), Unsupported (не поддерживается), Warning (предупреждение), WWW-Authenticate (аутентификация WWW-сервера).

Заголовок состоит из названия, за которым следует отделенное двоеточием значение заголовка. В поле значения содержатся передаваемые данные. Если сервер принимает сообщения, заголовки которых ему не известны, то они игнорируются при обработке. Поясним некоторые из упомянутых выше, наиболее часто используемых заголовков.

Заголовок **Call-ID** – уникальный идентификатор сеанса связи; он подобен метке соединения *Call reference* в сигнализации DSS1 [5].



Рис. 4.2. Структура сообщения протокола SIP

Значение идентификатору присваивается стороной, инициирующей вызов. Заголовок **Call-ID** состоит из буквенно-числового значения и имени рабочей станции, которая присвоила значение этому идентификатору. Между ними должен стоять символ @, например, *2345call@niits.ru*.

Заголовок **To** – определяет адресата. Кроме SIP-адреса, здесь может стоять параметр tag для идентификации определенного терминала пользователя, например, домашнего, рабочего или мобильного телефона, в том случае, когда все они зарегистрированы под одним адресом SIP URL. Запрос может множиться и достигать разных терминалов одного пользователя; чтобы их различить и нужна метка tag. Если необходим визуальный вывод имени пользователя, например, на дисплей, то имя пользователя также размещается в поле **To**.

Заголовок **From** – идентифицирует отправителя запроса; по структуре он аналогичен полю To.

Заголовок **CSeq** — уникальный идентификатор запроса, относящегося к одному соединению. Он служит для корреляции запроса с ответом на него. Заголовок состоит из двух частей: натурального числа в диапазоне от 1 до 2^{32} и типа запроса. Сервер должен проверять значение величины **CSeq** в каждом принимаемом запросе, и считает его новым, если значение больше предыдущего. Пример заголовка CSeq: 2 INVITE.

Заголовок **Via** необходим, чтобы избежать закливания запроса, а также в тех случаях, когда требуется, чтобы запросы и ответы обязательно проходили по одному и тому же пути (например, при использовании *межсетевого экрана firewall*). Дело в том, что запрос может проходить через несколько прокси-серверов, каждый из которых принимает, обрабатывает и переправляет запрос к следующему прокси-серверу, пока этот запрос не достигнет адресата.

В заголовке **Via** указывается весь путь, пройденный запросом: каждый прокси-сервер добавляет поле со своим адресом. При необходимости (в частности, чтобы обеспечить секретность) действительный адрес может скрываться. Например, пусть запрос на своем пути обрабатывался двумя прокси-серверами: сначала сервером niits.ru, потом sip.telecom.com. Тогда в запросе появятся следующие поля: *Via: SIP/2.0/UDP sip.telecom.com:5060;branch=721e418c4.1* и *Via: SIP/2.0/UDP niits.ru:5060*, где параметр *branch* означает, что на сервере sip.telecom.com запрос был размножен и направлен одновременно по разным направлениям, и наш запрос был передан по направлению, которое идентифицируется 721e418c4.1. Содержимое полей *Via* копируется из запросов в ответы на них, и каждый сервер, через который проходит ответ, удаляет поле со своим именем.

В заголовок **Record-route** прокси-сервер вписывает свой адрес – SIP URL, – если хочет, чтобы следующие запросы прошли через него.

Сообщения протокола SIP могут содержать так называемое **тело сообщения**. Некоторые запросы, например, запрос BYE, не содержат тела сообщения. С ответами дело обстоит иначе: тело сообщения могут содержать любые ответы, но содержимое их тела довольно сильно различается.

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

Заголовок **Content-Length** показывает размер тела сообщения.

4.4. Команды (запросы)

Запросы (команды) SIP или, как их называют в спецификациях, *SIP-методы (methods)*, предназначены для выполнения широкого круга задач при предоставлении базовых и дополнительных услуг связи в стационарных сетях и в сетях подвижной связи. С помощью запросов клиент сообщает о своем текущем местоположении, приглашает пользователей принять участие в сеансах связи, модифицирует уже установленные сеансы, завершает их и т.д. Сервер определяет тип принятого запроса по названию, указанному в стартовой строке. В этой же строке в поле **Request-URI** указан SIP-адрес оборудования, которому этот запрос адресован. Содержание полей **To** и **Request-URI** может быть различным, например, в поле **To** указан адрес абонента, а в **Request-URI** – адрес прокси-сервера, через который проходит запрос.

Команда **INVITE** приглашает пользователя принять участие в сеансе связи и обычно содержит описание сеанса связи, вид принимаемой информации и параметры (список возможных вариантов параметров), необходимые для приема информации. В нем может также указываться вид информации, которую вызывающий пользователь желает передавать, и данные, необходимые для аутентификации абонента. В случае необходимости изменения характеристик подготовленных или уже используемых каналов передается запрос INVITE с новым описанием сеанса связи. Для приглашения нового участника к уже установленному соединению также используется сообщение INVITE.

Команда **ACK** подтверждает прием ответа на команду INVITE, содержит описание сеанса связи, переданное вызывающим пользователем и используется только совместно с запросом INVITE, т.е. этим сообщением оборудование вызывающего пользователя показывает, что на свой запрос INVITE оно получило окончательный ответ.

Команда **CANCEL** отменяет обработку ранее переданных запросов с такими же, как и в команде CANCEL значениями полей Call-ID, To, From и CSeq, но не влияет на те запросы, обработка которых уже завершена. Например, команда CANCEL применяется тогда, когда прокси-сервер размножает запросы для поиска пользователей по нескольким направлениям и по одному из них его находит. Тогда обработку запросов, разосланных по всем остальным направлениям, сервер отменяет при помощи команды CANCEL.

Командой **BYE** оборудование вызываемого или вызывающего пользователей разрушает соединение. Сторона, получившая запрос BYE, должна прекратить передачу речевой (мультимедийной) информации и подтвердить это ответом **200 OK**.

При помощи команды **REGISTER** пользователи сообщают свое текущее местоположение. В этом сообщении содержатся поле **To** с адресом, который надо сохранить или модифицировать на сервере, поле **From** с адресом инициатора регистрации (зарегистрировать пользователя может другое лицо, например, секретарь может зарегистрировать своего начальника), поле **Contact** с новым адресом пользователя, по которому должны передаваться все дальнейшие запросы INVITE (если в команде поле **Contact** отсутствует, регистрация остается неизменной, а в случае отмены регистрации здесь размещается символ «*»), и поле **Expires**, в котором указывается время в секундах, по истечении которого регистрация заканчивается (если это поле отсутствует, то по умолчанию назначается время – 1 час). Регистрацию можно отменить и передачей сообщения REGISTER с полем Expires, которому присвоено значение 0, и с соответствующим полем Contact.

Командой **OPTIONS** вызывающий пользователь запрашивает информацию о возможностях терминального оборудования вызываемого пользователя. В ответ на этот запрос оборудование вызываемого пользователя сообщает требуемую информацию. Применение команды связано с теми случаями, когда существует необходимость узнать о возможностях оборудования до установления соединения.

После испытания протокола SIP в реальных сетях оказалось, что для решения ряда задач вышеуказанных шести запросов недостаточно. Так, не был предусмотрен способ передачи информации управления соединением или другой информации во время разговорного сеанса.

Для решения этой задачи был предложен новый запрос **INFO**, который можно использовать для переноса между шлюзами сигнальных сообщений в течение сеанса связи, для переноса сигналов DTMF, созданных в ходе сеанса, для переноса информации об остатке на счете (биллинговой информации), для переноса между

участниками сеанса связи изображений и другой не потоковой информации. Запрос **INFO** не изменяет состояния процесса обработки SIP-вызовов, как не изменяет и состояния сеансов связи, инициированных при помощи протокола SIP. Однако он обеспечивает перенос дополнительной информации прикладного уровня, которая может способствовать в дальнейшем более производительному функционированию приложений, использующих протокол SIP для доставки информации.

Объекты сети SIP могут подписаться на предоставление информации о состоянии определенного ресурса или процесса обслуживания вызова в сети при помощи сообщения **SUBSCRIBE**. Объекты, располагающие этими сведениями (или объекты, действующие от их лица), будут передавать уведомления **NOTIFY** каждый раз, когда состояние изменится.

Запрос типа **MESSAGE** предназначен для реализации служб интерактивного обмена текстовыми сообщениями с использованием модели, аналогичной отправке SMS. Запрос **REFER**, передаваемый отправителем, предписывает получателю связаться с третьей стороной, используя контактную информацию, которая содержится в этом сообщении. Такой механизм может быть использован для многих целей, например, для переадресации вызова Call Transfer.

4.5. Ответы

После приема и интерпретации запроса, адресат (прокси-сервер) передает ответ на полученный запрос. Назначение ответов бывает разным, в том числе: подтверждение установления соединения, передача запрашиваемой информации, сообщение о неисправностях и т.д. Структуру и виды ответов протокол SIP унаследовал от протокола HTTP. Определено шесть типов ответов, которые несут разную функциональную нагрузку. Тип ответа кодируется трехзначным числом. Самой важной является первая цифра, она определяет класс ответа, остальные две цифры лишь дополняют первую. В некоторых случаях оборудованию даже необязательно знать все коды ответов, но интерпретировать первую цифру ответа оно должно обязательно.

Протокол SIP определяет два типа ответов на запрос, инициирующий соединение: предварительные и окончательные. *Окончательные ответы* несут результат обработки запроса и передаются «надежно», т.е. с подтверждением. *Предварительные ответы* несут информацию о текущей стадии обработки запроса, но передаются без подтверждения.

Однако в некоторых случаях, включая взаимодействие с ТфОП, необходим механизм, обеспечивающий надёжность передачи

предварительных ответов. Для этого вводится механизм надёжности по схеме, схожей с существующими механизмами для окончательных ответов класса 2xx на запрос INVITE. Используется запрос **PRACK**, который играет ту же роль, что и ACK, но для предварительных ответов. Однако здесь имеется принципиальное различие – PRACK является обычным SIP-сообщением и требует при его получении передачи ответа 200 (OK).

Возникают случаи, когда необходимо изменить некоторые параметры сеанса (например, тип кодека) до прихода окончательного ответа на начальное сообщение INVITE, для чего вводится запрос UPDATE. Он используется следующим образом: вызывающая сторона передает сообщение INVITE, в поле заголовка Allow которого, среди запросов прочих типов, помещается **UPDATE** для того, чтобы указать на способность вызывающей стороны принимать запросы этого типа. Любой ответ (предварительный или окончательный) вызываемой стороны тоже содержит заголовок Allow с указанным в нем значением UPDATE. Далее вызывающая сторона может создать запрос UPDATE, который содержит предложение с описанием сеанса связи в формате SDP для обновления параметров сеанса. На этот запрос передается ответ с указанием принятых параметров (также в формате SDP).

Итак, ответы делятся на *предварительные (информационные)* и *окончательные*. Информационные ответы показывают, что запрос находится в стадии обработки, и кодируются трехзначным числом, начинающимся с единицы **1xx (provisional)**. Некоторые ответы, например, **100 Trying**, предназначены для обнуления таймеров в оборудовании пользователя. Если до срабатывания таймера ответ на запрос не получен, считается, что запрос потерян, и может (по усмотрению изготовителя) производиться его повторная передача. Этот информационный ответ аналогичен сообщению CALL PROCEEDING протокола Q.931.

Еще один распространенный ответ **180 Ringing**; его назначение идентично назначению сигнала «Контроль посылки вызова» в ТфОП или сообщению ALERTING протокола Q.931. Если прокси-сервер передает ответ **181 Call Forwarding**, он может также указать в теле сообщения, к какому пользователю он переправляет вызов. Ответ **182 Queued for Service** используется в приложениях, которые позволяют ставить текущий вызов в очередь для ожидания, пока не будут обслужены вызовы, находящиеся перед ним. Основными пользователями этой возможности являются отделы обслуживания клиентов в крупных корпорациях. Ответ **183 Session Progress** аналогичен сообщению CALL PROGRESS протокола Q.931 и используется для того, чтобы заранее получить описание сеанса информационного обмена от шлюзов на пути к вызываемому пользователю таким образом, чтобы мог быть проключен ранний речевой тракт

еще до того, как вызывающий пользователь получит сигнал КПВ. Этот ответ используется, например, при взаимодействии протокола SIP с сетью ТфОП, при котором передача ответа Session Progress с SDP-описанием шлюза ТфОП позволяет входящей АТС послать сигнал КПВ.

Среди других вариантов использования этого ответа – воспроизведение приветственного объявления или музыкальной фразы при входе в домен перед установлением соединения. Ответ **189** на запрос **REFER** используется для предоставления текущей информации о состоянии соединения, переключаемого на другой номер в фазе разговора. При этом ожидается получить либо ответ об успешной обработке, либо ответ об отказе вызываемой стороны. Окончательные ответы кодируются трехзначными числами, начинающимися с цифр 2, 3, 4, 5 и 6. Все они означают завершение обработки запроса, а каждый из них в отдельности – результат обработки запроса.

Ответы **2xx (success)** означают, что запрос был успешно обработан. Базовым ответом данной группы является сообщение **200 OK**. Значение этого ответа зависит от соответствующего запроса, например: ответ 200 OK на запрос INVITE означает, что вызываемый пользователь согласен принять участие в сеансе связи, а в теле ответа указываются возможности оборудования вызываемого пользователя; ответ 200 OK на запрос BYE означает завершение связи, а в теле ответа никакой информации не переносится; ответ 200 OK на запрос CANCEL означает отмену поиска, и в теле ответа тоже не переносится никакой информации; ответ 200 OK на запрос REGISTER означает, что регистрация прошла успешно; ответ 200 OK на запрос OPTION означает согласие вызываемого пользователя сообщить возможности своего оборудования, сведения о которых и содержатся в теле ответа.

Ответы **3xx (redirection)** информируют оборудование вызывающего пользователя о новом местоположении вызываемого пользователя или переносят другую информацию, которая может быть использована, чтобы с ним связаться. В ответе **300 Multiple Choices** указывается несколько SIP-адресов, по которым можно найти вызываемого пользователя, а вызывающему пользователю предлагается выбрать один из них. Ответ **301 Moved Permanently** означает, что вызываемый пользователь больше не находится по адресу, указанному в запросе, и направлять запросы нужно на адрес, указанный в поле Contact. Ответ **302 Moved Temporarily** означает, что пользователь временно (промежуток времени может быть указан в поле Expires) находится по другому адресу, указанному в поле Contact, и все запросы нужно посылать туда.

Ответы **4xx (client error)** информируют о том, что в запросе обнаружена ошибка. После получения такого ответа пользователь не должен передавать тот же самый запрос без его модификации. Ответ **400 Bad Request** означает, что запрос не понят из-за синтаксических ошибок в нем. Ответ **401 Unauthorized** означает, что запрос требует проведения процедуры аутентификации пользователя. Существуют разные варианты аутентификации, и в ответе может быть указано, какой из них использовать в данном случае. Ответ **403 Forbidden** означает, что сервер понял запрос, но отказался его обслуживать. Повторный запрос посылать не следует. Причины могут быть разными, например, запросы с этого номера не обслуживаются и т.д. Непосредственно из HTTP заимствован ответ **404 Not Found**. А ответ **485 Ambiguous** означает, что адрес вызываемого пользователя не однозначен. Ответ **486 Busy Here** означает, что вызываемый пользователь в настоящий момент занят и не желает (не может) принять входящий вызов.

Ответы **5xx (server error)** информируют о том, что запрос не может быть обработан из-за ошибки сервера. Ответ **500 Server Internal Error** означает, что сервер не имеет возможности обслужить запрос из-за внутренней ошибки. Клиент может попытаться повторно послать запрос через некоторое время. Ответ **501 Not Implemented** означает, что в сервере не реализованы какие-либо функции, необходимые для обслуживания запроса. Ответ передается в том случае, когда сервер не может распознать тип запроса, полученного им от любого из пользователей. Ответ **502 Bad Gateway** информирует о том, что сервер, функционирующий в качестве шлюза или прокси-сервера, принимает некорректный ответ от сервера, к которому он направил запрос. Ответ **503 Service Unavailable** указывает, что сервер не может в данный момент обслужить вызов вследствие перегрузки или проведения технического обслуживания.

Ответы **6xx (global failure)** информируют о том, что соединение с вызываемым пользователем установить невозможно. Ответ **600 Busy Everywhere** сообщает, что вызываемый пользователь занят и не желает принимать вызов в данный момент. Ответ может содержать указание на время, подходящее для его вызова. Если с пользователем можно связаться по другому адресу или, к примеру, оставить сообщение на речевой почтовый ящик, то используется ответ 486 Busy Here. Ответ **603 Decline** означает, что вызываемый пользователь не желает принимать входящие вызовы, не указывая причину отказа. Ответ **604 Does Not Exist Anywhere** означает, что вызываемого пользователя не существует.

Запросы и ответы на них образуют SIP-транзакцию. Она происходит между клиентом и сервером и включает в себя все сообщения, начиная с первого запроса и заканчивая окончательным ответом.

После того как мы рассмотрели запросы и разные ответы на них, видно, что протокол SIP предусматривает различные алгоритмы установления соединения.

4.6. Сценарии сеансов связи

Протоколом SIP предусмотрено 3 основных типа сценариев установления соединения: с участием прокси-сервера, с участием сервера перенаправления и непосредственно между пользователями.

Различие между этими сценариями заключается в процедуре поиска и приглашения вызываемого пользователя. В первом случае эти функции возлагает на себя прокси-сервер, а вызывающему пользователю необходимо знать только постоянный SIP-адрес вызываемого пользователя. Во втором случае вызывающая сторона самостоятельно устанавливает соединение, а сервер перенаправления вызова лишь преобразует постоянный адрес вызываемого абонента в его текущий адрес. И, наконец, в третьем случае вызывающему пользователю для установления соединения необходимо знать текущий адрес вызываемого пользователя.

Перечисленные сценарии являются базовыми. Прежде чем вызов достигнет адресата, он может пройти через несколько прокси-серверов или сначала попасть на сервер перенаправления, а затем пройти через один или несколько прокси-серверов. Кроме того, прокси-серверы могут размножать запросы и передавать их по разным направлениям и т.д.

4.6.1. Алгоритм установления соединения с участием сервера перенаправления

В этом разделе описан алгоритм установления соединения с участием сервера перенаправления вызовов. Администратор сети сообщает пользователям адрес сервера перенаправления. Вызывающий пользователь передает запрос INVITE (1) на известный ему адрес сервера перенаправления и порт 5060, используемый по умолчанию (рис. 4.3), и указывает в запросе адрес вызываемого пользователя. Сервер перенаправления запрашивает текущий адрес вызываемого абонента у сервера определения местоположения (2), который сообщает ему требуемый адрес (3). Сервер перенаправления в ответе 302 Moved Temporarily передает вызывающей стороне текущий адрес вызываемого абонента (4) или может сообщить список зарегистрированных адресов вызываемого пользователя и предложить вызывающему пользователю самому выбрать адрес. Вызываемая сторона подтверждает прием ответа 302 передачей сообщения ACK (5).

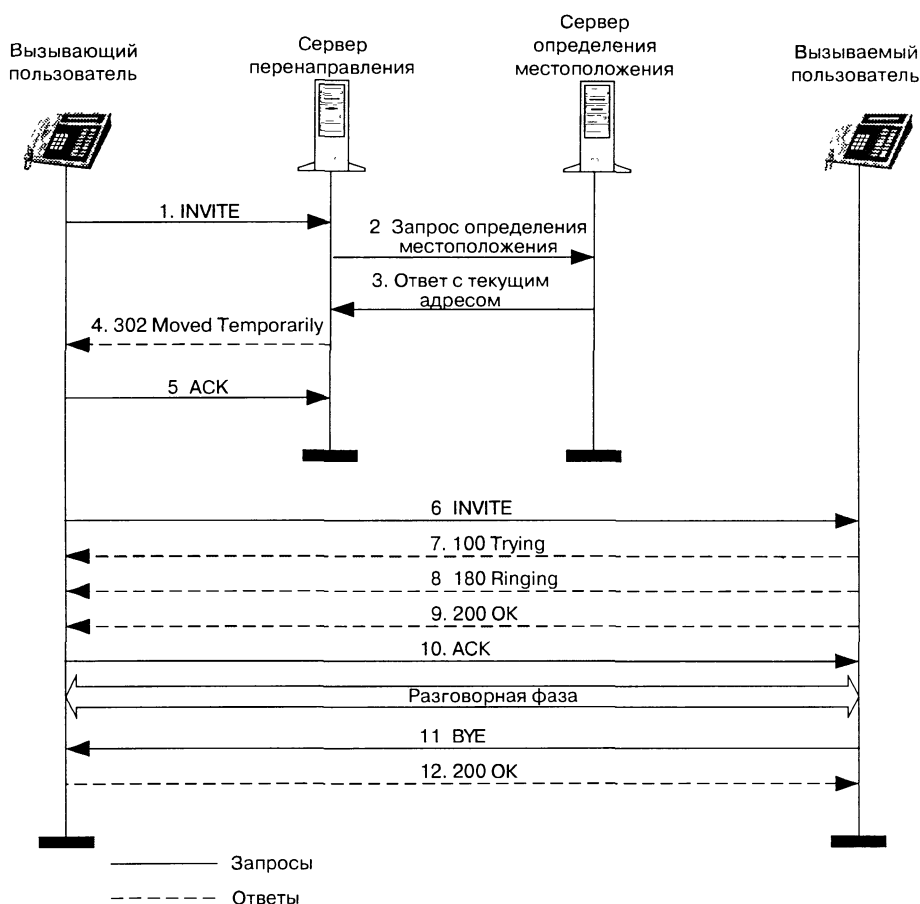


Рис. 4.3. Сценарий установления соединения через сервер перенаправления

Теперь вызывающая сторона может связаться непосредственно с вызываемой стороной. Для этого она передает новый запрос INVITE (6) с тем же идентификатором Call-ID, но с другим номером CSeq. В теле сообщения INVITE указываются возможности вызывающей стороны в формате протокола SDP. Вызываемая сторона принимает запрос INVITE и начинает его обработку, о чем сообщает ответом 100 Trying (7) встречному оборудованию для рестарта его таймеров.

После завершения обработки поступившего запроса оборудование вызываемого пользователя сообщает своему пользователю о поступлении входящего вызова, а встречной стороне передает ответ 180 Ringing (8).

После приема вызываемым пользователем входящего вызова удаленной стороне передается сообщение 200 OK (9), в котором содержится описание возможностей вызываемого терминала в формате протокола SDP. Терминал вызывающего пользователя подтверждает прием ответа запросом ACK (10). На этом фаза установления соединения закончена, и начинается разговорная фаза.

По завершении разговорной фазы передается запрос BYE (11), который подтверждается ответом 200 OK (12).

4.6.2. Алгоритм установления соединения с участием прокси-сервера

Теперь рассмотрим алгоритм установления соединения с участием прокси-сервера. Администратор сети сообщает пользователям адрес прокси-сервера. Вызывающий пользователь передает запрос INVITE (1) на адрес прокси-сервера и порт 5060, используемый по умолчанию (рис. 4.4).

В запросе он указывает известный ему адрес вызываемого пользователя. Прокси-сервер запрашивает текущий адрес вызываемого абонента у сервера определения местоположения (2), который и сообщает ему требуемый адрес (3). Далее прокси-сервер передает запрос INVITE непосредственно вызываемому абоненту (4). Опять в запросе указываются возможности терминала, но при этом в запрос добавляется поле **Via** с адресом прокси-сервера для того, чтобы ответы на обратном пути шли через него. После получения запроса и его обработки оборудование вызываемого пользователя сообщает ему о том, что поступил входящий вызов, а встречной стороне передает ответ 180 Ringing (5), копируя в него из запроса поля **To**, **From**, **Call-ID**, **CSeq** и **Via**.

После приема вызываемым пользователем входящего вызова удаленной стороне передается сообщение 200 OK (9), в котором содержится описание в формате протокола SDP возможностей вызываемого терминала. Терминал вызывающего пользователя подтверждает прием ответа запросом ACK (10). На этом фаза установления соединения закончена, и начинается разговорная фаза. По завершении разговорной фазы передается запрос BYE (11), который подтверждается ответом 200 OK (12). Все сообщения проходят через прокси-сервер, который может модифицировать некоторые поля сообщений.

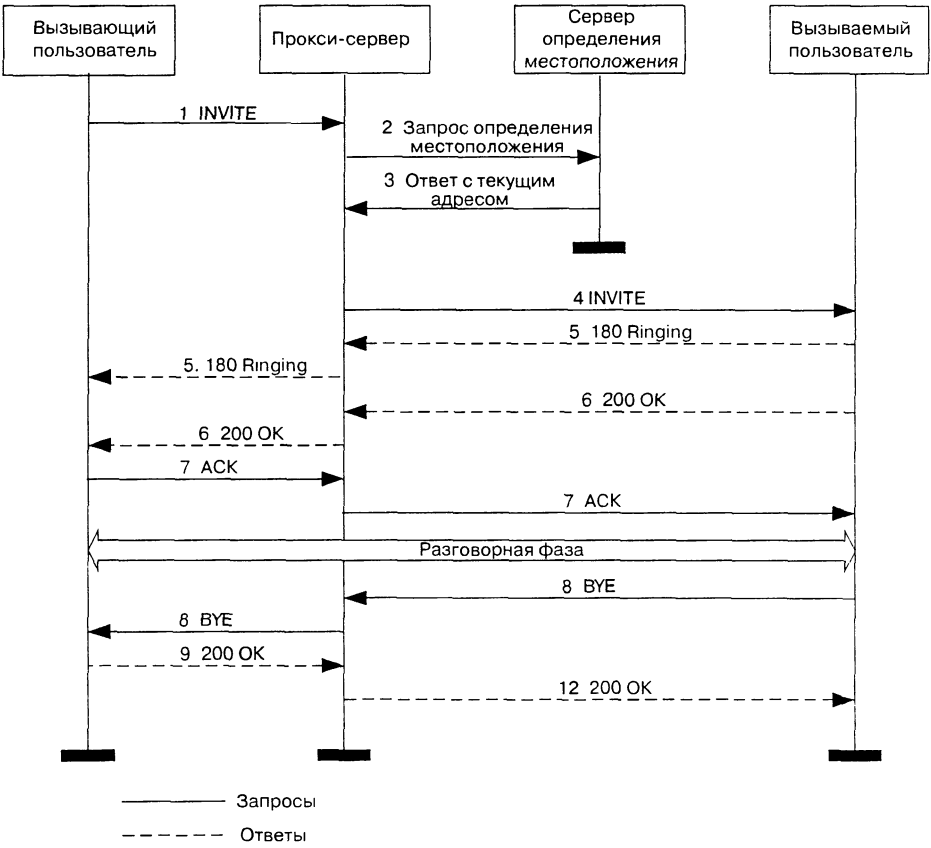


Рис. 4.4. Сценарий установления соединения через прокси-сервер

4.7. Дополнительные услуги

В этом параграфе рассматриваются примеры реализации на базе протокола SIP некоторых простых дополнительных услуг. Дополнительная услуга **Переключение связи** позволяет пользователю переключить уже установленную с ним связь к третьей стороне. На рис. 4.5 приведен пример реализации этой услуги. Пользователь В устанавливает связь с пользователем А, далее пользователь А производит переключение этой связи к пользователю С.

Дополнительная услуга **Переадресация вызова** позволяет сделать так, чтобы все входящие к пользователю вызовы направлялись на другой адрес. Основные варианты переадресации: при занятости пользователя, в случае отсутствия ответа или безусловная переадресация. Услуга реализуется с помощью заголовка **Also**, который интерпретируется следующим образом: терминал,

получивший запрос **INVITE** с таким заголовком, посылает новый вызов по адресу, указанному в поле **Also**.

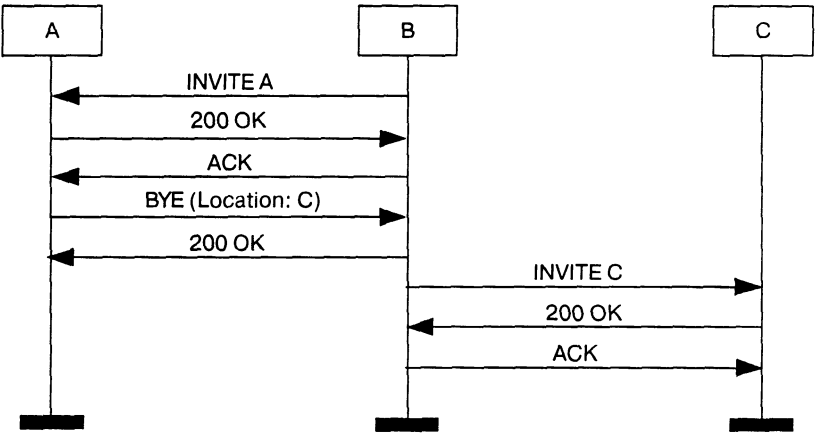


Рис. 4.5. Дополнительная услуга «Переключение связи»

В нашем случае пользователь А вызывает пользователя В, а последний переадресует вызов к пользователю С, как это показано на рис. 4.6.

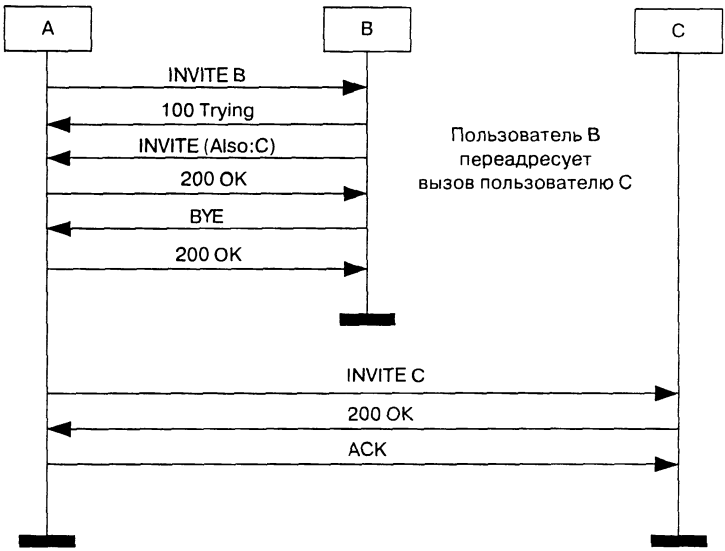


Рис. 4.6. Дополнительная услуга «Переадресация вызова»

Услуги **Переключение связи** и **Переадресация вызова** могут быть реализованы также с применением запроса **REFER**.

Дополнительная услуга **Уведомление о входящем вызове** позволяет пользователю, участвующему в телефонном разговоре, получить уведомление о том, что к нему поступил новый входящий вызов (рис. 4.7).

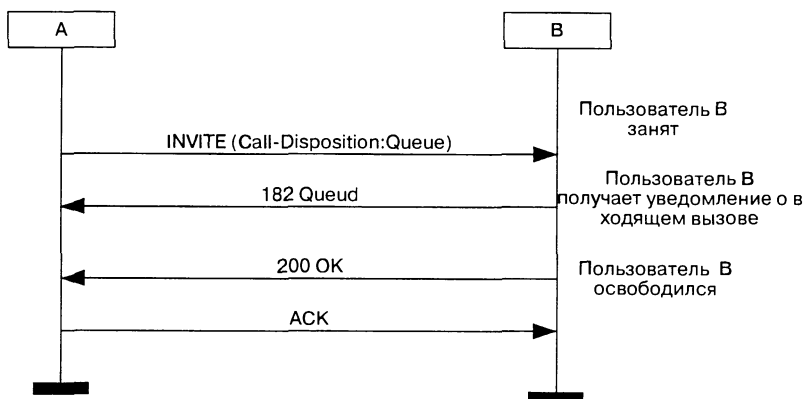


Рис. 4.7. Дополнительная услуга «Уведомление о входящем вызове»

Услуга реализуется с помощью заголовка **Call-Disposition**, в котором содержится инструкция, как нужно обслуживать вызов. Вызывающий пользователь передает запрос **INVITE** с заголовком **Call-Disposition: Queue**, который интерпретируется следующим образом: вызывающий пользователь хочет, чтобы вызов был поставлен в очередь, если вызываемый пользователь будет занят. Вызывающая сторона подтверждает запрос ответом **182 Queued**, который может передаваться неоднократно в течение периода ожидания. Вызываемый пользователь получает уведомление о входящем вызове, а когда он освобождается, вызывающей стороне передается окончательный ответ.

4.8. SIP в NGN

Основную роль SIP в контексте этой книги, посвященной Softswitch, равно как и в архитектуре сети NGN в целом, иллюстрирует рис. 4.8. Работая на разных сетевых уровнях, протокол SIP обеспечивает как взаимодействие между несколькими программными коммутаторами Softswitch, так и взаимодействие между Softswitch и конечными устройствами: IP-телефонами, soft-телефонами, IAD и т.п. В Softswitch выполняется также преобразование протокола SIP в протоколы H.323, MGCP или H.248/MEGACO, Sigtran, BICC, рассматриваемые в следующих главах книги.

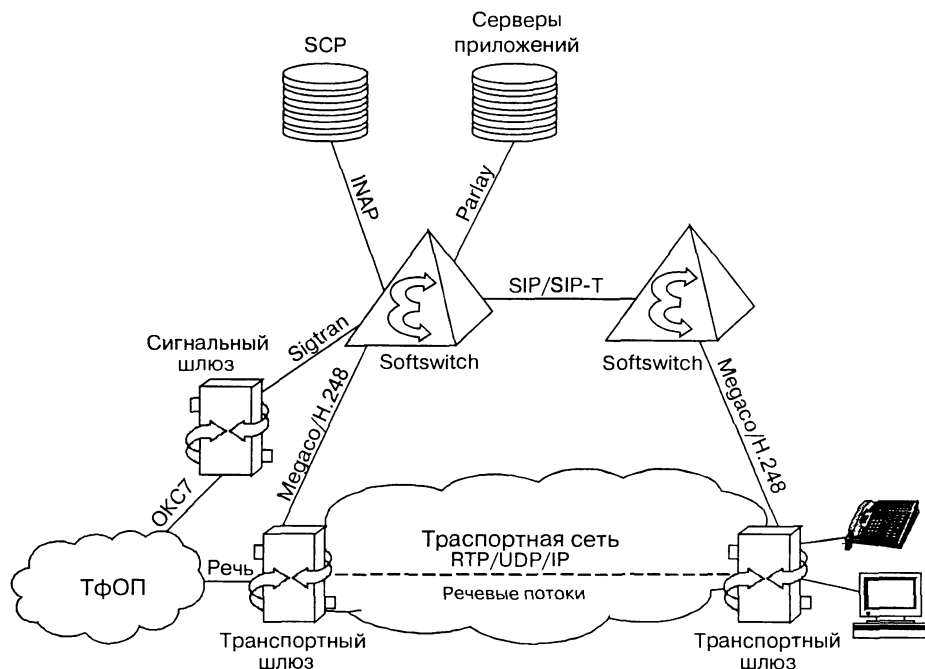


Рис. 4.8. SIP в NGN

SIP для телефонии *SIP-T (SIP for Telephony)* представляет собой механизм, который позволяет использовать SIP для установления соединений ISUP между коммутируемой телефонной сетью общего пользования на базе ОКС7 и сетями IP-телефонии на базе SIP.

SIP-T переносит полезную нагрузку сообщения ISUP в теле сообщения SIP. Заголовок SIP переносит преобразованную информацию маршрутизации ISUP. Кроме того, SIP-T специфицирует использование метода SIP INFO для обеспечения сигнализации ISUP при прохождении вызова в сети IP. Работа же группы преобразования сигнализации **Sigtran** будет рассматриваться подробнее в главе 7.

Работа над развитием протокола SIP для сетей связи следующего поколения не прекращается. Разработки IPCC в этом направлении обсуждались в двух первых главах, здесь же мы упомянем другие наиболее интересные разработки.

Взаимодействие ТФОП с Интернет **PINT (PSTN and Internet Interworking)** рассмотрено в стандарте PINT согласно RFC 2848. Согласно рекомендации PINT услуги сети ТФОП иницируются запросами IP. Клиент SIP Java, встроенный в Java servlet на Web-сервере, передает запросы, которые иницируют речевые вызовы к ТФОП.

В настоящее время внимание сосредоточено на том, чтобы обеспечить Web-доступ к речевому содержимому и обеспечить услугу *click-to-dial* (набор номера с помощью мыши компьютера), организующую взаимодействие между Web-страничкой и элементом шлюза ТфОП или сервером PINT, включая запрос телефонной связи, запрос факсимильной связи, запрос прослушивания содержимого и, в перспективе, запрос конференции.

Запросы из ТфОП/IN услуг Интернет исследует рабочая группа **SPIRITS** (*Service in the PSTN/IN Requesting Internet Service*). В рекомендации SPIRITS услуги сети IP инициируются запросами ТфОП. Рекомендации SPIRITS охватывают услуги уведомления о новом вызове Интернет, определение вызывающего абонента Интернет, получение речевой почты, разрушение соединения с провайдером услуг Интернет (ISP), попытки переадресовать вызовы и т.п. Таким образом, PINT имеет дело с услугами, инициированными в сети IP, а SPIRITS имеет дело с услугами, которые инициируются из ТфОП.

Отображение телефонных номеров ENUM определяет взаимное соответствие телефонных номеров и адресов устройств Интернет. ENUM обеспечивает процесс преобразования номера телефона по стандарту E.164 в адрес DNS (URL).

Телефонная маршрутизация через сеть IP TRIP ориентируется на организацию административного взаимодействия между доменами для уведомления серверов о доступности телефонных адресатов и об атрибутах маршрутов к этим адресатам. Сам протокол TRIP не зависит от протоколов сигнализации, поэтому может поддерживать телефонную маршрутизацию при любой системе сигнализации.

Решение о выборе SIP проектом *3rd Generation Partnership Project* (**3GPP**) оказалось, по мнению авторов, самым важным событием в развитии протокола и его роли в сетях 3G и в концепции IMS, в частности. Настолько важным, что этой теме в книге посвящена отдельная глава 11.

Глава 5

Протокол H.323

Нам нужен прогресс, но чтобы оставалось все как раньше.
Э. Макензи

5.1. H.323 в процессе эволюции IP-телефонии

История развития протокола H.323 достаточно подробно описана в книге «IP-телефония» [8] вместе с основами IP-телефонии на базе этого протокола. За прошедшие после ее опубликования годы очень многое изменилось. В настоящей главе основное внимание уделяется тому, что нового появилось в версиях рекомендации H.323 ко времени написания этой книги, и рассматривается вопрос об актуальности H.323 в России.

В процессе становления VoIP как телекоммуникационной индустрии появилось довольно четкое разделение между H.323 и SIP. На рассматриваемый в [8] период протокол H.323 считался удачным решением для интеграции IP-телефонии в ТФОП (во многом из-за его принадлежности к ITU-T и простоты реализации сценария телефон-телефон, который являлся основным источником дохода Оператора IP-телефонии), а протокол SIP, как считалось вначале, годился разве что для организации связи в корпоративной IP-сети (основным аргументом служило отсутствие механизмов взаимодействия с телефонной сигнализацией). Дальнейшее развитие SIP и появление SIP-T, о чем уже говорилось в предыдущей главе, серьезно изменило взгляды на IP-телефонию, и непрерываемым лидером для неё и для NGN в целом стал протокол SIP. Казалось бы, естественным было бы теперь отложить в сторону рекомендацию H.323 и сосредоточить усилия на развитии SIP-сетей. Некоторые операторские компании в новых областях так и поступают, однако по России в целом большая часть сетей IP-телефонии строилась именно на H.323, и перспективы немедленного переоборудования сетей этих Операторов сегодня вряд ли экономически оправданы.

Итак, попробуем пересмотреть для этих условий подход к Н.323, кратко напоминая читателю уже описанные элементы и подробнее останавливаясь на обновлениях.

5.2. Адресация в сетях Н.323

Каждый терминал пользователя, а также любое оборудование сети Н.323 должно иметь ряд адресов, используемых для разных целей. Основными являются сетевой и транспортный адреса, рассматриваемые ниже в этом параграфе. Для окончательного оборудования могут вводиться дополнительные адреса других типов, более удобные для человеческого восприятия, чем сетевой и транспортный.

5.2.1. Сетевой адрес

Любое оборудование Н.323 должно иметь, как минимум, один сетевой адрес, который однозначно его идентифицирует и является специфическим для той сети, в которой это оборудование находится (т.е. в зависимости от типа сети может изменяться формат адреса). Оконечное оборудование может во время обслуживания одного вызова использовать для разных каналов разные сетевые адреса.

5.2.2. Идентификатор TSAP

Для каждого сетевого адреса каждое оборудование Н.323 может иметь несколько *идентификаторов TSAP (транспортных адресов)*. Такой идентификатор позволяет создать несколько каналов к одному сетевому адресу.

Все оконечные устройства Н.323 имеют известные идентификаторы TSAP для канала сигнализации. У *привратников (Gatekeepers)* имеются один транспортный адрес для канала RAS и один – для организации поиска привратников в режиме многоадресной передачи.

Транспортные адреса для других каналов (аудио, видео, передачи данных, канала Н.245 и др.) могут задаваться динамически как в оконечных устройствах, так и в других устройствах Н.323. Важно отметить, что транспортные адреса каналов сигнализации и RAS могут быть изменены, но только во время процедуры регистрации.

5.2.3. Alias-адрес

Оконечное оборудование Н.323 может иметь один или несколько *alias-адресов*. Такой адрес является альтернативным адресом оконечного оборудования.

Этот адрес состоит из набранных цифр (номера вызываемого абонента), идентификатора Н.323 ID (символьный адрес, такой, как адрес e-mail), а также любые другие адреса, определенные

в рекомендации H.225.0. Адрес этого типа может иметь только окончечное оборудование. Его нельзя присвоить привратнику или устройству видеоконференций.

Можно отметить, что число адресов у одного оборудования может быть более одного (причем может быть несколько адресов одного и того же типа). Главное, чтобы все они ссылались на одни и те же сетевой и транспортный адреса этого оборудования.

Чтобы установить однозначное соответствие адресов разных типов, в привратнике создается специальная *таблица перевода (translation table)*.

5.2.4. Схема H.323 URL

Одной из разновидностей alias-адресов, определенных в рекомендации H.323, является url-ID, где содержится запись вида стандартного URL, позволяющая обращаться к требуемым ресурсам. Оборудование H.323 может принимать любые существующие URL, но при этом обязано поддерживать H.323 URL, определенные в одноименной рекомендации.

Назначение H.323 URL упрощает решение проблемы, связанной с присвоением адресов оборудованию H.323. Сам URL состоит из двух частей: user и hostport. Часть user определяет только имя оборудования (оно не несет в себе никакой информации о том, где расположено это оборудование). Часть hostport определяет доменное имя окончечного устройства, привратника или пограничного элемента.

5.3. Архитектура и основные устройства сети H.323

На рис. 5.1 изображена архитектура сети, построенной на базе рекомендации H.323. Основными устройствами сети являются: терминал, шлюз, привратник и устройство управления конференциями, рассматриваемые ниже.

5.3.1. Терминал H.323

Первое определение терминала H.323 выглядело так: «Терминал H.323 – это окончечное устройство сети IP-телефонии, обеспечивающее двустороннюю речевую или мультимедийную связь с другим терминалом, шлюзом или устройством управления конференциями». При организации децентрализованной конференции терминал H.323 мог принимать более чем один поток речевой информации, и эти потоки могли быть мультиплексированы в один логический канал.

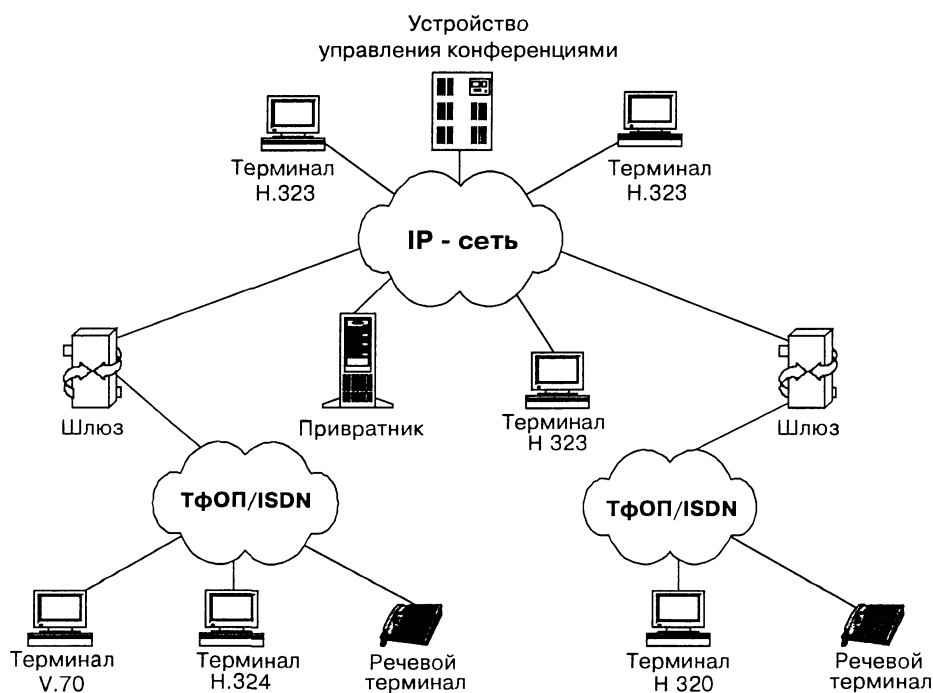


Рис. 5.1. Архитектура сети H.323

По мере развития IP-телефонии функциональные возможности терминала H.323 расширились, а его определение упростилось. Сегодня под терминалом H.323 понимается оконечный терминал пользователя, удовлетворяющий всем требованиям рекомендации H.323, т.е. поддерживающий передачу текстовых, аудио и видео потоков. Но в процессе общения пользователям зачастую не требуется видеть друг друга, а иногда даже и слышать (достаточно обмена текстовыми сообщениями).

Появилось понятие *упрощенный терминал пользователя SET (Simple Endpoint Type)*. Упрощенный текстовый терминал – это терминал, который не поддерживает большую часть рекомендации H.323, но способен вступать в текстовое взаимодействие с полноценным (или другим упрощенным) терминалом H.323, шлюзом или устройством управления конференциями. Обязательной для него является поддержка передачи текста (данных) по протоколу T.120. Текстовое общение может проводиться как в режиме точка-точка, так и в виде конференции. Следует отметить, что плюсом такого терминала является относительная простота его реализации, причем функции передачи текста могут быть достаточными для большого числа пользователей.

Упрощенный аудио-терминал – терминал, не поддерживающий часть рекомендации H.323, но способный реализовать аудио-связь с полноценным терминалом H.323 (или с другим упрощенным аудио-терминалом), шлюзом или устройством управления конференциями. Такой терминал может дополнительно поддерживать передачу текстовых сообщений. Помимо текстового и аудио-терминалов в рекомендации H.323 определяются терминалы других видов, такие как упрощенный терминал защищенной текстовой, аудио- или видеосвязи.

5.3.2. Шлюз H.323

Шлюз H.323 преобразует информацию (сигнализацию, речь и др.), поступающую со стороны ТфОП с постоянной скоростью, в вид, пригодный для передачи по IP-сетям, а также производит обратное преобразование. Последние версии H.323 не обошли стороной идеи декомпозиции шлюзов, которые пропитали практически все, что связано с NGN и IP-телефонией. В рекомендации идентифицированы интерфейсы и функции, которые должны быть использованы при декомпозиции шлюзов H.323. Конечные реализации шлюзов могут являться группой из двух и более функциональных компонентов внутри одного физического устройства. По этой причине интерфейсы могут иметь возможность прозрачного переноса сообщений других протоколов.

На рис. 5.2 показана эта идея декомпозиции шлюзов в контексте H.323 в месте окончания канала ТфОП, несущего речевой сигнал, и его преобразования в поток пакетов.

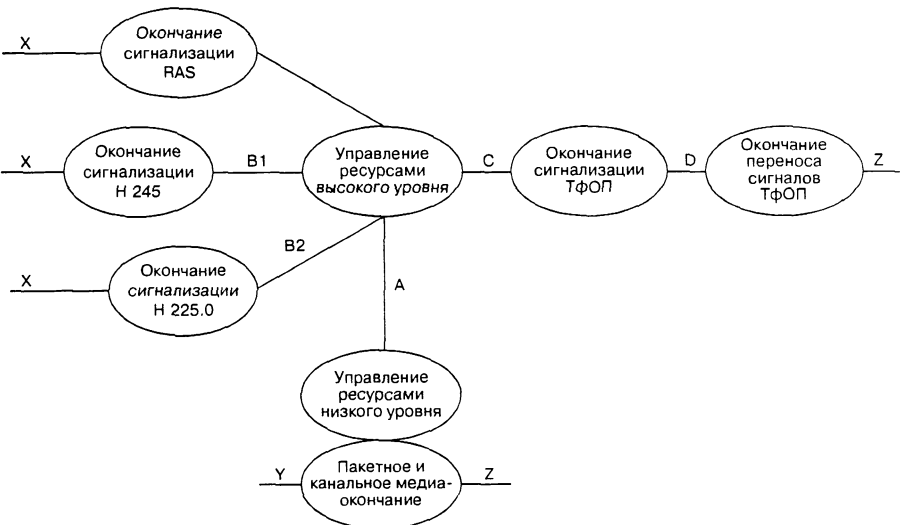


Рис. 5.2. Функциональная архитектура шлюза после его декомпозиции

В интерфейсе А используется рассматриваемый в следующей главе протокол Н.248, управляющий устройствами при создании, модификации и удалении медиа-соединений. Через интерфейс А передается сигнальная информация между стороной ТФОП шлюза и его стороной Н.323. Интерфейс В содержит компоненты протоколов Н.225.0 и Н.245 пакетной стороны шлюза. Интерфейс С обеспечивает управление обслуживанием вызовов ТФОП/ISDN при взаимодействии сигнализации FAS, связанной с устройством сети, и логикой управления шлюзом. В интерфейсе D применяется протокол, который доставляет к контроллеру сигнальную информацию NFAS, не связанную с устройством сети коммутации каналов.

Элементы управления ресурсами разделяются на верхний уровень управления ими в контроллере шлюза и нижний уровень управления ресурсами в самом шлюзе. Задача производителей оборудования состоит в реализации этих компонентов в физических устройствах, а также в стандартизации соответствующих интерфейсов, чтобы обеспечить высокую масштабируемость и совместную работу в шлюзе компонентов разных производителей.

Роль остальных интерфейсов на рис. 5.2: интерфейс Х является внешним интерфейсом Н.323, интерфейс Y – внешним интерфейсом для передачи RTP-пакетов, а интерфейс Z – внешним интерфейсом сети с коммутацией каналов.

В разделе, посвященном физической декомпозиции шлюза, описываются примеры возможной его декомпозиции и необходимые внутренние интерфейсы. В этих случаях внешние интерфейсы, такие как Н.323, и сеть с коммутацией каналов остаются неизменными. Как уже отмечалось не раз в этой книге, управляет шлюзом Н.323 так называемый MGC (Media Gateway Controller) или Softswitch, функциями которого в Н.323-сетях являются обработка сообщений Н.225.0, сигнализации RAS от привратника, а также взаимодействие с сигнализацией ОКС7. Задачами транспортного шлюза MG (Media Gateway) остаются: служить окончанием интерфейсов IP-сети, служить окончанием интерфейсов ТФОП с коммутацией каналов, а также обрабатывать сигнализацию Н.323 и сигнализацию сети с коммутацией каналов в некоторых физических декомпозициях.

В целом же, при декомпозиции шлюза не обязательно реализовать все интерфейсы. Исключение составляет интерфейс А, т.к. его реализация обязательна именно с точки зрения NGN. Дело в том, что это позволит Softswitch управлять медиашлюзами MG разных типов, что, в конечном итоге, может быть оптимизировано (например, использование речевых и мультимедиа шлюзов Н.320/Н.323). Декомпозиция интерфейсов В и С в MG, которая может потребовать протокола для транспортировки сигнальной информации от MG к MGC, пока отложена для дальнейшего изучения.

Рис. 5.3 иллюстрирует принцип декомпозиции для шлюза ISUP-to-Н.323, где функции шлюза ОКС7, MGC и MG разнесены по разным физическим устройствам. Такая архитектура позволяет передавать сигнальные сообщения ISUP через D интерфейс и вести контроль через интерфейс А. Для организации взаимодействия сетей, конфигурация шлюза после декомпозиции должна поддерживать интерфейс А и обрабатывать в MGC внутреннюю сигнализацию Н.323 и сигнализацию сетей с коммутацией каналов.

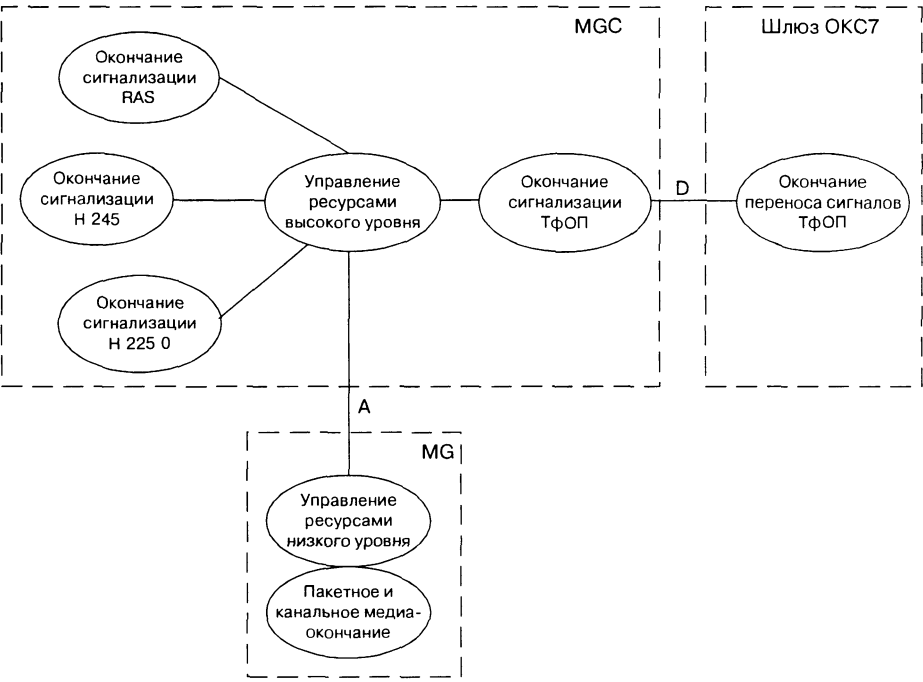


Рис. 5.3. Функциональная архитектура шлюза после его декомпозиции

В новых версиях рекомендации Н.323 есть еще несколько вариантов декомпозиции, но в этом параграфе упомянуты только основные из них.

5.3.3. Привратник

Первоначальная идея о сосредоточении в привратнике всего интеллекта сетей IP-телефонии, базирующихся на рекомендации ITU Н.323, не потеряла свою актуальность с изобретением Softswitch, но видоизменилась следующим образом: к самому Softswitch теперь предъявляется требование обладать всеми функциями привратника для управления сетями по протоколу Н.323.

Напомним наиболее важные функции, выполняемые привратником:

- преобразование *alias*-адреса в транспортный адрес сетей с маршрутизацией пакетов IP (IP-адрес и номер порта TCP),
- управления доступом пользователей системы к услугам IP-телефонии,
- контроль и резервирование пропускной способности сети, а также управление ею,
- маршрутизация сигнальных сообщений между терминалами, расположенными в одной зоне.

При отсутствии в сети привратника преобразование адреса вызываемого абонента, поступающего со стороны ТФОП в формате E.164, в транспортный адрес IP-сетей должно выполняться шлюзом или полностью возлагаться на Softswitch.

5.3.4. Устройство управления конференциями

Рекомендация H.323 предусматривает конференции трех видов:

- централизованная конференция, в которой оконечные устройства соединяются в режиме точка-точка с устройством *управления конференциями МС (Multipoint Control)*, контролирующим процесс создания и разрушения конференции, а также обрабатывающим потоки пользовательской информации,
- децентрализованная конференция, в которой каждый ее участник соединяется с остальными участниками в режиме точка – множество точек, и оконечные устройства сами обрабатывают (переключают или смешивают) потоки информации, поступающие от других участников конференции,
- смешанная конференция, т.е. комбинация конференций двух предыдущих видов.

Так как в сети может быть несколько контроллеров МС, то для каждой вновь создаваемой конференции должна проводиться процедура определения ведущего и ведомого оборудования, чтобы выявить тот из контроллеров МС, который будет управлять этой конференцией. При организации централизованной или смешанной конференции, кроме контроллера МС, должен использоваться *процессор МР (Multipoint Processor)*, обрабатывающий пользовательскую информацию и отвечающий за переключение или смешивание речевых потоков, видеоинформации и данных в зависимости от текущей активности собеседников. МР не используется только при организации децентрализованной конференции. Примеры организации централизованной конференции для двух рассмотренных вариантов приведены на рис. 5.4 и 5.5, соответственно.

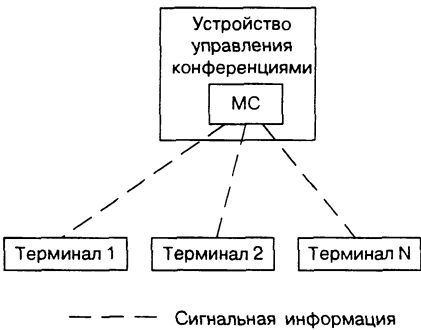


Рис. 5.4. Организация централизованной конференции с одним МС

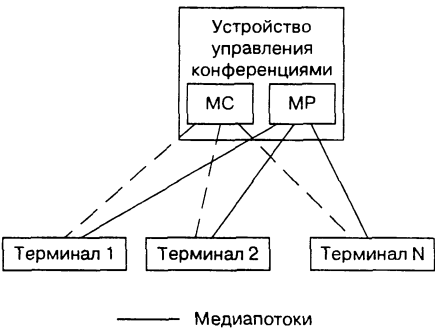


Рис. 5.5. Организация централизованной конференции с МС и МР

5.4. Протоколы Н.323

В стек Н.323 входят три основных протокола: протокол взаимодействия оконечного оборудования с привратником RAS (Registration, Admission and Status), протокол управления соединениями Н.225 и протокол управления логическими каналами Н.245, которые представлены на рис. 5.6 совместно с Интернет-протоколами TCP/IP, UDP, RTP и RTCP, а также с протоколом Q.931 (все они описаны в [5]). Как видно на этом рисунке, протокол TCP используется для переноса сигнальных сообщений Н.225 и управляющих сообщений Н.245, сигнальные сообщения RAS переносятся с помощью протокола UDP, а перенос речевой и видеоинформации производится посредством использования RTP/RTCP.

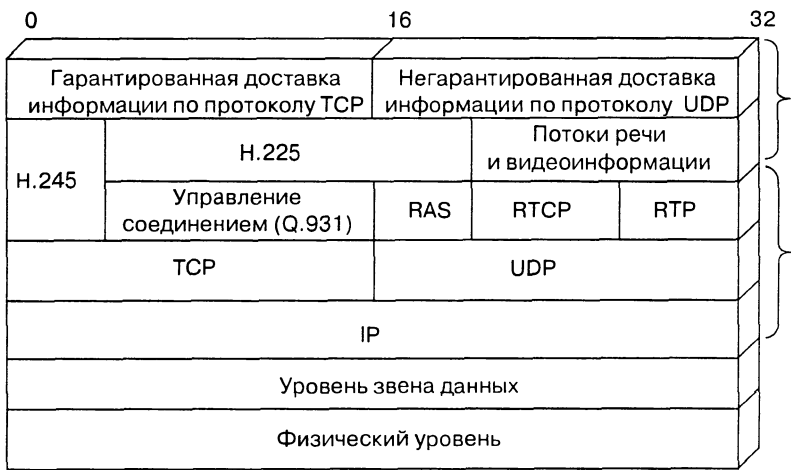


Рис. 5.6. Семейство протоколов Н.323

5.4.1. Протокол RAS

Область действия этого протокола – взаимодействие оконечного оборудования с привратником или с Softswitch. С помощью RAS происходит обнаружение привратника и регистрация в нем, контроль за состоянием соединения и контроль доступа. Поясним это. Процесс определения сетевого адреса привратника называется *обнаружением привратника*. Существуют два способа обнаружения:

- ручной, когда привратник, обслуживающий определенное устройство, задается заранее при конфигурации этого устройства;
- автоматический, когда каждый раз передается запрос *GRQ* (*Gatekeeper Request*) в режиме многоадресной рассылки (multicasting) с использованием IP-адреса 224.0.1.41 – Gatekeeper UDP Discovery Multicast Address – и UDP порта 1718 – Gatekeeper UDP Discovery Port.

При автоматическом способе обнаружения привратника оконечное устройство получает на адрес, указанный в поле **rasAddress** запроса GRQ, сообщение *GCF* (*Gatekeeper Confirmation*) с предложением своих услуг и с указанием транспортного адреса канала RAS от привратника или от выполняющего его функции Softswitch. В случае, если на GRQ отвечает несколько привратников или Softswitch, оконечное оборудование может выбрать по своему усмотрению любой из них, после чего инициировать процесс регистрации. Если в течение 5 секунд ни один привратник не ответит на GRQ, оконечное оборудование может повторить запрос. Если ответ опять не будет получен, необходимо прибегнуть к ручному способу выбора привратника.

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

С точки зрения простоты технического обслуживания сети автоматический способ обнаружения предпочтительнее ручного, так как при возникновении каких-либо неисправностей в работе привратника для переключения к новому привратнику не надо будет вручную менять конфигурацию оборудования зоны: переключение устройств к другому привратнику произойдет автоматически. Чтобы облегчить эту задачу и повысить надежность работы сети, привратник может предоставлять в поле **alternateGatekeeper** сообщений GCF и RCF перечень альтернативных привратников, к которым устройство может переключиться в случае выхода из строя его собственного привратника.

После выполнения процедуры обнаружения привратника оконечное оборудование должно быть присоединено к зоне сети, им обслуживаемой. Для этого оборудование должно сообщить при-

вратнику свою адресную информацию: список *alias*- и транспортных адресов. Этот процесс называется регистрацией окончного оборудования у привратника.

Если в качестве окончного оборудования выступают шлюз или устройство управления конференциями, то они могут зарегистрировать у привратника несколько транспортных адресов для каналов сигнализации RAS и H.225.0 (Q.931). Кроме того, для повышения надежности работы сети окончному оборудованию разрешается иметь дополнительные транспортные адреса, что дает возможность иметь в одном оборудовании два сетевых интерфейса или предусматривать дублирующее оборудование. Дополнительные транспортные адреса указываются в параметре **alternateEndpoint** некоторых сообщений сигнализации RAS.

Для регистрации служит запрос *RRQ (Registration Request)*, передаваемый на сетевой адрес привратника (либо полученный при выполнении процедуры его автоматического обнаружения, либо известный априори) на общеизвестный Gatekeeper UDP Registration and Status Port. Привратник отвечает на запрос подтверждением *RCF (Registration Confirmation)* или отказом в регистрации *RRJ (Registration Reject)*. Напомним, что окончное оборудование может зарегистрироваться только у одного привратника.

Регистрация производится на определенный промежуток времени, длительность этого промежутка в секундах указывается в параметре **timeToLive** сообщения *RRQ*. Привратник может подтвердить регистрацию сообщением *RCF* с параметром **timeToLive**, имеющим то же или меньшее значение. В течение указанного промежутка времени окончное оборудование может продлить регистрацию, используя алгоритм облегченной или дополнительной регистрации. В первом случае необходимо передать сообщение *RRQ* с параметром **keepAlive**. Получив это сообщение, привратник должен перезапустить таймер. Второй случай является опциональным (т.е. привратник или терминал могут его не поддерживать). В этом случае окончное оборудование передает сообщение *RRQ* с включенным в него полем **additiveRegistration**. При получении такого сообщения, привратник рассматривает его как информацию, дополнительную к существующей регистрации окончного оборудования, т.е. он должен:

- обновить свою таблицу перевода в соответствии со списком *alias*-адресов, принятых в сообщении;
- обновить таблицу перевода в соответствии с поддерживаемыми префиксами, принятыми в сообщении;
- заменить адреса сигнального и RAS-каналов в соответствии со значениями в полях **callSignalAssress** и **rasAddress**, если они представлены в сообщении;
- перезапустить таймер **timeToLive**, если таковой запущен.

При этом адреса и возможности оборудования, зарегистрированные ранее, не теряют свою силу, но надо учитывать, что дополнительная регистрация невозможна, если оборудование не прошло процедуру полной регистрации.

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

Окончное оборудование может отменить регистрацию у привратника, передав сообщение *URQ (Unregister Request)*, на что привратник отвечает подтверждением *UCF (Unregister Confirmation)* или отказом *URJ (Unregister Reject)*, если оборудование не было зарегистрировано у привратника. Такая процедура позволяет оборудованию изменить свой *alias*- или транспортный адрес.

В случае, если отмену регистрации инициирует привратник, оборудование обязательно отвечает подтверждением, и чтобы получить возможность участия в любом соединении, оно должно перерегистрироваться у того же привратника или зарегистрироваться у нового.

В начальной фазе установления соединения, а также после получения запроса *Setup*, оборудование обращается к привратнику при помощи запроса *ARQ (Admission Request)* с просьбой разрешить соединение с другим оборудованием, что является началом процедуры доступа к сетевым ресурсам. Важно отметить, что процедура доступа выполняется всеми участниками соединения.

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

В сообщении *ARQ* указывается также верхний предел суммарной скорости передачи и приема пользовательской информации по всем речевым и видеоканалам без учета заголовков *RTP/UDP/IP* и другой служебной информации. Во время связи средняя за секунду суммарная скорость передачи и приема информации окончным оборудованием не должна превышать этот верхний предел. Отметим, что суммарная скорость не включает в себя скорость передачи и приема информации по каналу передачи данных, по управляющему и сигнальному каналам.

Привратник может выделить требуемую полосу пропускания или снизить предел суммарной скорости, передав сообщение *ACF (Admission Confirm)*. В этом же сообщении, кроме суммарной

скорости, указывается транспортный адрес сигнального канала встречного оборудования, если сигнальный канал будет организован непосредственно между тем и другим оборудованием, или адрес привратника, если он будет маршрутизировать сигнальные сообщения.

Если требуемая полоса недоступна, привратник передает сообщение *ARJ* (*Admission Reject*).

Привратник в любой момент времени может определить текущее состояние оборудования, т.е. установить, доступно ли ему это оборудование. Такой процесс называется *опросом текущего состояния* оборудования (рис. 5.7). Очевидно, что если питание оборудования выключено, или если в его работе возникла какая-либо неисправность, оно становится недоступным.

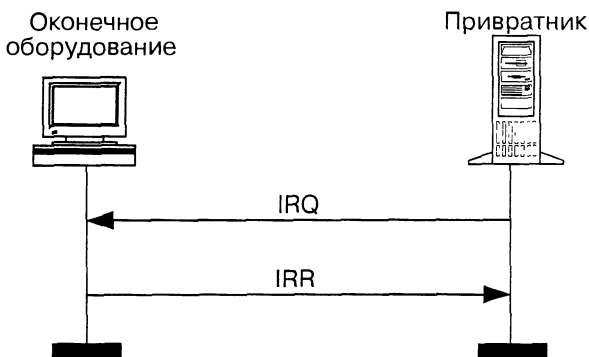


Рис. 5.7. Опрос текущего состояния оборудования

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

Привратник может дать оконечному оборудованию предписание передавать сообщения *IRR* без запросов с его стороны. Для этого привратник использует сообщение *ACF*, в поле **irrFrequency** которого указывается частота, с какой оконечное оборудование должно передавать информацию о своем текущем состоянии. Получив такое предписание, оконечное оборудование должно передавать сообщения *IRR* с указанной частотой в течение всего времени обслуживания вызова, причем привратник может запрашивать дополнительную информацию, используя сообщения *IRQ*, как было описано выше.

В конечной фазе разрушения соединения оборудование извещает привратник об освобождении ранее занимавшейся полосы пропускания, для чего передает своему привратнику сообщение *DRQ (Disengage Request)*, на которое тот должен ответить подтверждением *DCF (Disengage Confirm)*. Привратник может сам инициировать освобождение сетевых ресурсов, т.е. разрушение существующего соединения, передав сообщение *DRQ*. Получив сообщение *DRQ*, оконечное оборудование должно разрушить логические каналы, управляющий и сигнальный каналы, а затем ответить подтверждением *DCF*. В случае, если привратник инициирует разрушение конференции, сообщение *DRQ* должно передаваться каждому ее участнику.

Рассмотрим некоторые дополнительные возможности RAS и напомним с *метки доступа*. Эта метка передается в некоторых сообщениях сигнализации RAS и в сообщении *Setup*, причем имеются два основных варианта ее использования.

Первый вариант служит для сокрытия транспортного и *alias*-адресов оконечного оборудования в целях безопасности. Пользователь, желающий сохранить в тайне свои адреса, сообщает каким-либо образом вызываемому пользователю метку доступа, о наличии которой привратник заранее оповещен в процессе регистрации. Вызывающий абонент использует метку доступа для установления соединения с вызываемым абонентом, причем сигнальные каналы непременно должны проходить через привратник, который маршрутизирует сигнальные сообщения от одного абонента к другому.

Во втором варианте использования метки доступа она назначается привратником и должна передаваться во всех сообщениях, служащих для установления соединения. Примером такого использования метки доступа может служить установление соединения со шлюзом. По наличию метки шлюз определяет, что устанавливать соединение с его участием абоненту разрешено.

Еще одной возможностью RAS являются *информационные отчеты*. Для упрощения биллинга и расчетов оконечное оборудование может иметь функции сбора статистической информации о вызовах. Привратник может опросить оконечное устройство на предмет наличия такой информации. Но в этом случае необходимо использовать определенные механизмы защиты.

Путем использования опциональных кредитных возможностей оконечное оборудование может запросить абонентский кредит или получить информацию о задолженности у привратника до или после установления связи и, соответственно, уведомлять об этом пользователя. В случае задолженности оконечное оборудование может фиксировать продолжительность связи в соответствии с указаниями привратника (например, терминал может прервать

связь в случае окончания денежных средств на счету или по истечении определенного времени).

Оконечное оборудование может указать поддержку запасных транспортных протоколов, заполнив поле **alternateTransportAddresses** в сообщении RRQ. В одном случае привратник может информировать окончное оборудование о том, какой именно транспортный протокол сигнализации будет использован для связи, заполнив поле **useSpecifiedTransport** в сообщении RCF или ACF. Привратник должен заполнять это поле с учетом протоколов, занесенных в список запасных. Во втором случае привратник может предложить окончному оборудованию выбрать протокол самостоятельно.

5.4.2. Сигнальный канал Н.225.0

Процедуры управления соединениями в сетях Н.323 специфицированы в рекомендации Н.225.0. Эти процедуры предусматривают использование в базовом процессе обслуживания вызова ряда сигнальных сообщений Q.931 [5], причем должен быть реализован симметричный обмен сигнальными сообщениями в соответствии с приложением D к рекомендации Q.931.

Для активизации различных услуг в направлении от пользователя к сети могут быть использованы сообщения двух следующих типов.

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

Сообщение *Information* используется для активизации разных услуг в любой момент времени, в отличие от предыдущего, которое передается только во время фазы установления соединения.

Остальные сообщения используются для управлением услугами, а также для того, чтобы информировать встречную сторону об изменении состояния различных ресурсов.

Сообщение *Call Proceeding* передается вызывающему оборудованию, чтобы известить его о том, что вызов принят к обслуживанию. Сообщение *Alerting* передается вызывающему оборудованию и информирует его о том, что вызываемое оборудование не занято и что пользователю подается сигнал о входящем вызове.

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

Сообщение *Release Complete* передается вызывающим или вызываемым оборудованием с целью разрушить соединение.

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

Сообщение *Q.932 Notify* используется в случае, когда сеть регистрирует изменение в пользовательском профиле услуг и ей нужно информировать об этом пользователя. Оборудование, получившее такое сообщение, уведомляет об этом пользователя.

Транспортировку сигнальных сообщений обеспечивает протокол с установлением соединения и с гарантированной доставкой информации *TCP (Transport Control Protocol)*. В соответствии с первой и второй версиями рекомендации H.323 для каждого нового вызова используется отдельный сигнальный канал. Начиная с третьей версии рекомендации H.323 один сигнальный канал H.225.0 может переносить сообщения, относящиеся к разным вызовам и имеющие разные *метки соединения (call reference)*. Наличие такой возможности позволяет значительно уменьшить время установления соединения с участием шлюзов и объем передаваемой служебной информации.

Оборудование, поддерживающее управление множеством сигнальных соединений в одном сигнальном канале, присваивает значение TRUE информационному полю **multipleCalls** в сигнальных сообщениях. Оборудование может ограничивать количество сигнальных соединений, использующих один сигнальный канал, назначая определенный порог. Если этот порог достигнут, оборудование передает отказ в попытке установить соединение – сообщение *Release Complete* с указанием причины **newConnectionNeeded** (требуется новый сигнальный канал). Кроме того, в версии 3 рекомендации H.323 говорится о том, что сигнальный канал H.225.0 может быть установлен перед тем, как по нему потребуются передавать сигнальную информацию, и оставаться в рабочем состоянии после завершения соединения.

Оборудование, поддерживающее постоянно активный сигнальный канал, должно присваивать значение TRUE информационному полю **maintainConnection** в сигнальных сообщениях. Желательно также указывать на эту возможность при регистрации у привратника, что позволит привратнику (в случае маршрутизации им сигнальной информации) подключаться к оборудованию в любой момент после регистрации.

В сетях, не имеющих привратника, создается сигнальный канал H.225.0, непосредственно связывающий вызывающее окончное оборудование с вызываемым. В этом случае вызывающий пользователь должен знать транспортный адрес сигнального канала (*Call Signalling Transport Address*) оборудования вызываемого пользователя.

В сетях с привратником вызывающее оборудование передает по транспортному адресу канала RAS привратника сообщение ARQ

с указанием alias-адреса вызываемого пользователя. Если сигнальные сообщения будет маршрутизировать привратник (Gatekeeper Routed Call Signalling), то в ответном сообщении он передаст транспортный адрес своего сигнального канала, а если сигнальный канал будет устанавливаться непосредственно между вызывающим и вызываемым оборудованием (Direct Endpoint Call Signalling), то будет передан транспортный адрес сигнального канала вызываемого оборудования. Выбор варианта передачи сигнальных сообщений оставлен за привратником, хотя окончное оборудование может указывать, какой вариант для него предпочтителен. И в первом, и во втором случае сигнальный канал H.225 выполняет одни и те же функции и переносит одни и те же сообщения.

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

После обмена с привратником сообщениями ARQ и ACF по каналу RAS вызывающее оборудование передает запрос соединения Setup либо по транспортному адресу сигнального канала привратника (если сигнальные сообщения будет маршрутизировать привратник), либо по транспортному адресу сигнального канала вызываемого оборудования (если сигнальный канал будет связывать вызывающее и вызываемое оборудование непосредственно). В ответ на сообщение Setup вызываемое оборудование может передать сообщение Call Proceeding, означающее, что вся информация, необходимая для установления соединения, получена, и вызов принят к обслуживанию. Далее от вызываемого оборудования может поступить сообщение Alerting, означающее, что вызываемому пользователю подается вызывной сигнал. После того как пользователь принимает вызов, вызывающему оборудованию передается сообщение Connect с транспортным адресом управляющего канала H.245 вызываемого оборудования, если управляющий канал устанавливается непосредственно между вызывающим и вызываемым оборудованием, или транспортный адрес канала H.245 привратника, если управляющие сообщения маршрутизирует привратник.

В некоторых случаях, например, для проключения разговорных каналов в предответном состоянии, транспортный адрес управляющего канала H.245 включается в сообщения Call Proceeding или Alerting.

5.4.3. Управляющий канал Н.245

В рекомендации ITU-T Н.245 определен ряд независимых процедур для управления информационными каналами. Для выполнения этих процедур между оконечными устройствами или между оконечным оборудованием и устройством управления конференциями или привратником организуется управляющий канал Н.245. При этом оконечное оборудование должно создавать один (и только один) управляющий канал для каждого соединения, в котором оно участвует. Перенос управляющей информации Н.245 производится протоколом ТСП по нулевому логическому каналу, который должен быть постоянно открытым с момента организации канала Н.245 и вплоть до его ликвидации. Следует отметить, что нормальные процедуры открытия и закрытия логических каналов, описываемые в этой главе, для управления нулевым логическим каналом не применяются.

По управляющему каналу Н.245 передаются сообщения четырех категорий: *запросы, ответы, команды и индикации*. Получив сообщение-запрос, оборудование должно выполнить определенное действие и немедленно передать обратно сообщение-ответ. Получив сообщение-команду, оборудование должно также выполнить определенное действие, но отвечать на команду не должно. Сообщение-индикация служит для того, чтобы информировать о чем-либо получателя, но не требует от него ни ответа, ни каких бы то ни было действий. Ниже дается краткое описание основных процедур Н.245, выполняемых в процессе управления логическими каналами.

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

В ответ на полученные сообщения **masterSlaveDetermination** оба устройства передают сообщения **masterSlaveDeterminationAck**, в которых указывается, какое оборудование является для данного соединения ведущим, а какое – ведомым.

Как правило, устройства поддерживают несколько алгоритмов кодирования и декодирования информации каждого вида, поэтому

для согласования режимов работы передающей и принимающей сторон используется процедура, называемая *обменом данными о функциональных возможностях оборудования*, в ходе которой терминалы обмениваются сообщениями **TerminalCapabilitySet**, в которых каждый из них указывает алгоритмы, используемые для декодирования принимаемой и кодирования передаваемой информации, то есть режимы, в которых оборудование может функционировать. Кроме того, оборудование может указывать режимы, которые оно поддерживает при передаче информации, и предоставлять возможность выбора режима приемной стороне.

В сообщении **TerminalCapabilitySet** включается поле **capabilityTable** – таблица функциональных возможностей, где каждому алгоритму кодирования/декодирования присвоен порядковый номер. Например, возможности приема речевой информации, закодированной по алгоритму G.723.1, соответствует номер 1, возможности приема речевой информации, закодированной по алгоритму G.728, – номер 2, возможности приема видеосигналов, закодированных по алгоритму H.263, – номер 3 и т. д.

Указанные порядковые номера объединяются в список альтернативных режимов **alternativeCapabilitySet**. Оборудование может использовать любой (но только один) из режимов, указанных в списке. Например, список альтернативных режимов {G.711, G.723.1, G.728} означает, что оборудование может функционировать в любом из указанных режимов обработки речи, но только в одном.

В свою очередь, альтернативные режимы объединяются в наборы одновременно возможных режимов функционирования **simultaneousCapabilities**.

Функциональные возможности терминала описываются набором дескрипторов (**capabilityDescriptor**), каждый из которых состоит из одного набора одновременно возможных режимов функционирования оборудования и номера дескриптора (**capabilityDescriptorNumber**). Если при обмене данными о функциональных возможностях оборудования указывает более чем один дескриптор, это означает, что оборудование поддерживает несколько режимов функционирования.

Заметим, что функциональные возможности оборудования, не определенные рекомендацией ITU H.245, могут быть указаны в поле **nonStandartParameter**.

Оборудование может в любое время передать сообщение **TerminalCapabilitySet** с дескриптором, добавляющим новые функциональные возможности, или с дескриптором, исключаящим некоторые из ранее указанных возможностей. Любое оборудование стандарта H.323 должно включать в сообщение **TerminalCapabilitySet**, по крайней мере, один дескриптор. Исключение составляет сообщение **EmptyCapabilitySet** (пустой набор

функциональных возможностей), которое используется для реализации дополнительных возможностей системы.

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

Теперь рассмотрим процедуры *открытия и закрытия логических каналов*. Информация, передаваемая источником к одному или более приемникам в сетях, базирующихся на рекомендации H.323, переносится по логическим каналам, которые идентифицируются уникальным для каждого направления передачи номером канала. Рекомендацией H.245 предусмотрена возможность открытия логических каналов двух видов: *однонаправленных (uni-directional)* при помощи процедуры Uni-directional Logical Signalling, т.е. открывающихся в направлении от источника к приемнику информации, и *двухнаправленных (bi-directional)* при помощи процедуры Bi-directional Logical Signalling, открывающихся сразу в двух направлениях – от источника к приемнику информации и в обратном направлении.

В требовании открыть логический канал **openLogicalChannel** оборудование указывает вид информации, который будет передаваться по этому каналу, и алгоритм кодирования информации. Если логический канал предназначается для переноса речи или видеоинформации с помощью протокола RTP (Real Time Protocol), то в сообщении **openLogicalChannel** должен включаться параметр **mediaControlChannel** с указанием транспортного адреса канала протокола RTCP (Real Time Control Protocol), при помощи которого ведется контроль передачи RTP пакетов.

Оборудование, получившее запрос открыть логический канал для приема данных, вид которых не поддерживается или не распознан, должно ответить сообщением **openLogicalChannelReject**, а получение корректного сообщения **openLogicalChannel** оборудование должно подтвердить сообщением **openLogicalChannelAck**. В случае открытия двустороннего канала добавляется сообщение **openLogicalChannelConfirm**, которое передается в ответ на сообщение **openLogicalChannelAck** и подтверждает, что двунаправленный логический канал открыт. Закрытие логических каналов может производиться с помощью процедуры **CloseLogicalChannel**, но она используется, в основном, для поддержки предоставления дополнительных услуг, в первую очередь, постановки на удержание. Для нормального разрушения соединения стороны обмениваются сообщениями **endSessionCommand**. После обмена этими сообщениями закрываются не только логические каналы, но и управляющий канал H.245.

Еще одним важным аспектом является *мультиплексирование потоков в H.245*. Такая ситуация возникает, когда через один логический канал по протоколу RTP передается поток, который содержит в себе несколько медиапотоков, мультиплексированных с использованием протоколов H.222.0 или H.223. Благодаря применению протоколов мультиплексирования, оконечное оборудование H.323 может использовать выделенную полосу пропускания более эффективно, упростить процедуру синхронизации, а также снизить возникающие при передаче мультимедиа потока задержки.

Существует два подхода к вопросу контроля конфигурации мультиплексированного потока.

Для первого варианта сообщения H.245 передаются внутри мультиплексированного RTP-потока. В этом случае оконечное оборудование сначала открывает двунаправленный логический канал для передачи мультиплексированного потока, используя сообщения H.245, как и для обычного RTP потока. Далее контроль мультиплексированного потока ведется, используя сообщения H.245 внутри RTP-пакетов этого мультиплексированного потока. Контроль мультиплексированного потока делает возможным обмен информацией относительно доступных для данного потока медиа-кодексов, обмен мультиплексной таблицей и открытие/закрытие логических каналов.

Второй вариант заключается в контроле логических каналов мультиплексированного потока тем же самым путем, что и контроль не мультиплексированных логических каналов, т.е. сообщения H.245 для мультиплексированного потока передаются тем же способом, что и обычные сообщения H.245. В таком случае оконечное оборудование открывает одно/двунаправленный логический канал для передачи мультиплексированного потока, используя процедуры открытия и закрытия логических каналов H.245, как для обычных RTP медиа-потоков. Когда логические каналы мультиплексированного потока открыты, используя указанные процедуры с параметрами конфигурации протокола мультиплексирования и параметрами числа логических каналов мультиплексированного потока, создается новый логический канал.

Обмен данными о функциональных возможностях относительно мультиплексированного потока представляет собой следующее. Терминалы H.323, поддерживающие одиночные потоки, отображают эту возможность, включая заголовок **MultiplexedStreamCapability**, как часть возможностей терминала H.323. Параметр **controlOnMuxStream** в заголовке **MultiplexedStreamCapability** отображает, поддерживается ли контроль мультиплексированного потока с использованием сообщения H.245, или контроль ведется посредством пакетов RTP. Если параметр **controlOnMuxStream**

равен логической единице, возможности терминала относительно работы с кодеками могут быть выражены в параметре **capabilityOnMuxStream**. В случае отсутствия параметра **capabilityOnMuxStream**, терминал должен производить обмен данными о функциональных возможностях, передавая сообщения Н.245 в RTP пакетах через мультимплексированный поток в открытом логическом канале. В случае, когда **controlOnMuxStream** равен логическому нулю, возможности работы оборудования с кодеками должны быть определены в параметре **capabilityOnMuxStream**.

Сигнализация логических каналов для транспортировки мультимплексированного потока происходит следующим образом. Логический канал для мультимплексированного потока открывается путем передачи сообщения **openLogicalChannel** с параметром **dataType** заголовка **MultiplexedStreamCapability** и параметрами **multiplexParameters** заголовка **h2250LogicalChannelParameters**. Если в заголовке **MultiplexedStreamCapability** параметр **controlOnMuxStream**=1, открываемый логический канал должен быть двусторонним, т.е. должны быть установлены параметры **reverseLogicalChannelParameters**. Иначе логический канал будет односторонним. Необходимо отметить, что если логический канал открыт как односторонний, некоторые функции протокола мультимплексирования не смогут действовать (например, AL3 в протоколе Н.223). Терминал не должен открывать более одного логического канала с параметрами **multiplexFormat** заголовка **h223Capability** и **controlOnMuxStream**, равными логическому нулю.

Сигнализация логических каналов для транспортировки медиа-потоков через мультимплексированный поток происходит очень похоже. Логический канал через мультимплексированный поток открывается с помощью сообщения **openLogicalChannel** с соответствующим значением **dataType** для транспортировки медиа информации и со значением **multiplexParameters**, соответствующим используемому протоколу мультимплексирования (например, **h223logicalChannelParameters**). Если параметр **controlOnMuxStream** соответствует логической единице, сообщения Н.245 доставляются через управляющий канал Н.245, как обычно. В случае протокола Н.222.0, параметры **resourceID** заголовка **h2220LogicalChannelParameters** назначаются в соответствии с числом логических каналов для мультимплексированного потока, через который открывается новый логический канал. Необходимо отметить, что в случае протокола Н.223 сигнализации такого рода не требуется благодаря тому, что более одного логического канала существовать не может. Образованные через мультимплексированный поток логические каналы закрываются с помощью передачи сообщения **closeLogicalChannel**, которое пересылается тем же самым путем, что и сообщение **openLogicalChannel**.

Логический канал для мультиплексированного потока, который был открыт со значением параметра **controlOnMuxStream**, равным логической единице, может быть закрыт в любое время с помощью сообщения **closeLogicalChannel**. Если при создании логического канала параметр **controlOnMuxStream** имел значение «логический ноль», этот канал необходимо закрывать только после того, как будут закрыты все логические каналы мультиплексированного потока.

В последних версиях протокола H.323 было сделано немало шагов в сторону повышения стабильности и устойчивости работы. Были также введены механизмы переноса часто передающихся по сети ТФОП сигналов модема и факса, а также обеспечено туннелирование через H.323 сигнализации QSIG, ISUP и DSS1. Можно сказать, что введение новых версий рекомендации и дополнений функций есть не что иное, как попытка превратить H.323 в полноценный протокол NGN. Рассмотрим некоторые из этих дополнений и начнем с *передачи пакетов T.38 протоколом H.323*.

Связь между двумя факсимильными аппаратами группы 3 рассматривается в H.323 как поток данных, когда пользователь передает факс в режиме реального времени, для чего факсимильные сигналы должны переноситься аналогично речевым сигналам. Случай передачи факсимильных сообщений по технологии *Store & Forward* не рассматривается. Таким образом, задача сети H.323 при передаче факсимильных сообщений заключается в передаче пакетов T.38 через сеть IP в режиме реального времени. Любое оборудование H.323, поддерживающее факсимильные возможности, должно поддерживать протокол T.38.

Для передачи пакетов T.38 используется процедура *Fast connect*. При этом открываются два логических канала (от отправителя к получателю и обратный) или один двунаправленный канал, как показано на рис. 5.8.

Поддержка оборудованием второго варианта является необязательной. Пакеты T.38 могут пересылаться с использованием протокола TCP или UDP. В общем случае, протокол TCP является более эффективным, когда пропускная способность факсимильного соединения ограничена. В ином случае более эффективен протокол UDP. Следует отметить, что помимо факсимильных каналов, дополнительно может быть открыто до двух аудио-каналов, если оконечное оборудование поддерживает такую функцию.

Аналогичным образом обстоит дело с *передачей через H.323 модемных сигналов*. В рекомендации H.323 описано, как использовать протокол V.150.1 для передачи модемных сигналов в среде H.323. Это определило новую концепцию в протоколе H.245, названную *MPS (Multiple Payload Streams)*.

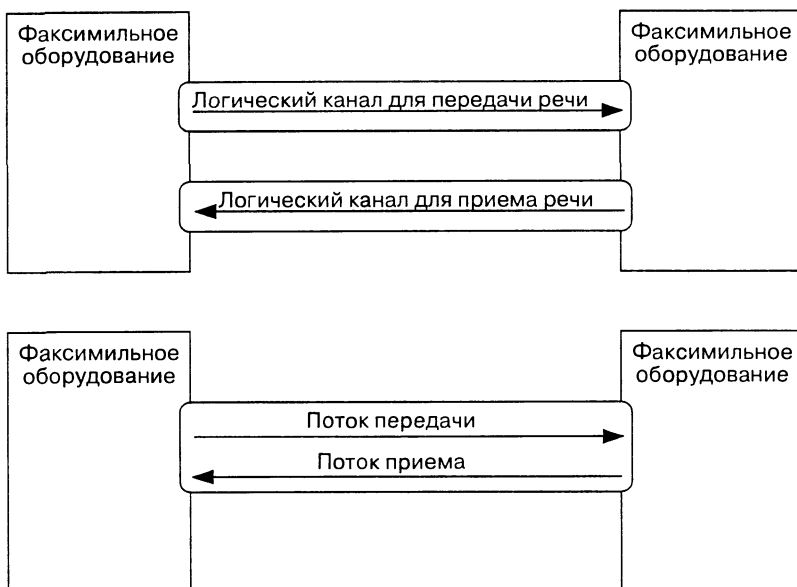


Рис. 5.8. Организация двух логических каналов или одного двунаправленного канала

В последней версии протокола H.245 окончательному оборудованию позволено создавать RTP-сеансы, которые могут переносить как речевые, так и модемные сигналы (а также и любые другие, например, DTMF, факс и т.п.).

5.5. Алгоритмы установления, поддержания и разрушения соединения

5.5.1. Базовое соединение

В общем случае алгоритмы установления, поддержания и разрушения соединений по протоколу H.323 включают в себя следующие фазы:

Фаза А. Установление соединения.

Фаза В. Определение ведущего/ведомого оборудования и обмен данными о функциональных возможностях.

Фаза С. Установление аудиовизуальной связи между вызывающим и вызываемым оборудованием.

Фаза D. Изменение полосы пропускания, запрос сведений о текущем состоянии оборудования, создание конференций и обращение к дополнительным услугам.

Фаза Е. Завершение соединения.

Здесь мы рассмотрим базовое соединение с участием Softswitch, выполняющего функции привратника. Сценарий этого случая приведен на рис. 5.9. Другие варианты рассматривались в [8].

Вызывающее оборудование передает сообщение ARQ с alias-адресом вызываемого абонента, в ответ на которое привратник передает сообщение ACF с уведомлением, что именно он будет маршрутизировать сигнальные сообщения (Gatekeeper routed call signaling), и с указанием транспортного адреса своего сигнального канала.

Далее вызывающее оборудование передает на этот транспортный адрес запрос соединения Setup. Привратник пересылает сообщение Setup вызываемому оборудованию и передает вызывающему оборудованию сообщение Call Proceeding, означающее, что полученной информации достаточно для обслуживания поступившего вызова. Вызываемое оборудование также отвечает на Setup сообщением Call Proceeding. Если оборудование имеет возможность принять вызов, оно передает запрос на допуск к ресурсам сети ARQ, на который привратник может ответить подтверждением ACF или отказом в допуске к ресурсам сети ARJ. В первом случае вызываемое оборудование передает сообщение Alerting, и привратник маршрутизирует его к вызываемому оборудованию. Вызываемому пользователю подается визуальный или акустический сигнал о входящем вызове, а вызывающему дается индикация того, что вызываемый пользователь не занят и ему подается вызывной сигнал. При отказе в допуске к ресурсам сети вызываемое оборудование закрывает сигнальный канал путем передачи привратнику сообщения Release Complete.

После того как вызываемый пользователь примет входящий вызов, привратнику передается сообщение Connect с транспортным адресом управляющего канала H.245 вызываемого оборудования. Привратник заменяет этот адрес транспортным адресом своего управляющего канала H.245 и пересылает Connect вызывающему оборудованию, после чего открывается управляющий канал H.245.

Чтобы ускорить создание разговорного сеанса, управляющий канал может быть открыт вызываемым оборудованием после получения сообщения Setup с транспортным адресом управляющего канала H.245 вызывающего оборудования или привратника, или вызывающим пользователем после получения сообщения Call Proceeding или Alerting, содержащего транспортный адрес управляющего канала H.245 вызываемого пользователя или привратника.

После открытия управляющего канала H.245 начинается обмен данными о функциональных возможностях оборудования. В рассматриваемом нами случае все управляющие сообщения, передаваемые от одного оконечного оборудования к другому, маршрутизируются привратником.

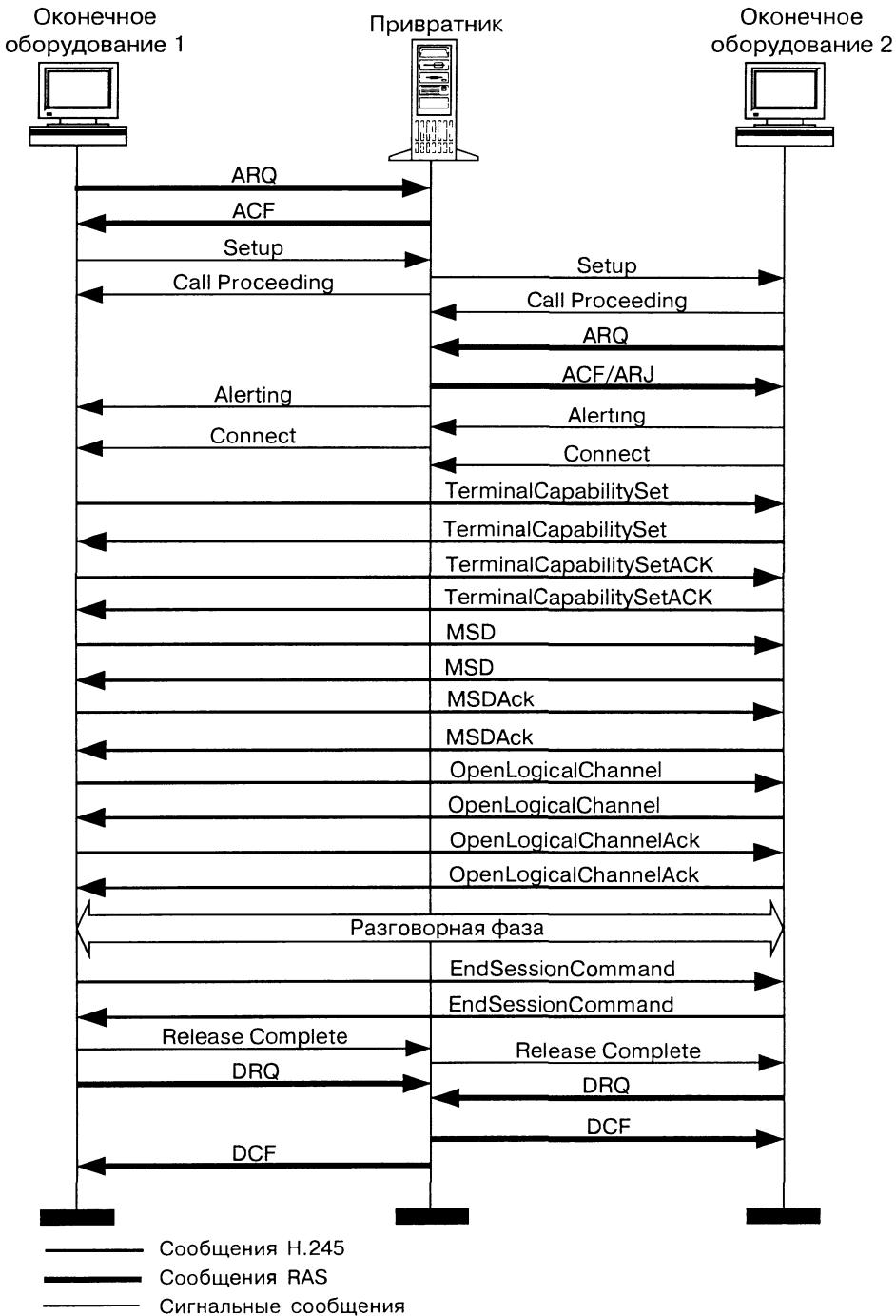


Рис. 5.9. Пример соединения с участием привратника

Терминалы обмениваются сообщениями **TerminalCapabilitySet**, в которых указываются возможные алгоритмы декодирования принимаемой информации. Следует отметить, что сообщение **TerminalCapabilitySet** должно быть первым сообщением, передаваемым по управляющему каналу. Оборудование, принявшее сообщение **TerminalCapabilitySet** от другого оборудования, подтверждает его получение передачей сообщения **TerminalCapabilitySetAck**.

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

В ответ на полученные сообщения **masterSlaveDetermination** оба устройства передают сообщения **masterSlaveDeterminationAck**, в которых указывается, какое из этих устройств является для данного соединения ведущим, а какое – ведомым.

Напомним, что возможен сценарий работы процедуры Master-Slave Determination, предусматривающий сокращение количества передаваемых сообщений: оборудование, передавшее сообщение **masterSlaveDetermination** и получившее в ответ сообщение **masterSlaveDeterminationAck**, передает сообщение **masterSlaveDeterminationAck**.

После обмена данными о функциональных возможностях и определения ведущего и ведомого оборудования может выполняться процедура открытия однонаправленных логических каналов. В требовании открыть логический канал (в нашем случае – прямой логический канал) **openLogicalChannel** оборудование указывает вид информации, который будет передаваться по этому каналу, и алгоритм кодирования. В нашем случае логический канал предназначается для переноса речи, поэтому в сообщении **openLogicalChannel** включается параметр **mediaControlChannel** с указанием транспортного адреса канала RTCP, при помощи которого производится контроль передачи RTP-пакетов. В ответ на сообщение **openLogicalChannel** оборудование должно передать подтверждение **openLogicalChannelAck**, в котором указывается транспортный адрес, на который передающей стороне следует передавать RTP-пакеты, а также транспортный адрес канала RTCP.

Далее открывается разговорный сеанс. Оборудование вызывающего пользователя передает речевую информацию, упакованную в пакеты RTP/UDP/IP, на транспортный адрес RTP-канала оборудования вызванного пользователя, а вызванный пользователь передает пакетизированную речевую информацию на транспортный

адрес RTP-канала оборудования вызвавшего пользователя. При помощи канала RTCP ведется контроль передачи информации по RTP-каналам.

После окончания разговорной фазы начинается фаза разрушения соединения. Оборудование пользователя, инициирующее разъединение, должно прекратить передачу речевой информации, закрыть логические каналы и передать по управляющему каналу сообщение H.245 **endSessionCommand**, означающее, что пользователь хочет разрушить соединение. Далее от встречного оборудования ожидается сообщение **endSessionCommand**, после приема которого управляющий канал H.245 закрывается. Следующим шагом, если сигнальный канал еще открыт, передается сообщение Release Complete.

Пользователь, получивший команду **endSessionCommand** от пользователя, инициировавшего разрушение соединения, должен прекратить передачу речевой информации, закрыть логические каналы и передать сообщение **endSessionCommand**. Далее, если сигнальный канал остался открытым, передается сообщение Release Complete, и сигнальный канал закрывается.

После вышеописанных действий окончное оборудование извещает привратник об освобождении резервированной полосы пропускания. С этой целью каждый из участников соединения передает по каналу RAS запрос выхода из соединения DRQ, на который привратник должен ответить подтверждением DCF, после чего обслуживание вызова считается завершенным.

5.5.2. Туннелирование управляющих сообщений

Для ускорения установления соединения может использоваться процесс, известный как инкапсуляция или туннелирование управляющих сообщений H.245. При этом передача сообщений H.245 производится по сигнальному, а не по отдельному управляющему каналу. Одно или несколько сообщений H.245 переносятся в элементе **h245Control** информационного поля **h323_uu_pdu** в любом из разрешенных сообщений Q.931.

Чтобы применить инкапсуляцию сообщений H.245, вызывающее оборудование должно присвоить значение TRUE элементу **h245Tunnelling**, передаваемому в сообщении Setup и в следующих сообщениях Q.931. Вызываемое оборудование, получившее в сообщении Setup элемент **h245Tunnelling** со значением TRUE и желающее использовать инкапсуляцию управляющих сообщений, также должно присвоить значение TRUE элементу **h245Tunnelling** в сообщении, передаваемом в ответ на сообщение Setup, и в следующих сообщениях Q.931.

Вызываемое оборудование, не поддерживающее туннелирование управляющих сообщений, присваивает элементу **h245Tunnelling**, передаваемому в ответе на сообщение Setup, значение FALSE. В этом случае для передачи управляющих сообщений открывается отдельный канал H.245.

5.5.3. Процедура быстрого установления соединения

Самый быстрый способ установления соединения в сети, базирующейся на рекомендации H.323, это использование процедуры *Fast Connect*. Чтобы инициировать процедуру Fast Connect, вызывающее оборудование передает сообщение Setup с элементом **fastStart**. Этот элемент может включать в себя одну или несколько структур **OpenLogicalChannel**. Одна из структур **OpenLogicalChannel** обязательно должна содержать элемент **forwardLogicalChannelParameters** и может содержать элемент **reverseLogicalChannelParameters**, но, в то же время, структура **OpenLogicalChannel** описывает всего один однонаправленный логический канал. Это означает, что когда описывается прямой логический канал, то в структуре присутствует только элемент **forwardLogicalChannelParameters**. Элемент содержит информацию об алгоритме, который используется вызывающим оборудованием для кодирования передаваемой информации, и адрес канала RTP. При описании канала обратного направления в элементе **forwardLogicalChannelParameters** не содержится никакой информации, хотя сам он обязательно присутствует, а в элементе **reverseLogicalChannelParameters** содержатся сведения об алгоритме декодирования принимаемой информации, транспортный адрес RTP, на который следует передавать информацию, и адрес канала RTP.

В элементе **fastStart** может присутствовать несколько альтернативных структур **OpenLogicalChannel**, различающихся алгоритмами кодирования передаваемой информации или декодирования принимаемой информации, причем наиболее предпочтительные алгоритмы указываются в первую очередь.

Вызываемое оборудование может отклонить процедуру Fast Connect, либо если оно ее не поддерживает, либо если существует потребность в использовании процедур H.245 с открытием отдельного канала H.245 или с туннелированием управляющих сообщений. В этом случае элемент **fastStart** не включается ни в одно из сообщений, передаваемых после приема Setup, до сообщения Connect включительно. Открытие логических каналов для передачи речевой информации производится с использованием процедур H.245. Вызываемое оборудование, получившее сообщение Setup с элементом **fastStart** и могущее поддержать процедуру Fast Connect, должно включить элемент **fastStart** в любое из сообщений Q.931, передаваемых после приема Setup,

до сообщения Connect включительно. Элемент **fastStart** содержит структуры **OpenLogicalChannel**, которые выбраны вызываемым оборудованием из структур, предложенных вызывающим оборудованием. И снова одна из структур **OpenLogicalChannel** содержит элемент **forwardLogicalChannelParameters** со сведениями об алгоритме кодирования информации, с транспортными адресами каналов RTP и RTCP вызываемого оборудования. Вторая структура **OpenLogicalChannel** включает в себя элемент **forwardLogicalChannelParameters**, не содержащий никакой информации, и элемент **reverseLogicalChannelParameters** со сведениями об алгоритме кодирования информации и с транспортным адресом канала RTCP вызываемого оборудования.

Вызываемое оборудование может начинать передачу информации сразу вслед за любым сообщением Q.931 с элементом **fastStart**. Это означает, что вызывающее оборудование должно быть готовым к приему информации, закодированной любым из указанных в сообщении Setup способов. Сообщение Q.931 с элементом **fastStart**, переданное вызываемым оборудованием после получения сообщения Setup, может прийти после начала передачи пользовательской информации. Если вызывающее оборудование не желает принимать речевую информацию до прихода сообщения Connect, оно присваивает значение TRUE элементу **mediaWaitForConnect**, передаваемому в сообщении Setup.

Вызывающее оборудование, инициировавшее процедуру Fast Connect, может начать передачу речевой информации сразу после приема любого из разрешенных сообщений Q.931, содержащего элемент **fastStart**.

При разрушении соединения одним из участников передается сообщение Release Complete, после чего закрывается сигнальный канал и соединение считается завершенным.

Следует отметить, что при использовании процедуры Fast Connect или при туннелировании управляющих сообщений как одна, так и другая сторона может открыть управляющий канал H.245, для чего оборудование этой стороны должно включить в любое сообщение Q.931 элемент **h245Address**. При этом процедура Fast Connect или туннелирование прерывается.

В заключение стоит отметить, что процедура быстрого старта наиболее удобна для установления соединений. Скорее всего, H.323 останется в сетях IP-телефонии на ближайшее время, но с точки зрения Softswitch эта рекомендация будет учтена лишь для взаимодействия с уже существующими сетями.

Глава 6

Управление транспортными шлюзами

*Если вы говорите с Богом, это молитва,
а если Бог говорит с вами, это шизофрения.*
Томас Сас

6.1. Еще раз о декомпозиции шлюза

Эпиграф к этой главе подчеркивает принципиальное отличие асимметричных по своей сути протоколов MGCP и Megaco/H.248 от рассмотренных в предыдущих главах симметричных протоколов H.323 и SIP. Эта асимметрия типа *ведущий-ведомый (master-slave)* обусловлена самим назначением протоколов – *управление транспортными шлюзами*.

Поясним это. В главе 3 были описаны преимущества технологии VoIP перед традиционной телефонией в сети TDM (меньшая стоимость, уменьшение требуемой полосы пропускания для телефонной связи, интеграция приложений передачи речи и передачи данных, новые функциональные возможности и т.п.). Было бы прекрасно, если бы все телефоны работали на основе IP, чтобы указанные преимущества стали бы доступными глобально. К сожалению, немедленная замена всех традиционных сетей с коммутацией каналов на IP-сети нереальна просто в силу непомерной цены такой замены. Поэтому происходит постепенный переход от сетей с коммутацией каналов к IP-сетям, причем сети обоих типов будут сосуществовать бок о бок очень долгое время. Делать это нужно как можно более «бесшовно», пользователи существующих систем

с коммутацией каналов должны иметь возможность свободно связываться с пользователями VoIP, и наоборот, что достигается путем применения *транспортных шлюзов*. Мы видели в двух предыдущих главах, что сигнализация SIP или H.323, обслуживающая вызовы VoIP, может выбирать совершенно другой путь, чем путь передачи самой речевой информации.

Кстати, в следующей главе 7 мы напомним, что логическое разделение среды сигнализации и среды передачи информации – концепция отнюдь не новая; подобный подход существует много лет в системе общеканальной сигнализации №7 сети TDM. В контексте же этой главы важно, что сетевой шлюз имеет две отдельные функции: преобразование сигнализации (непосредственно в Softswitch) и преобразование формы передачи информации пользователей (в управляемых Softswitch транспортных шлюзах), как это показано на рис. 6.1, который является модифицированным фрагментом рис.1.1, рассмотренного в главе1.

Упрощенно же можно сказать, что все функции управления обслуживанием вызовов и соответствующая сигнализация управления соединениями возлагаются на Softswitch, в то время как транспортный шлюз получает команды из Softswitch и, в основном, выполняет то, что приказывает Softswitch. Команды из Softswitch обычно касаются установления соединений и отмены соединений одной стороны шлюза с другой. В большинстве случаев Softswitch приказывает транспортному шлюзу соединить абонентскую или соединительную линию на стороне шлюза, подключенной к средствам коммутации каналов, с портом RTP на стороне IP шлюза, как показано на рис. 6.1.

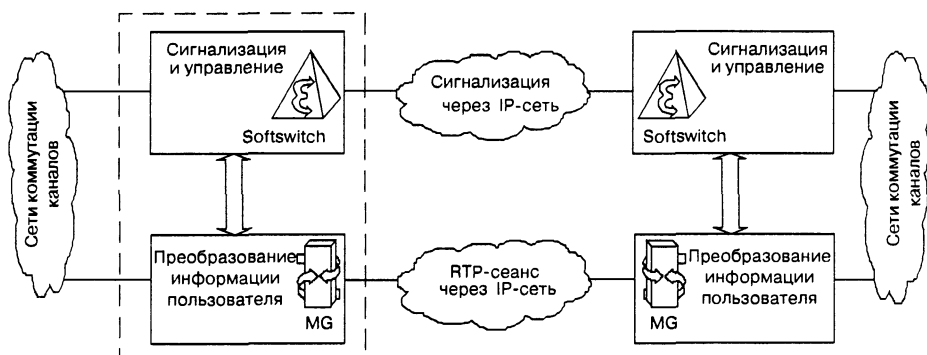


Рис. 6.1. Управление транспортными шлюзами

При разработке протокола управления шлюзами рабочая группа Megaco опиралась именно на рассматривавшийся в предыдущем параграфе (и ранее на страницах книги) *принцип декомпозиции шлюза*, при котором шлюз разбивается на следующие функциональные блоки:

- *транспортный шлюз Media Gateway*, который преобразует речевую информацию, поступающую со стороны ТФОП, в вид, пригодный для передачи по сетям с маршрутизацией пакетов IP, т.е. кодирование и упаковку речевой информации в пакеты RTP/UDP/IP, а также выполняет обратное преобразование;
- *устройство управления шлюзом Media Gateway Controller (Softswitch, Call Agent)*, выполняющее функции управления шлюзом и содержащее весь интеллект шлюза после его декомпозиции;
- *шлюз сигнализации Signaling Gateway*, который обеспечивает доставку сигнальной информации, поступающую со стороны ТФОП, к устройству управления шлюзом и перенос сигнальной информации в обратном направлении, т.е., в частности, выполняет функции STP – транзитного пункта системы сигнализации по общему каналу ОКС7.

Один Softswitch, как правило, управляет одновременно несколькими транспортными шлюзами. В сети может присутствовать несколько Softswitch, которые связаны между собой и согласованно управляют шлюзами, участвующими в соединении. Заметим, что в MGCP или Megaco протокол взаимодействия нескольких Softswitch не определяется; для этой цели предназначены рассмотренные в двух предыдущих главах протоколы H.323 или SIP, а также протокол BICC, которому посвящена глава 8.

В компетенцию рабочей группы Sigtran комитета IETF (подробнее о ней в следующей главе) входит механизм взаимодействия Softswitch и шлюза сигнализации, который должен принимать поступающие из ТФОП пакеты трех нижних уровней системы сигнализации ОКС7 (уровней подсистемы переноса сообщений МТР) и передавать сигнальные сообщения верхнего, пользовательского, уровня к Softswitch. Если же используется сигнализация по выделенным сигнальным каналам (ВСК), то сигналы сначала поступают вместе с пользовательской информацией в транспортный шлюз, а затем передаются в устройство управления без посредничества шлюза сигнализации. В этих условиях устройства, реализующие протокол MGCP, работают в режиме без сохранения данных о состояниях, т.е. устройствам не требуется конечный автомат для описания последовательности транзакций между Softswitch и транспортным шлюзом, и в них не сохраняется информация о предыдущих транзакциях. Сами шлюзы становятся не интеллектуальными устройствами, требуют меньшей производительности процессоров и меньших затрат на разработку. Кроме того, добавление новых

протоколов сигнализации или дополнительных услуг затрагивает только Softswitch, но не транспортные шлюзы.

Приведем более детальную классификацию транспортных шлюзов:

- *Trunking Gateway* – шлюз между ТфОП и IP-сетью, подключающийся к телефонной сети при помощи большего числа цифровых трактов (от 10 до нескольких тысяч) и системы сигнализации OKC7;
- *Voice over ATM Gateway* – шлюз между ТфОП и АТМ-сетью;
- *Residential Gateway* – шлюз, подключающий к IP-сети аналоговые устройства: кабельные модемы, линии xDSL и устройства беспроводного доступа; в большинстве случаев – синоним IAD;
- *Access Gateway* – шлюз с аналоговым или цифровым интерфейсом «пользователь — сеть»; часто используется для межсетевого доступа любого типа и для связи между равноправными сетями;
- *Business Gateway* – шлюз для подключения к IP-сети учрежденческой АТС при помощи, например, системы сигнализации DSS1.

Именно так классифицируются транспортные шлюзы рабочей группой Megaco, на подходы которой и будет ориентирован материал этой главы.

6.2. Эволюция протоколов управления шлюзами

Один из первых протоколов управления транспортными шлюзами был разработан компанией Telcordia, носившей тогда название Bellcore, и назывался *простым протоколом управления шлюзами SGCP (Simple Gateway Control Protocol)*. Фирма Level 3 разработала схожий *протокол управления оборудованием IDCP (IP Device Control Protocol)*, в ряде материалов именуемый также *IPDC (IP Device Control)*. Эти протоколы через год были объединены в *MGCP* (рис. 6.2).

Первая спецификация протокола MGCP приведена в документе RFC 2705, так и оставшимся информационным и не получившим силу стандарта. Причина заключается в том, что у него очень скоро появился преемник Megaco, хотя многие разработчики применяли MGCP при разработке своих изделий, предпочитая не дожидаться, когда появится Megaco/H.248.

Протокол Megaco/H.248 был разработан совместными усилиями IETF и исследовательской комиссии SG 16 ITU-T (International Telecommunication Union Telecommunication Standardization Sector).

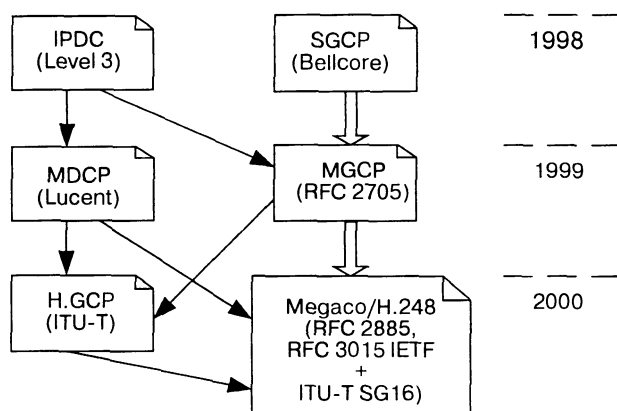


Рис. 6.2. Эволюция MGCP – Megaco/H.248

По этой причине у протокола Megaco/H.248 такое странное двойное название: в IETF он известен как Megaco (протокол управления транспортным шлюзом), а в ITU его называют H.248.

Первой публикацией Megaco/H.248 с элементами стандартизации протокола был проект RFC 2885. Впоследствии обнаружилось, что в этом проекте есть некоторые ошибки, и был подготовлен документ RFC 2886, перечисляющий опечатки и предлагающий соответствующие исправления. Затем доработанный исходный RFC был опубликован как RFC 3015, содержащий необходимые исправления RFC 2885 и ставший официальной версией 1 протокола Megaco.

Сегодня Megaco/H.248 можно считать преемником MGCP и основным протоколом управления транспортным шлюзом в оборудовании NGN. И все же, протокол MGCP еще встречается во многих реализациях транспортных шлюзов, поэтому начнем именно с него.

6.3. Протокол MGCP

6.3.1. Модель соединения

Для описания процесса обслуживания вызова с использованием протокола MGCP рабочей группой Megaco была разработана модель соединения (*Connection model*). Основой модели являются компоненты двух видов: *оконечные пункты*, называемые также английским термином *Endpoints*, и подключения – *Connections*.

Первый компонент, *Endpoints*, – это *оконечные пункты* (порты, *окончания*) оборудования, являющиеся источниками и/или приемниками информации. В их состав входят такие элементы, как

интерфейсы соединительных линий или интерфейсы линий услуг традиционной телефонии (POTS). Оконечные пункты находятся в транспортных шлюзах, и, в зависимости от типа оконечного пункта, могут каждый иметь или не иметь один или несколько внешних каналов или линейных интерфейсов. Например, оконечный пункт аналоговой линии может быть соединен с физической аналоговой линией, которая, в свою очередь, обычно подсоединена к обычному телефону. С другой стороны, существуют также оконечные пункты, не имеющие внешних соединений. Одним из примеров такого оконечного пункта является автоинформатор, который обычно интегрирован в шлюз. Другие объекты IP-сети могут соединяться с автоинформатором для получения речевых сообщений.

Подключение – это связь, устанавливаемая между оконечным пунктом и сеансом RTP/IP. Рассмотрим, например, оконечный пункт цифрового канала 64 Кбит/с (DS0). Если DS0 свободен, с этим оконечным пунктом не ассоциированы никакие соединения, а на IP-стороне шлюза ему не отведены никакие ресурсы. Однако когда DS0 используется для передачи разговорного трафика, оконечному пункту отводятся IP-ресурсы, и создается связь DS0 на линейной стороне шлюза с сеансом IP на IP-стороне шлюза. В терминологии MGCP эта связь и называется подключением. Если между собой связываются два оконечных пункта, используются два подключения. При этом связь между портами разных шлюзов через IP-сеть или связь между портами внутри одного шлюза является необходимым условием для организации сеанса связи, и называется соединением.

Коммутируемая связь в модели соединения является такой группой подключений, при которой ассоциированные с этими подключениями оконечные пункты могут передавать информацию друг другу и/или принимать информацию друг от друга. На рис. 6.3 представлены примеры использования этих двух компонентов. Отметим, что порты некоторых видов могут участвовать в нескольких подключениях одновременно. Рассмотрим представленные на рис. 6.3 порты (окончания) протокола MGCP. На рис. 6.3а показан *цифровой канал* 64 Кбит/с, который обычно бывает мультиплексированным в более производительном оборудовании передачи, например, в E1 (2.048 Мбит/с). В большинстве случаев по каналу DS0 передается речь, кодированная в соответствии с рекомендацией G.711. Иногда по цифровому каналу 64 Кбит/с может передаваться не речь, а сигнальные сообщения, как в D-канале ISDN. В таких случаях необходимо, чтобы принятая сигнальная информация проходила от транспортного шлюза к Call agent для обработки.

Аналоговая линия на рис. 6.3б представляет собой совокупность порта и стандартной телефонной линии, обеспечивающая обслуживание обычного телефона.

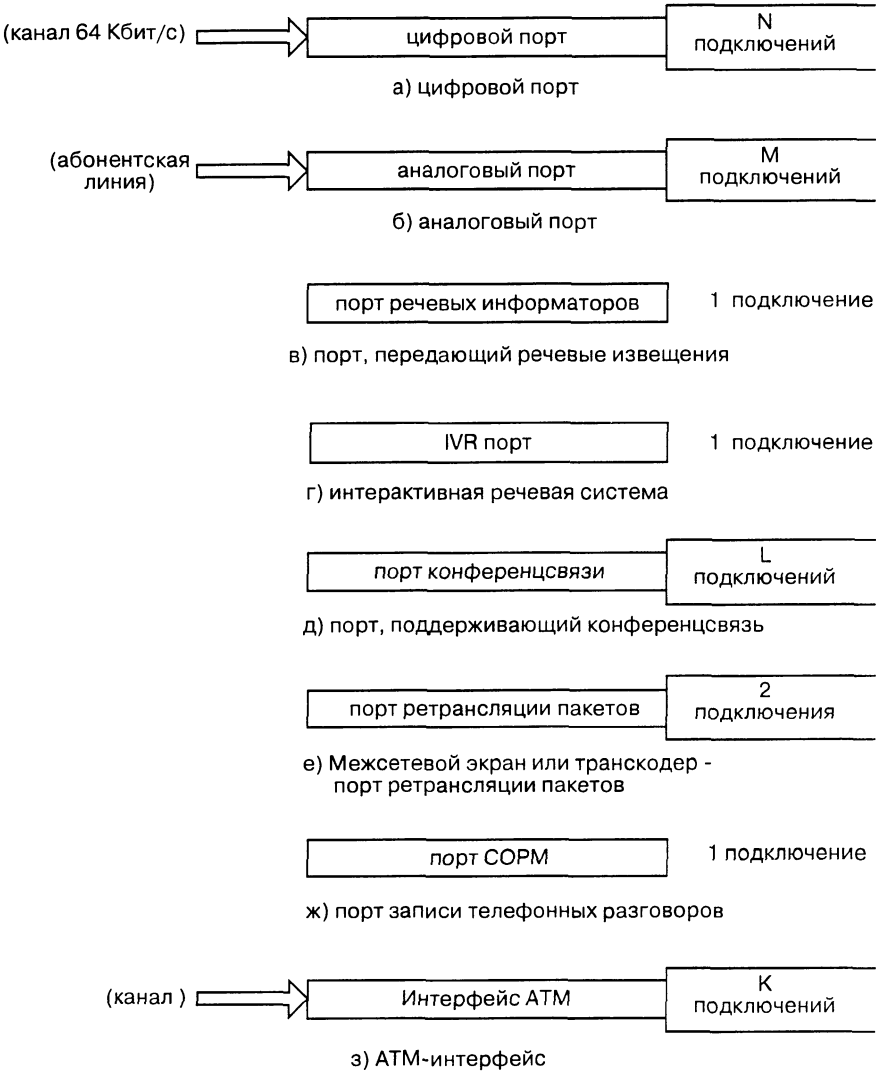


Рис. 6.3. Примеры использования компонентов модели

Среда, в которой работает аналоговая линия, – это, как правило, аналоговый речевой трафик, однако может быть и данными, кодированными с помощью модема. В последнем случае от шлюза требуется извлекать данные и пересылать их в виде пакетов IP. Порт на рис.6.3в обеспечивает доступ к единственному автоинформатору. Обычно соединение к оконечному пункту этого типа бывает односторонним, поскольку информацию необходимо передавать от автоинформатора, а не к нему. Предполагается, что сервер автоинформатора находится в сети IP, и с ним необходимо устанавли-

вать соединения на базе IP, в связи с чем конечный пункт не имеет никаких внешних коммутируемых каналов или линий.

Порт интерактивной речевой системы (IVR) на рис. 6.3г обеспечивает доступ к системе IVR, воспроизводящей приглашения или сообщения, причем ответы от слушателя могут влиять на воспроизведение.

Порт конференцсвязи на рис. 6.3д – окончание, в котором потоки информации от нескольких абонентов могут смешиваться, а результат – передаваться некоторым или всем участникам конференции.

Ретранслятор пакетов на рис. 6.3е – конференц-мост особого вида, поддерживающий только два подключения. Типичным примером служит межсетевой экран (брандмауэр) между открытой и защищенной сетью, когда медиа-поток проходит через такой ретранслятор (транскодер), а не непосредственно от конечного пункта одной сети к конечному пункту другой.

Через *порт доступа к СОРМ* на рис. 6.3ж устанавливается соединение с другим конечным пунктом для прослушивания информации, передаваемой или принимаемой на том конечном пункте. Соединения с пунктом доступа к перехвату бывают только односторонними.

Интерфейс АТМ на рис. 6.3з соответствует окончанию соединительной линии (виртуального канала) АТМ и используется в шлюзе, который обеспечивает сопряжение между сетью VoIP на одной стороне и сетью Voice over АТМ – на другой.

Каждый конечный пункт определяется идентификатором. Этот идентификатор содержит доменное имя шлюза, которому принадлежит пункт, и локальное имя в шлюзе. Локальное имя зависит от рассматриваемого шлюза, но обычно имеет иерархическую форму типа X/Y или X/Y/Z, где Y является логическим объектом X, а Z является логическим объектом Y. Примером может служить шлюз, который поддерживает несколько интерфейсов ЕЗ.

Если нужно идентифицировать единичный канал 64 Кбит/с в шлюзе, то следует идентифицировать конкретный ЕЗ (X), конкретный тракт Е1 в тракте ЕЗ (Y) и конкретный временной канал (Z) в тракте Е1.

Если нужно идентифицировать временной канал 64 Кбит/с номер 12 внутри тракта номер 6 из цифрового потока ЕЗ номер 3, то идентификатор может быть примерно таким: trunk3/6/12@gateway.niits.ru.

Для определенных компонентов идентификатора можно использовать групповой символ, подставляя \$ (в значении *любой*) или *

(в значении **все**). Таким образом, когда мы хотим сослаться на любой временной канал в пределах третьего E1 во втором E3 нашего примера, можно записать: *trunk2/3/\$@gateway.niits.ru*.

Этот способ использования групповых символов полезен, когда Softswitch хочет создать соединение с оконечным пунктом в шлюзе и ему безразлично, какой оконечный пункт используется. Благодаря подстановке символа \$ выбор оконечного пункта может быть оставлен самому шлюзу. С помощью символа * Call agent может приказывать шлюзу выполнить некоторое действие, связанное с номерами оконечных пунктов, как в случае, когда Call agent запрашивает статистическую информацию обо всех оконечных пунктах в шлюзе.

Подключения создаются устройством управления MGC для каждого порта, привлеченного к соединению, как это показано на рис. 6.4 .

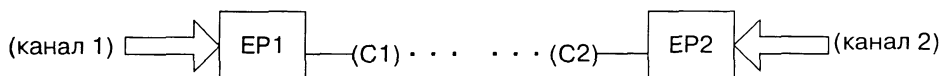


Рис. 6.4. Соединение в сети, построенной на базе протокола MGCP

6.3.2. Команды протокола MGCP

MGCP определяет девять команд, причем некоторые из них передаются от Softswitch в шлюз, а другие из шлюза в Softswitch. Команды протокола и их общее описание приводятся в табл. 6.1. Команда MGCP содержит командную строку, несколько строк параметров и, не обязательно, описание сеанса. Командная строка и параметры являются текстом, использующим набор символов ASCII. Во время установления, поддержания и разрушения соединения при помощи протокола MGCP устройство управления и шлюз обмениваются командами и ответами.

MGCP поддерживает концепцию инкапсуляции, при которой одна команда может быть включена в состав другой. Например, когда Softswitch передает к шлюзу команду создать соединение (команду CRCX), он может одновременно передать шлюзу команду уведомлять его об определенных событиях. Таким образом, мы можем встретить команду NotificationRequest, инкапсулированной в команду CreateConnection. Эта функциональная возможность особенно полезна в тех случаях, когда некоторое действие должно выполняться или событие следует обнаруживать только в сочетании с другими условиями. Например, Softswitch может потребовать от MG обнаружения и сообщения о тональных сигналах DTMF, но только при продолжении обслуживания вызова. В таком случае команда NotificationRequest, настраивающая шлюз на обнаружение тональ-

ных сигналов DTMF и сообщение об их содержании, могут быть инкапсулированы в команду CreateConnection, и обнаружение тонального сигнала будет происходить только в контексте созданного соединения. MGCP предусматривает только один уровень инкапсуляции. Иначе говоря, одна команда не может быть инкапсулирована в другую команду, если эта вторая команда уже инкапсулирована в третью команду. Однако MGCP позволяет передавать несколько команд одновременно в одном и том же пакете UDP.

Таблица 6.1. Команды протокола MGCP

Команда	Код	Направление передачи	Назначение
EndpointConfiguration (Конфигурация оконечного пункта)	EPCF	Softswitch → MG	Softswitch инструктирует шлюз, каким образом ему нужно обрабатывать получаемые речевые сигналы
CreateConnection (Создать подключение)	CRCX	Softswitch → MG	Softswitch дает указание шлюзу создать подключение
ModifyConnection (Модифицировать подключение)	MDCX	Softswitch → MG	Softswitch дает указание шлюзу изменить параметры существующего подключения
DeleteConnection (Разрушить подключение)	DLCX	Softswitch → MG, MG → Softswitch	Softswitch и шлюзы ликвидируют подключение
NotificationRequest (Запрос уведомления)	RQNT	Softswitch → MG	Softswitch инструктирует шлюз, какие события нужно обнаруживать и уведомлять о них
Notify (Уведомление)	NTFY	MG → Softswitch	Шлюз информирует Softswitch о том, что произошло событие из числа тех, которые были специфицированы в команде NotificationRequest
AuditEndpoint (Проверить порт)	AUEP	Softswitch → MG	Softswitch запрашивает информацию о каком-либо порте шлюза
AuditConnection (Проверить подключение)	AUCX	Softswitch → MG	Softswitch запрашивает параметры подключения
ReStartInProgress (Идет рестарт)	RSIP	MG → Softswitch	Шлюз информирует Softswitch о том, что один или несколько портов выводятся из рабочего состояния или возвращаются в рабочее состояние

Команда протокола MGCP обязательно содержит заголовок, за которым может следовать описание *сеанса связи* (*session description*). Заголовок команды и описание сеанса связи представляют собой набор текстовых строк. Описание сеанса отделено от заголовка команды пустой строкой. Заголовок содержит командную строку, например, вида *CRCX 1204 ts/1@skri.niits.ru MGCP 0.1*, и список параметров.

Как видно из примера, командная строка состоит из нескольких информационных полей. Первое поле – название команды – представлено в виде кода из четырех букв (табл. 6.1). Далее следует *идентификатор транзакции*.

Протокол MGCP предусматривает корреляцию команд и ответов: команда и ответ на нее образуют транзакцию, имеющую уникальный идентификатор *TransactionIdentifier*. Идентификатор транзакции включается в заголовок и команды, и ответа. Значения идентификаторов выбираются из диапазона чисел 1 – 999999999, причем значение идентификатора текущей транзакции всегда на единицу больше идентификатора предыдущей транзакции.

Идентификатор порта определяет тот порт, которому надлежит выполнить команду, за исключением команд *Notify* и *ReStartInProgress*, в которых идентификатор определяет порт, передавший команду. Идентификаторы портов кодируются таким же образом, как кодируются адреса электронной почты (в соответствии с RFC 821). Например, возможен идентификатор *ts/1@skri.niits.ru*, который идентифицирует первый порт (временной интервал) шлюза *skri*, расположенного в домене *niits*. Замыкает пример *версия протокола*, которая кодируется очевидным образом – MGCP 1.0.

Выше указывалось, что заголовок команды, кроме командной строки, содержит список параметров. Параметры команд протокола MGCP сведены в табл. 6.2. Каждый параметр идентифицируется кодом, который состоит из одной или двух заглавных букв. За кодом параметра следуют одно двоеточие, один символ пробела и значение параметра.

В некоторых случаях значение параметра может быть единой численной величиной. В других случаях значение параметра может быть единой шестнадцатеричной строкой. Еще в ряде случаев оно может быть списком разделенных запятыми значений или включать в себя список субполей. Один и тот же набор параметров допускается для использования и в командах, и в ответах.

Не все параметры, приведенные в таблице, должны обязательно присутствовать во всех командах протокола MGCP, спецификации включают в себя таблицу возможных комбинаций параметров в командах MGCP (обязательное присутствие параметра в команде – M, необязательное присутствие – O, запрет присутствия параметра – F).

Таблица 6.2. Параметры команд протокола MGCP

Название параметра	Код	Описание и значение параметра
ResponseAck (Подтверждение транзакции)	K	Подтверждает завершение одной или нескольких транзакций. Например, параметр K: 6234-6255, 6257, 19030-19044 подтверждает завершение транзакций, имеющих идентификаторы с 6234 по 6255, 6257 и с 19030 по 19044
BearerInformation (Сведения о доставке информации)	B	Служит для передачи сведений о законе кодирования речевой информации – A или µ
ReasonCode (Код причины)		Определены следующие коды причины: 000 – нормальное состояние порта, передается только в ответе на запрос о состоянии порта 900 – неисправность порта 901 – порт выведен из обслуживания 902 – отказ на физическом уровне (например, потеря синхронизации)
CallID (Идентификатор сеанса связи)	C	Идентифицирует сеанс связи, в котором может использоваться одно или несколько соединений. Кодировается шестнадцатеричной последовательностью символов длиной не более 32 символов
ConnectionID (Идентификатор подключения)	I	Идентифицирует подключение данного порта к одному соединению, так как один порт может быть одновременно подключен к нескольким соединениям
NotifiedEntity (Уведомляемый объект)	N	Идентификатор объекта, к которому следует передавать уведомления об обнаруженных событиях. Если параметр отсутствует, порт сообщает об этом объекту, от которого была получена команда. Идентификатор объекта кодируется так же, как кодируются адреса электронной почты согласно RFC 821, например, MGCP@alex.niits.ru:5625 или Alex@[128.23.0.4]. При использовании IP-адреса, он должен быть заключен в квадратные скобки
RequestIdentifier (Идентификатор запроса)	X	Согласует требование уведомить о событии, полученное от Softswitch, с уведомлением, передаваемым шлюзом в команде Notify
LocalConnectionOptions (Параметры подключения порта к соединению)	L	Данные об алгоритме кодирования информации, о периоде пакетизации в мс, об используемой полосе пропускания в Кбит/с, о типе обслуживания, использовании эхокомпенсации и другие сведения. Передается от Softswitch к шлюзу, обычно в команде CRCX
ConnectionMode (Режим соединения)	M	Определены следующие режимы соединения: передача, прием, прием/передача, конференция, передача данных, отсутствие активности, петля, тест и другие режимы. Значение параметру присваивает Softswitch
RequestedEvents (Запрашиваемые события)	R	Список событий, о которых следует оповестить Softswitch, и действия шлюза при обнаружении события. Определены следующие действия: оповестить Softswitch о событии немедленно; ожидать дальнейших событий; если событием является прием сигнала DTMF, то накапливать цифры в соответствии с требованиями параметра DigitMap, в определенных ситуациях передавать в канал акустические или вызывные сигналы, обработать инкапсулированную команду Endpoint Configuration, игнорировать событие и др.

Окончание табл. 6.2.

Название параметра	Код	Описание и значение параметра
SignalRequests (Требование передать сигнал)	S	Специфицирует сигнал, который должен быть передан абоненту, например, акустический сигнал «Ответ станции»
DigitMap (План нумерации)	D	Специфицирует правила обработки сигналов DTMF. При накоплении количества цифр, указанного в параметре, шлюз должен передать их устройству управления
ObservedEvents (Обнаруженные события)	O	Список обнаруженных событий
ConnectionParameters (Параметры соединения)	P	Статистические данные о соединении, передаваемые шлюзом после его разрушения
SpecifiedEndPointID (Идентификатор порта)	Z	Идентификатор порта в формате RFC821, например, EndPoint@alex niits ru.1234
RequestedInfo (Запрашиваемая информация)	F	Описывает информацию, которую Softswitch запрашивает у шлюза, например, цифры номера вызываемого абонента, набранные вызывающим абонентом
QuarantineHandling (Карантинная обработка)	Q	Определяет правила обработки событий, которые были обнаружены до получения этой команды в период так называемого карантина (quarantine period), и о которых Softswitch еще не был оповещен
DetectEvents (Выявляемые события)	T	Перечень событий, которые окончательный пункт должен обнаруживать, а при их обнаружении – извещать об этом Softswitch
EventStates (Состояния, обусловленные событиями)	ES	Перечень состояний окончательного пункта, обусловленных, например, тем, что абонент снял или положил трубку, информация об этих состояниях должна передаваться к Softswitch в ответ на команду AuditEndpoint
RestartMethod (Метод рестарта)	RM	Способ индикации шлюзом вывода окончательного пункта из обслуживания или ввода его в обслуживание. Поддерживаются несколько вариантов рестарта «graceful», «forced», «restart», «disconnected» or «cancel-graceful»
RestartDelay (Задержка перезапуска)	RD	Определяет время в секундах. Если этот параметр отсутствует, задержка рестарта равна нулю. При получении от Softswitch требования о принудительном рестарте окончательного пункта команда выполняется незамедлительно
Capabilities (Функциональные возможности порта)	A	Softswitch запрашивает сведения о функциональных возможностях окончательного пункта. Эти возможности включают в себя: поддерживаемые алгоритмы кодирования, период пакетизации, полосу пропускания, эхокомпенсацию, подавление пауз речи, режимы соединения, тип обслуживания, совокупность событий и др.

6.3.3. Ответы на команды

На каждую команду MGCP передается ответ. Структура ответов на команды в протоколе MGCP идентична вышеописанной структуре самих команд. Строку ответа составляет код возврата, за которым следует идентификатор транзакции и, опционально, – фраза комментария или причины. Каждый из этих элементов отделен символом единичный пробел (SP), при этом строка ответа заканчивается символом возврат каретки/ перевод строки (CRLF). Коды возврата являются целыми числами и разделяются на следующие категории:

- 0XX (от 000 до 099) – ответ с подтверждением,
- 1XX (от 100 до 199) – предварительные ответы; окончательный ответ последует позже,
- 2XX (от 200 до 299) – команда успешно выполнена,
- 4XX (от 400 до 499) – отказ из-за случайной ошибки,
- 5XX (от 500 до 599) – отказ из-за постоянной ошибки,
- 8XX (от 800 до 899) – ответы с пакетной спецификой.

В табл. 6.3 приведены возможные варианты кода ответа на команды протокола MGCP.

Из представленного перечня кодов ответов видно, что ответ должен быть увязан с командой, на которую он отвечает. Поэтому идентификатор TransactionId появляется как в командах, так и в ответах. Ответ на команду должен использовать тот же самый TransactionId, что и вызвавшая ответ команда. Те же параметры, которые разрешено применять в командах MGCP, разрешено применять и в ответах MGCP. Однако разрешенное использование в ответах отличается от разрешенного использования в командах. Например, параметр LocalConnectionOptions является опциональным параметром в команде CRCX, но он запрещен в ответе на команду CRCX.

Основная роль ответов заключается в защите от ошибок протокола, конфигурации или функциональных ошибок. И, все же, на основании информации, предоставляемой кодами ошибок, невозможно реализовать осмысленный механизм диагностики. Для получения диагностической информации от шлюзов и портов шлюза нужны другие методы. Одним из них является использование протокола SNMP.

Таблица 6.3. Коды ответов на команды протокола MGCP

Код	Значение кода
100	Полученная команда обрабатывается, сообщение о выполнении команды будет передано позже
200	Полученная команда выполнена
250	Соединение разрушено
400	Транзакция не может быть выполнена из-за временной ошибки
401	Трубка телефона уже снята
402	Трубка телефона уже положена
403	Команда не может быть выполнена из-за отсутствия необходимых ресурсов
404	В настоящий момент отсутствует необходимая полоса пропускания
500	Команда не может быть выполнена, потому что порт неизвестен
501	Команда не может быть выполнена, потому что порт не готов к ее выполнению
502	Команда не может быть выполнена, потому что порт не имеет необходимой полосы пропускания
510	Команда не может быть выполнена из-за ошибки в протоколе
511	Команда не может быть выполнена, так как в ней содержится нераспознанное расширение
512	Команда не может быть выполнена, потому что шлюз не имеет средств детектирования одного из указанных в ней сигналов
513	Команда не может быть выполнена, потому что шлюз не имеет средств генерирования одного из запрашиваемых сигналов
514	Команда не может быть выполнена, потому что шлюз не может передать необходимое речевое уведомление или подсказку
515	Команда имеет некорректный идентификатор соединения, например, идентификатор уже завершенного соединения
516	Команда имеет некорректный идентификатор сеанса связи
517	Не поддерживаемый или некорректный режим
518	Не поддерживаемая или неизвестная совокупность сигналов или событий
519	Порт не имеет сведений о плане нумерации
520	Команда не может быть выполнена, потому что идет рестарт порта
521	Порт передан другому Call Agent
522	Нет такого события или сигнала
523	Неизвестное действие или неразрешенная комбинация действий
524	Внутреннее несоответствие в параметре LocalConnectionOptions
525	Неизвестное расширение параметра LocalConnectionOptions
526	Недостаточная полоса пропускания
527	Отсутствует параметр LocalConnectionOptions
528	Несовместимая версия протокола
529	Отказ в аппаратном обеспечении
530	Ошибка в сигнальном протоколе CAS
531	Отказ группы каналов или трактов
532	Не поддерживаемое значение(ия) в параметре LocalConnectionOptions
533	Ответ слишком большой
534	Неисправность согласования кодека
535	Период пакетизации не поддерживается
536	Неизвестный или не поддерживаемый параметр RestartMethod
537	Неизвестное или не поддерживаемое расширение плана нумерации
538	Ошибка параметра события/сигнала (отсутствует, ошибочный, не поддерживается, неизвестный и пр.)
539	Неверный или не поддерживаемый параметр команды
540	Превышен предел числа соединений в расчете на оконечный пункт
541	Неверный или не поддерживаемый параметр LocalConnectionOptions

6.3.4. Описание сеансов связи SDP

При установлении соединений Softswitch предоставляет портам шлюзов, участвующим в этих соединениях, необходимую информацию друг о друге – описание сеансов связи. Описание сеанса связи вводится в состав некоторых команд и ответов протокола MGCP и включает в себя IP-адрес, номер UDP/RTP-порта, указание вида информации и алгоритма ее кодирования информации, данные о периоде пакетизации и т.д. Синтаксис описания сеанса связи в протоколе MGCP соответствует синтаксису протокола SDP (Session Description Protocol), уже упоминавшегося в главе 4.

Рассмотрим синтаксис протокола SDP в части описания сеанса речевой связи. Для описания такого сеанса в протоколе предусмотрено несколько информационных полей:

- *версия протокола SDP* кодируется $v=0$;
- *IP-адрес шлюза* содержит IP-адрес, который будет использоваться для обмена пакетами RTP, причем если это поле включено в команды протокола MGCP, то оно означает адрес удаленного шлюза, а если поле включено в ответы, то – адрес шлюза, передающего ответ;
- *поле описания речевого канала* кодируется буквой «m» и содержит индикацию вида передаваемой или принимаемой информации (в нашем случае – речи), номер порта, используемого для приема RTP пакетов удаленным шлюзом (если поле описания речевого канала включено в команды MGCP) или локальным шлюзом (если это поле включено в ответы), индикацию использования протокола RTP для передачи речи и указание алгоритма кодирования речевой информации;
- *режим соединения* может быть одним из следующих: *sendonly* – шлюзу надлежит только передавать информацию, *recvonly* – шлюзу надлежит только принимать информацию, *sendrecv* – шлюзу надлежит передавать и принимать информацию, *inactive* – шлюз не должен ни передавать, ни принимать информацию, *loopback* – шлюз должен передавать принимаемую информацию в обратном направлении и *conttest* – шлюзу надлежит перевести порт в режим тестирования.

Кроме вышеуказанных полей, для описания сеанса речевой связи в протоколе SDP предусмотрено еще несколько необязательных информационных полей. Отметим, что если в команду или в ответ протокола MGCP включены описания нескольких сеансов связи, то они отделяются друг от друга строкой с указанием версии протокола SDP. Типичный пример описания сеанса речевой связи с использованием протокола SDP:

$v = 0$

$c = \text{IN IP4 212.18.62.1}$

$m = \text{audio 1234 RTP/AVP 0}$

Поясним приведенный пример: для описания сеанса связи используется протокол SDP, версия 0, в сети используется протокол IP, версия 4, IP адрес шлюза – 212.18.62.1, передается или принимается речевая информация, упакованная в пакеты RTP, номер порта RTP – 1234, алгоритм кодирования речи – G.711, закон μ .

Приведенное описание протокола MGCP сможет быть полезным читателю хотя бы для того, чтобы сравнить его с протоколом Megaco/H.248, речь о котором пойдет ниже.

6.4. Протокол Megaco/H.248

6.4.1. Особенности Megaco/H.248

Этот протокол известен в комитете IETF под названием Megaco (MEdia GAteway COntrol Protocol), а в Международном союзе электросвязи ITU – под названием H.248. Протокол Megaco/H.248 во многом архитектурно схож с MGCP. Подобно MGCP, он определяет транспортные шлюзы MG, которые преобразуют информацию из формата, принятого в одной сети, в формат, необходимый в другой сети, и контроллеры транспортных шлюзов MGC или Softswitch, которые управляют установлением соединений и их отменой в пределах шлюзов MG. Едва ли стоит удивляться сходству протоколов, учитывая тот факт, что оба они были разработаны с учетом аналогичного набора требований.

Для переноса сигнальных сообщений Megaco/H.248 может использоваться протокол UDP, протокол TCP, протокол SCTP или транспортная технология ATM. Поддержка для этих целей протокола UDP – обязательное требование только к контроллеру шлюзов, протокол TCP должен поддерживаться и контроллером, и транспортным шлюзом, а поддержка протокола SCTP, как и технологии ATM, является необязательной.

Еще одной особенностью протокола Megaco/H.248 является то, что сообщения этого протокола могут кодироваться двумя способами. Комитет IETF предложил *текстовый способ* кодирования сигнальной информации, а для описания сеанса связи предложил использовать протокол SDP. Кодирование текста пишется в соответствии с *формами Бэкуса-Наура ABNF (Augmented Backus-Naur Form)*, описанными одним из авторов в главе 2 книги [4]. В свою очередь, ITU-T предусматривает бинарный способ представления сигнальной информации на *языке ASN.1 (Abstract Syntax Notation One)*, рассмотренным в рекомендации ITU-T X.680 от 1997 года,

а для описания сеансов связи рекомендует специальный инструмент – схему *TLV (тип-длина-значение)*, подробно обсуждавшуюся авторами в их предыдущей книге [3].

В результате, спецификация Megaco/H.248 написана таким образом, что обеспечивает как кодирование текста, так и двоичное кодирование протокола, нивелирует различие между IETF, который обычно использует ABNF, и ITU, где выбран формат ASN.1. Вопрос о том, является ли текстовый протокол лучшим решением, чем протокол сигнализации в виде машинных кодов (или наоборот), в процессе разработки протокола решен не был. Сегодня H.248/Megaco поддерживает оба варианта и рекомендует, чтобы при реализации Softswitch использовались и тот, и другой вариант протокола, а при реализации транспортных шлюзов или *устройств интегрированного доступа IAD* может быть выбран любой предпочтительный для разработчика вариант.

В настоящий момент еще нет информации, достаточной для того, чтобы уверенно сказать, какой вариант (двоичный или текстовый) будет преобладать в реализациях систем. Однако поскольку протокол Megaco предназначен заменить реализации на базе протокола MGCP, которые являются текстовыми, ожидается, что это обстоятельство окажет сильное влияние. В этой книге в примерах, иллюстрирующих использование Megaco, для представления сообщений применяется форма синтаксиса ASN.1.

Между протоколами MGCP и Megaco/H.248 много общего и помимо сходства их архитектуры. Оба протокола работают по принципу «ведущий-ведомый», при котором Softswitch управляет транспортным шлюзом и его портами через запросы включения питания, уведомления о событиях, генерации сигналов, передаваемых к порту, а также установлением и разрушением сигнального соединения путем создания и ликвидации логических соединений между портами.

И все же, при всех общих чертах, присущих этим двум протоколам, синтаксис команд и ответов на команды в протоколах MGCP и Megaco абсолютно разный. Кодирование и условные обозначения событий и сигналов, а также модель обслуживания вызовов имеют ряд различий.

6.4.2. Модель обслуживания вызова

Описание алгоритма установления соединения с использованием протокола Megaco опирается на модель процесса обслуживания вызова, отличную от рассмотренной в предыдущем параграфе модели MGCP. В своей модели процесса обслуживания вызова протокол Megaco оперирует двумя логическими объектами: *окончание или порт (termination)* и *контекст (context)*. Мы можем рассматривать окончание (порт) как логический объект транспортного шлюза

или IAD, который может являться источником и приемником мультимедийной информации, во многом аналогичным порту (endpoint) протокола MGCP. Контекст – это отображение логической связи между несколькими портами; например, все порты, участвующие в конференции, составляют единый контекст, т.е. находятся внутри одного контекста. Таким образом, контекст является абстрактным представлением более высокого уровня, чем MGCP, и в некотором смысле, включает в себя понятие «сеанс связи». Как мы увидим, в алгоритме установления соединения с помощью протокола Megaco, предназначенного для шлюза типа Residential Gateway, порт (окончание), соответствующий физическому устройству (например, телефонному аппарату), входит в тот же контекст, что и логическое RTP-соединение, для того чтобы обеспечить отображение двусторонней мультимедийной связи. Контекст имеет локальное значение, т.е. действителен для одного транспортного шлюза. Существует особый вид контекста – нулевой (null). В него по умолчанию входят все порты, которые не связаны ни между собой, ни с другими портами.

6.4.3. Окончания

Окончания (Terminations), называемые иногда, для простоты, *портами*, являются источниками и приемниками медиаинформации и, одновременно, логическими объектами транспортного шлюза. Можно выделить два вида окончаний в зависимости от того, какой они представляют интерфейс – физический или виртуальный.

Физические окончания аналогичны полупостоянным соединениям в традиционной телефонии и существуют с момента конфигурации шлюза. Это – аналоговые телефонные интерфейсы оборудования, поддерживающие одно телефонное соединение, или цифровые телефонные каналы.

Виртуальные окончания существуют только в течение разговора, являются интерфейсами со стороны IP-сети (например, RTP-окончания), через которые ведутся передача и прием пакетов. Виртуальные окончания создаются шлюзом при получении от Softswitch команды *Add* и ликвидируются при получении команды *Subtract*, тогда как физические окончания при получении команды *Add* или *Subtract*, соответственно, выводятся из нулевого контекста или возвращаются обратно в нулевой контекст.

Окончания имеют различные свойства. Очевидно, например, что подключенное к аналоговой линии окончание имеет не такие характеристики, как окончание, подключенное к цифровому каналу 64 Кбит/с. Свойства окончания определяются набором дескрипторов, включаемых в состав команд Megaco, что позволяет изменять свойства оконечных устройств в соответствии с указаниями, передаваемыми из Softswitch в MG.

Соответственно, каждое окончание имеет уникальный идентификатор *TerminationID*, который назначается шлюзом при конфигурации порта. Идентификаторы физических окончаний формируются непосредственно в транспортном шлюзе. Например, идентификатором порта может служить номер тракта E1 и номер временного канала внутри тракта. Иногда команды могут относиться ко всему шлюзу, тогда используется общий идентификатор окончаний *Root*. Используется также и механизм групповых символов *wildcard*: *ALL* и *CHOOSE*. Первый позволяет адресоваться к нескольким окончаниям одновременно, а второй – предоставить шлюзу право выбора подходящего окончания. К тому же, окончания обладают рядом изначальных свойств (*properties*), каждое из которых тоже имеет уникальный идентификатор *propertyID*. Например, окончания могут обладать способностью генерировать речевые подсказки, акустические и вызывные сигналы, а также выявлять сигналы DTMF. Некоторые свойства окончаний присваиваются им по умолчанию при создании, а при помощи команд протокола Megaco/H.248 эти свойства можно изменять. Описанию команд посвящен п. 6.4.5 этого параграфа. Сами свойства окончаний определяются включаемыми в команды Megaco/H.248 дескрипторами, которые описываются в п. 6.4.6. Окончания, как только что упоминалось, могут генерировать и передавать сигналы и быть запрограммированы на обнаружение событий, при возникновении которых транспортный шлюз должен будет передать извещение к Softswitch или выполнить определенные действия. В окончании могут накапливаться статистические данные и потом передаваться по запросу и/или при удалении окончания из контекста.

6.4.4. Контекст

Контекст (Context) представляет собой отображение связи между несколькими окончаниями, то есть абстрактное представление соединения двух или более портов одного шлюза. Окончания могут быть добавлены к контексту, удалены из контекста или перемещены из одного контекста в другой. В любой момент времени окончание может существовать только в одном контексте, который имеет свой уникальный идентификатор, и окончания могут обмениваться информацией, только находясь в одном и том же контексте.

Существует особый вид контекста – нулевой. Все окончания, входящие в нулевой контекст, не связаны ни между собой, ни с другими портами. Для рассматриваемой модели обслуживания вызовов окончание в нулевом контексте является абстрактным представлением свободного (не занятого) канала. В общем случае для присоединения окончания к контексту служит команда *Add*. Если команда *Add* не указывает контекст, в который должно быть добавлено окончание, в результате выполнения команды *Add* создается новый контекст. Это единственный механизм для создания нового контекста. Окончание

переводится из одного контекста в другой с помощью команды **Move**, а удаляется из контекста с помощью команды **Subtract**. Если в результате выполнения команды **Subtract** из контекста удаляется последнее окончание, этот контекст стирается.

Атрибутами контекста являются: идентификатор контекста **ContextID**, топология контекста (кто кому передает и от кого принимает информацию), приоритет (один из 16 уровней), индикатор «аварийного вызова» (высший приоритет в обслуживании). Протокол имеет средства, чтобы управлять параметрами контекста.

6.4.5. Команды

Megaco/H.248 определяет восемь команд, которые обеспечивают возможность управлять и манипулировать контекстами и окончаниями. Большинство команд предназначено для того, чтобы передаваться из **Softswitch** в транспортные шлюзы **MG**, за исключением команд **Notify** и **ServiceChange**. Рассмотрим эти 8 команд подробнее.

Команда **Add** (добавить). С ее помощью **Softswitch** дает указание шлюзу добавить окончание к контексту. Если команда **Add** не указывает контекст, куда добавляется окончание, то создается новый контекст. Если в команде не указан определенный **TerminationID**, а использован символ группового выбора (\$), **MG** создаст новое виртуальное окончание и добавит его в контекст.

Командой **Modify** (изменить) **Softswitch** дает указание шлюзу изменить свойства окончания. Команда **Modify** изменяет значения свойств окончания, приказывает окончанию отправить один или несколько сигналов или обнаруживать определенные события и докладывать о них.

Команда **Subtract** (исключить) удаляет окончание из контекста. Ответ на команду может содержать статистические данные, относящиеся к участию окончания в контексте. Эти данные зависят от типа окончного устройства. Для окончания **RTP**-статистические данные могут включать в себя сведения о переданных пакетах, о полученных пакетах, о джиттере и т.п. В этом отношении команда **Subtract** аналогична команде **DLCX** протокола **MGCP**.

Команда **Move** (переместить) перемещает окончание из одного контекста в другой. Она не используется для перемещения окончания из нулевого контекста или в него, поскольку эти операции должны выполняться командами **Add** и **Subtract**, соответственно. Возможность перемещать окончание из одного контекста в другой – это полезный инструмент для реализации услуги «вызов с ожиданием».

Команда **AuditValue** (проверить значение) используется Softswitch для поиска текущих значений свойств, событий и сигналов, ассоциированных с одним или несколькими окончаниями.

Команда **AuditCapabilities** (проверить возможности) используется Softswitch для поиска возможных значений свойств, событий и сигналов, ассоциированных с одним или несколькими окончаниями. На первый взгляд, эта команда может показаться очень похожей на команду AuditValue. Разница между ними заключается в том, что команда AuditValue используется для определения текущего состояния окончания, в то время как команда AuditCapabilities позволяет определять состояния, которые окончание может принимать. Например, AuditValue будет указывать любые сигналы, подаваемые окончанием в данный момент, а AuditCapabilities может указать все возможные сигналы, которые окончание может подавать в случае необходимости.

Команда **Notify** (уведомить) передается MG для того, чтобы информировать Softswitch о событиях, которые произошли в транспортном шлюзе. По поводу событий, о которых необходимо сообщать, обычно предварительно приходит запрос в составе команды из Softswitch в MG, например, в команде Modify. События, о которых сообщается, обычно сопровождаются параметром RequestedID, чтобы Softswitch мог увязать эти события с ранее переданными запросами.

Команда **ServiceChange** (изменение обслуживания) позволяет MG информировать Softswitch о предстоящем выводе из обслуживания или возврате в обслуживание группы окончаний. Команда используется также в ситуации, когда Softswitch передает управление некоторым транспортным шлюзом другому Softswitch. В этом случае команда сначала передается из Softswitch в MG, чтобы инициировать передачу управления, а затем MG передает команду ServiceChange в новый Softswitch для установления новых взаимоотношений.

6.4.6. Deskрипторы

Megaco/H.248 определяет ряд дескрипторов, предназначенных для использования вместе с командами и ответами. Эти дескрипторы образуют параметры команды и/или ответа и содержат дополнительную информацию об их свойствах. В зависимости от команды или ответа тот или иной дескриптор бывает обязательным, запрещенным или опциональным. В большинстве случаев, если дескриптор не является обязательным, он – опциональный. Случаев, когда дескриптор является запрещенным, относительно мало.

Общий формат дескриптора выглядит следующим образом:

Descriptorname=<someID>{parm=value, parm=value, ... }

Дескриптор модема, *Modem*, специфицирует тип модема и связанные с ним параметры, которые следует использовать в соединениях модема при передаче аудио, видео или данных. Определены следующие типы модемов: V.18 (текстовая телефония), V.22 (1200 б/с), V.22bis (2400 б/с), V.32 (9600 б/с), V.32bis (14400 б/с), V.34 (33600 б/с), V.90 (56 Кб/с), V.91 (64 Кб/с) и синхронная ISDN. По умолчанию окончание не имеет дескриптора модема. Иначе говоря, при начале работы окончания никакие свойства его модема не задаются. Они могут задаваться позже, в результате передачи команды Add или Modify из Softswitch в MG.

Дескриптор модема был включен в первую версию спецификации Megaco RFC 3015, а в синтаксис версии 2 он включен только затем, чтобы обеспечить обратную совместимость. Т.о., в следующих версиях протокола этот дескриптор не используется, и при приеме его необходимо игнорировать.

Дескриптор мультиплексирования, *Mux*, характеризует тип мультиплексирования в мультимедийном терминале. Протокол поддерживает типы мультиплексирования: H.211, H.223, H.226. V.76 и Nx64K.

Дескриптор среды, *Media*, описывает различные информационные потоки (медиа-потоки). Это – иерархический дескриптор в том отношении, что он содержит общий дескриптор, известный как *дескриптор состояния окончания*, который применим к окончанию в общем, и ряд дескрипторов потоков, применимых к каждому медиа-потoku отдельно. Кроме того, каждый дескриптор среды содержит до трех подчиненных дескрипторов, известных как *локальный дескриптор управления*, *локальный дескриптор* и *удаленный дескриптор*, соответственно. Иерархию этого типа можно представить следующим списком:

Дескриптор среды

Дескриптор потока

Локальный дескриптор управления

Локальный дескриптор

Удаленный дескриптор

Дескриптор состояния окончания, *TerminationState*, содержит сведения о двух характеристиках окончания: *ServiceStates* и *EventBufferControl*, а также сведения о ряде других характеристик, которые к медиа-потокам отношения не имеют.

Характеристика *ServiceStates* указывает, доступно ли окончание для использования. Она может иметь три значения: *тестирование*, *вне обслуживания* и *в обслуживании*. Значение *в обслуживании* не означает, что в данный момент окончание принимает участие в связи, а указывает, что окончание либо активно участвует в ней, либо может быть использовано для ее создания. Значение *в обслуживании* устанавливается по умолчанию.

Характеристика *EventBufferControl* указывает, следует ли сведения об обнаруженных окончанием событий помещать в буфер или их надо немедленно обрабатывать. Вначале окончание докладывает о событиях, извещение о которых заказал Softswitch с помощью команды, содержащей *EventsDescriptor*. Будет ли окончание фактически докладывать об указанных в *EventsDescriptor* событиях, зависит от того, установлена ли *EventBufferControl* в состояние *off* (выключено) или в состояние *lockstep* (жесткой конфигурации). Если установлено *off*, окончание немедленно доложит об обнаруженном событии. Если установлено *lockstep*, данные о событии будут помещены в буфер с дисциплиной FIFO (первым вошел, первым обслужен). Содержимое буфера проверяется при получении нового *EventsDescriptor*, указывающего, какие события должно обнаруживать окончание. Включение *EventBufferControl* в состав *TerminationStateDescriptor* позволяет Softswitch включать или выключать немедленное уведомление о событиях и не передавать каждый раз *EventsDescriptor* без необходимости.

Дескриптор состояния окончания является необязательным.

Дескрипторы потока, *Stream*. Поток определяется дескрипторами *LocalControlDescriptor*, *LocalDescriptor* *RemoteDescriptor* и идентифицируется с помощью *StreamID*. Значения *StreamID* используются между MG и Softswitch, чтобы указывать, какие медиа-потоки взаимосвязаны. В пределах одного контекста потоки с одним и тем же *StreamID* соединены. Поток создается определением в контексте нового *StreamID* в окончании. Поток удаляется с помощью установки пустого локального или удаленного дескриптора и установки значений *ReserveGroup* и *ReserveValue* в подчиненном *LocalControlDescriptor* в логическое значение *false*.

Дескриптор *LocalControlDescriptor* содержит сведения об особых характеристиках медиа-потока, в частности, о характеристиках *Mode*, *ReserveGroup* и *ReserveValue*.

Характеристика *Mode* (режим) может принимать одно из следующих значений: *только передача*, *только прием*, *передача/прием*, *неактивный* или *закольцован*. Направления передачи и приема определяются по отношению к внешней стороне контекста. Если установлен режим *только передача*, окончание может только передавать информацию в объекты за пределами контекста. Окончание не может пропускать информацию в другие логические объекты того же контекста. Если установлен режим *только прием*, окончание может только принимать информацию извне контекста и пропускать ее в другие окончания контекста, но не может принимать информацию от других окончаний и пропускать ее адресатам за пределами контекста. Когда Softswitch хочет добавить окончание в контекст, он может специфицировать набор вариантов для сеанса (используя

локальные и удаленные дескрипторы), которые Softswitch предпочитает для использования в MG, причем специфицирует их в порядке предпочтительности. MG не обязан выбрать первый из предлагаемых Softswitch вариантов, но может быть обязан резервировать ресурсы для сеанса, указанного Softswitch.

ReserveValue и *ReserveGroup* указывают, какие ресурсы должны быть резервированы для вариантов, специфицированных Softswitch в *LocalDescriptor* и *RemoteDescriptor*.

LocalDescriptor и *RemoteDescriptor* могут специфицировать несколько характеристик и/или групп характеристик. Например, описание SDP может указывать две группы характеристик: одну для G.711 A-закона и одну для G.729. Если логическое значение *ReserveGroup* равно *true* (истина), то MG должен резервировать ресурсы для одной из этих групп характеристик. *ReserveValue* используется аналогично, но применяется с целью резервирования ресурсов для одной определенной характеристики, а не для группы характеристик.

Дескрипторы *LocalDescriptor* и *RemoteDescriptor* содержат или не содержат несколько описаний сеансов SDP, описывающих сеанс на локальном и удаленном концах соединения, соответственно. Использование SDP согласно Megaco имеет некоторые отклонения от строгого синтаксиса SDP, как он специфицирован в документе RFC 2327. В частности, строки *s=*, *t=* и *o=* являются опциональными, знак группового выбора (\$) разрешен, допускается указывать несколько альтернативных значений параметра в тех местах, где обычно должно использоваться одно значение. И *LocalDescriptor*, и *RemoteDescriptor* могут содержать несколько описаний сеансов.

Дескриптор событий, *Events*, содержит *RequestIdentifier* и список событий, которые MG должен обнаруживать и про которые сообщать (переход в состояние трубка поднята, тональный сигнал факса и пр.). Назначение *RequestIdentifier* – увязывать запросы и последующие сообщения. Обычно сообщения об обнаруженных событиях немедленно передаются в Softswitch. Однако, в зависимости от значения *EventControlBuffer* (которое является специфицируемым в *TerminationStateDescriptor*), сведения о событиях могут и записываться в буфер. Когда события записываются в буфер, и затем о них должно сообщаться в Softswitch, то связанная с этими событиями информация хранится в *EventBufferDescriptor*.

Дескриптор сигналов, *Signals*, содержит список сигналов, которые должно подавать окончание. Сигналы могут подаваться только одному потоку или всем потокам в окончании. В состав типичных сигналов могут входить, например, такие подаваемые в абонентскую линию акустические сигналы, как ответ станции или контроль

посылки вызова. Существуют сигналы трех типов: *On/off* – сигнал остается включенным (*on*) до тех пор, пока явно не будет выключен (*off*), *Timeout* – сигнал сохраняется до тех пор, пока не истечет определенный период времени или пока не будет выключен еще до истечения заданного времени, *Краткий* – сигнал должен подаваться только на очень короткое время, как в случае многочастотных сигналов в соединительных линиях с сигнализацией R1.5. Дескриптор сигналов может включать в свой состав логическую последовательность сигналов, которые необходимо воспроизводить друг за другом.

Дескриптор проверки, *Audit Descriptor*, задает перечень информации, которую необходимо передавать из MG в Softswitch. Дескриптор проверки является просто списком других дескрипторов, которые должны переноситься в ответе. В их число могут входить дескрипторы: мультиплексирования, событий, сигналов, *ObservedEvents*, *DigitMap*, статистических данных и *EventBuffer*.

Дескриптор ServiceChangeDescriptor используется только в сочетании с командой *ServiceChange* и включает в себя такую информацию, как тип изменения обслуживания, которое произошло или должно произойти, причина изменения обслуживания и новый адрес для использования после изменения обслуживания.

Тип изменения обслуживания определяется параметром *ServiceChangeMethod*, который может принимать одно из следующих значений: *Graceful*, *Forced*, *Restart*, *Disconnected*, *Handoff*, *Failover* (постепенное, принудительное, перезапуск, отключено, передача управления, неисправность). *Graceful* указывает выведение окончаний из обслуживания после заданной задержки и без прерывания существующих соединений. *Forced* указывает внезапное, резкое выведение из обслуживания с потерей существующих соединений. *Restart* указывает, что восстановление обслуживания начнется после заданной задержки. *Disconnected* применяется ко всему MG и указывает, что соединение с Softswitch разрушено, но будет восстановлено. Softswitch может передавать команду *Audit* для проверки того, что характеристики окончного устройства не изменились за время потери контакта. *Handoff* передается из Softswitch в MG, чтобы указать, что Softswitch выводится из обслуживания и управление принимает новый Softswitch. Значение *Handoff* передается также из MG в новый Softswitch во время попытки установить контакт после приема *handoff* от предыдущего Softswitch. *Failover* передается из MG в Softswitch, если MG обнаружил неисправность и производится переключение на резервный MG.

Параметр *ServiceChangeDelay* определяет длительность используемой задержки в секундах. Его необходимо передавать, напри-

мер, в сочетании с изменением обслуживания типа Graceful. Если параметр отсутствует, или имеет значение ноль, задержки не происходит. В случае изменения обслуживания по типу Graceful нулевое значение указывает, что Softswitch должен ждать естественного удаления окончечных устройств из их контекста; т.е. ждать, когда сеансы связи с использованием указанных окончаний завершатся по инициативе их участников. Параметр ServiceChange Reason, как и следует из его названия, указывает причину изменения обслуживания.

Дескриптор DigitMap является описанием плана нумерации. Иначе говоря, DigitMap специфицирует множество разрешенных для набора комбинаций цифр. Оно хранится в MG, так что тот может передавать принятые цифры в Softswitch блоками, а не по одной. План нумерации может быть загружен в MG средствами эксплуатационного управления или из Softswitch по командам Megaco. Если план загружается из Softswitch, то чтобы переправить информацию, используется дескриптор DigitMap.

С точки зрения синтаксиса DigitMap является строкой или списком строк, причем каждая строка состоит из ряда символов, представляющих собой цифры от 0 до 9 и буквы от A до K. Букву X можно использовать как групповой символ, обозначающий любую цифру от 0 до 9, а символ «точка» (.) используется для указания нуля или нескольких повторений непосредственно предшествовавшей цифры или строки цифр. Этот символ можно использовать для указания номера с длиной, не определенной в плане нумерации. Кроме того, строка может содержать три символа, определяющих запуск таймера (T), короткого таймера (S) и длинного таймера (L). Чтобы понять назначение этих таймеров, рассмотрим, что происходит, когда абонент поднимает трубку обычного телефонного аппарата, чтобы вызвать станцию. АТС обнаруживает вызов, подает сигнал «Ответ станции» и готовится к приему первой цифры номера, включая таймер ожидания этой цифры (порядка 30 секунд). Если цифра не поступит в течение этого времени, АТС определит срабатывание таймера и передаст абоненту зуммер «Занято». Это – таймер T. Когда абонент начал набирать номер, запускается межцифровой таймер. Этот таймер бывает или коротким таймером S, или длинным таймером L, в зависимости от плана нумерации. Если абонент набрал некоторое количество цифр, а АТС нужно больше цифр для маршрутизации вызова, при ожидании следующей цифры обычно применяется короткий таймер. Кроме того, в АТС запускается таймер ограничения длительности непроизводительного занятия до момента получения сигнала «Ответ» от вызываемого абонента [t1], для чего применяется длинный таймер L.

Дескриптор StatisticsDescriptor содержит информацию, которая относится к использованию окончания в данном контексте.

Особенности статистических данных, которые должны передаваться по запросу, зависят от типа окончания. Строго говоря, этот дескриптор всегда является опциональным и может передаваться при удалении окончания из контекста по команде `Subtract` или в ответ на команду `AuditValue`.

Дескриптор `ObservedEvents` является обязательным параметром в команде `Notify`, где он используется для того, чтобы информировать `Softswitch` о событиях, которые были обнаружены. В большинстве остальных ответов на команды этот дескриптор является необязательным, кроме `ServiceChange`. При использовании в ответе на команду `AuditValue` он предназначен для передачи информации о событиях, которые записаны в буфере событий и еще не известны `Softswitch`. Дескриптор содержит `RequestIdentifier` со значением, которое согласовано с принятым в дескрипторе событий список таких событий, которые должны быть обнаружены в первую очередь. Этим обеспечивается увязка запрашиваемых данных о событиях и данных о событиях в сообщениях.

Дескриптор опционально допускает включение в него временных меток с указанием момента обнаружения каждого наблюдаемого события. Эта временная метка структурируется в виде `uuuymmddThhmmssss`, где записываются сотни секунд. Буква `T` отделяет год, месяц и день от часа, минуты и секунд. Сама временная метка отделяется от описания соответствующего события двоеточием.

Дескриптор `Error` передается в ответе, когда не может быть выполнена команда. Он может быть также включен в команду `Notify`, передаваемую из `MG` в `Softswitch`. Дескриптор ошибок состоит из кода ошибки и текстового описания ошибки, опционально сопровождающего этот код.

Дескриптор топологии `Topology` отличается от других дескрипторов в том смысле, что он соответствует только контексту, а не определенному окончанию в контексте. Назначение дескриптора – указать, как должны протекать в контексте медиа-поток, т.е. кто и кого должен слышать или видеть. По умолчанию все окончания в контексте могут передавать и принимать информацию друг от друга. Если желательна другая ситуация, то используется дескриптор топологии.

Дескриптор состоит из последовательности троек объектов вида *окончание1* – *окончание2* – *соединение*. Такая тройка указывает, существует или нет поток между двумя окончаниями (*isolate*), должен ли этот поток быть односторонним (*oneway*) или двусторонним (*bothway*). Порядок, в котором конечные устройства появляются в тройке, имеет значение: например, тройка *o1-o2-oneway* означает, что окончание1 может передавать информацию в окончание2, но окончание2 не может передавать информацию в окончание1.

Если в контексте используется более двух окончаний, то требуется более одной тройки. Например, если используется три окончных устройства (o1, o2 и o3), то в описании топологии нужны три тройки: для связи между o1 и o2, для связи между o1 и o3 и для связи между o2 и o3. Дескриптор топологии может быть полезным инструментом для реализации таких услуг как вызов с предварительным заказом или конференцсвязь с возможностью части ее участников провести отдельные разговоры перед возвращением в общую группу. По умолчанию характеристики всех дескрипторов, за исключением дескриптора состояния окончания и дескриптора локального управления, являются пустыми.

6.4.7. Транзакции

Команды, передаваемые между Softswitch и MG, группируются в структуры, которые устроены так, что за набором команд, относящихся к одному контексту, может следовать набор команд, относящихся к другому контексту. Сгруппированные команды передаются вместе в едином блоке TransactionRequest. Это можно представить так:

```
TransactionRequest (TransactionID {  
    ContextID1 {Command, Command, ... Command},  
    ContextID2 {Command, Command, ... Command},  
    ContextID3 {Command, Command, .. Command} } )
```

После приема TransactionRequest получатель выполняет вложенные команды. Команды выполняются последовательно, в том порядке, в каком они указаны в TransactionRequest. После выполнения всех команд передается ответ TransactionReply. Он имеет структуру, аналогичную структуре TransactionRequest в том смысле, что содержит несколько ответов для нескольких контекстов. TransactionReply можно представить так:

```
TransactionReply (TransactionID {  
    ContextID1 {Response, Response, ... Response },  
    ContextID2 { Response, Response, ... Response },  
    ContextID3 { Response, Response, ... Response } } )
```

Если получателю TransactionRequest потребуется некоторое время для выполнения запроса, он может передать отправителю этого запроса предварительный ответ, чтобы тот не считал запрос потерянным. Этот предварительный ответ TransactionPending извещает, что TransactionRequest принят и в данный момент обрабатывается. Такой ответ содержит принятый TransactionID без каких-либо параметров:

```
TransactionPending (TransactionID (.))
```

Параметр *normalMGExecutionTime* определяет интервал времени, в течение которого контроллер ожидает получение ответа от шлюза. Аналогичный параметр *normalSoftswitchExecutionTime* определяет время ожидания шлюзом ответа от контроллера.

Для ограничения времени ожидания используется пара параметров *MGOriGinatedPendingLimit* и *SoftswitchOriginatedPendingLimit*; она определяет предельно допустимое количество получаемых извещений *TransactionPending*. По достижении указанного предела передается либо ответ, либо извещение об ошибке транзакции.

6.4.8. Сообщения

Несколько транзакций протокола могут помещаться в *сообщение*. Сообщение снабжается заголовком, идентифицирующим отправителя. Идентификатором сообщения *MID (Message Identifier)* служит назначенное имя (например, доменный адрес/доменное имя/имя устройства) объекта, передающего сообщение. По умолчанию предлагается использовать доменное имя. Объекты протокола Megaco/H.248 (как MG, так и Softswitch) должны использовать один и тот же MID во всех создаваемых ими сообщениях в течение всего времени взаимодействия между ними. Каждое сообщение содержит номер версии протокола, создавшего сообщение. Для версии отводится два разряда. Текущая версия протокола – 2. Транзакции в пределах сообщения обрабатываются независимо. Порядок транзакций в сообщении не влияет на порядок, в котором их должен обрабатывать получатель сообщения. Заметим, что этот порядок отличается от порядка обработки команд в пределах транзакции, где очередность команд имеет значение.

Сообщение Megaco/H.248 – это, по сути, только транспортный механизм, в отличие от сообщений многих других сетевых протоколов. Общая структура сообщения представлена на рис. 6.5.

6.4.9. Наборы сигналов и событий

Шлюзы разных типов могут использовать окончания с сильно различающимися характеристиками. Чтобы обеспечить возможность взаимодействия MG и Softswitch, протокол Megaco определяет типовые *наборы (packages) характеристик, сигналов и событий* для Softswitch и шлюзов разных типов. Softswitch может запросить у шлюза сведения, необходимые, чтобы знать, с какими из таких наборов он может работать. Определяемые в наборе характеристики, события, сигналы или статистические данные, а также их параметры снабжаются идентификаторами. Для каждого набора идентификаторы перечисленных объектов имеют уникальные области имен, и в каждой из областей могут использоваться одинаковые идентификаторы, например, два идентификатора *propertyID* в разных наборах могут быть одинаковыми. Типовой набор характеризуется базовым описанием, свойствами, предусматриваемыми событиями, поддерживаемыми сигналами, предоставляемыми статистическими данными, годными для интерпретации и анализа, любыми процедурами, относящимися к надлежащей поддержке набора. Он содержит следующие разделы.

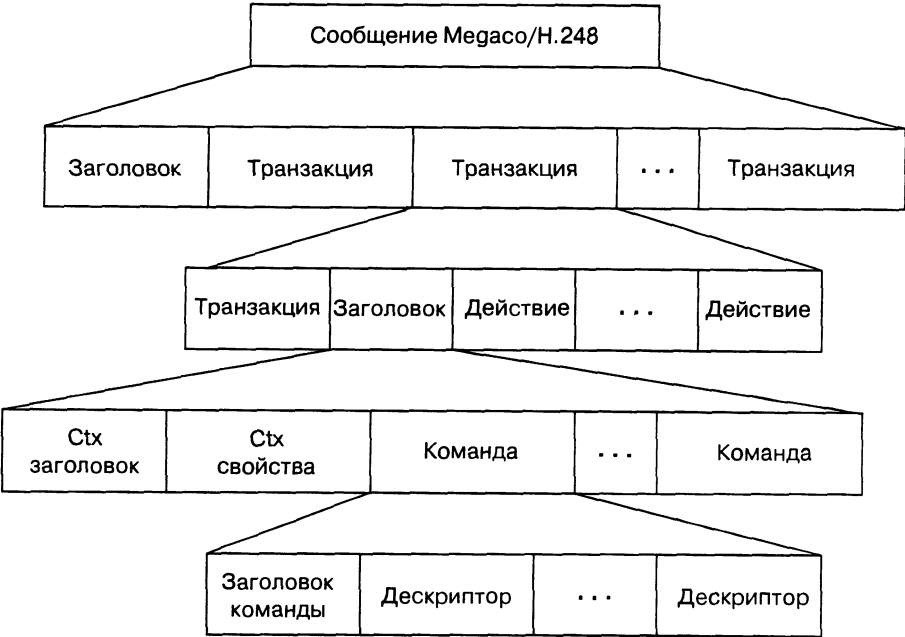


Рис. 6.5. Структура сообщений H.248/Megaco

Типовой набор характеризуется базовым описанием, свойствами, предусматриваемыми событиями, поддерживаемыми сигналами, предоставляемыми статистическими данными, годными для интерпретации и анализа, любыми процедурами, относящимися к надлежащей поддержке набора. Он содержит следующие разделы.

Раздел *Package* содержит общее описание набора, определяющее его имя, идентификатор (*PackageID*), текстовое описание, версию, и опциональные поля, определяющие, что набор предусматривает наличие расширения и/или что он сам является расширением уже существующего.

Раздел *Properties* определяет свойства (характеристики) набора и содержит имя каждого свойства, его идентификатор (*propertyID*), текстовое описание, тип (логическая переменная, символьная, целочисленная и т.д.), возможные значения, специфицирующие свойство и характеристики (*только чтение* или *только запись*, *чтение/запись*).

Раздел *Events* определяет события и содержит имя события, его идентификатор (*eventID*), текстовое описание, параметры дескриптора *Events* и параметры дескриптора *ObservedEvents*.

Раздел *Signals* определяет сигналы, имя и идентификатор каждого из них (*signalID*), его текстовое описание, тип (*on/off*, *timeout*, *brief*), продолжительность в сотых долях секунды и дополнительные параметры, которые мы опишем ниже.

Раздел *Statistics* определяет статистические данные, содержит имя и идентификатор данных каждого вида (*statisticID*), их текстовое описание, единицы измерения (т.е. миллисекунды, количество пакетов и т.д.).

Процедуры *Procedures* определяют дополнительные аспекты использования набора. *Параметры событий и сигналов* определяются именем параметра и его идентификатором (*parameterID*), типом (например, логическая, символьная или целочисленная переменная и т.д.), возможными значениями переменных, текстовыми описаниями. В базовой спецификации протокола Megaco/H.248 определены 13 типовых наборов, содержание которых сведено в табл. 6.4.

Таблица 6.4. Типовые наборы

Название набора	Описание
Общий (Generic) Идентификатор: g Пример синтаксиса: g/	События причина (<i>cause</i>) 1. NR – нормальное разъединение 2. UR – недоступны ресурсы 3. FT – временный отказ 4. FP – систематический (устойчивый) отказ 5. IW – ошибка взаимодействия 6. UN – не поддерживается Окончание сигнала (<i>sc</i>) 1. TO – истекла заданная выдержка времени 2. EV – прерван обнаруженным событием 3. SD – остановлен новым дескриптором сигнала 4. NC – не окончен по другой причине Общий набор не задает никаких характеристик, сигналов или видов статистических данных
Основной (Base Root) Идентификатор: root Пример синтаксиса: root/	Характеристики 1. MaxNrOfContexts (Максимальное число контекстов) 2. MaxTerminationsPerContext (Максимальное число портов на контекст) 3. NormalMGExecutionTime (Нормальное время работы MG на типовом этапе) 4. NormalSoftswitchExecutionTime (Нормальное время работы Softswitch на типовом этапе) 5. ProvisionalResponseTimerValue (Предварительное значение таймера ответа) В основном наборе отсутствуют процедуры, статистические данные, сигналы или события Все значения времени работы Softswitch на типовых этапах относятся к ответам на команды и к стандартному времени, требуемому контроллеру для ответа на команду В не масштабируемых платформах, которые не могут гарантировать независимость времени реакции системы от нагрузки, эти величины следует устанавливать очень тщательно

Продолжение табл. 6.4

Название набора	Описание
Набор для генератора тоновых сигналов (Tone Generator Package) Идентификатор: tonegen Пример синтаксиса: tonegen/	Сигналы 1. <i>pt (tl, ind)</i> определяет воспроизводимый тональный сигнал (характеристика сигнала, длительность паузы между сигналами). Не определено никаких характеристик, статистических данных, процедур или событий
Набор для детектора тоновых сигналов (Tone Detection Package) Идентификатор: tonedet Пример синтаксиса: tonedet/	События 1. <i>std (tl, tid)</i> – событие обнаружения начала сигнала Start Tone Detected (идентификатор сигнала) 2. <i>etd (tl, tid, dur)</i> – событие обнаружения конца сигнала End Tone Detected (идентификатор сигнала, длительность) 3. <i>ltd (tl, tid, dur)</i> – событие обнаружения длинного сигнала Long Tone Detected (идентификатор сигнала, длительность). Не определено никаких характеристик, сигналов, статистических данных или процедур. Набор полезен для обнаружения сигналов DTMF, а также сигналов, генерируемых факсимильными аппаратами и модемами
Базовый набор для генератора сигналов DTMF (Basic DTMF Generator Package) Идентификатор: dg Пример синтаксиса: dg/	Поддерживаемые сигналы Цифры DTMF 0-9, *, #, A-D. Кодирование, соответственно: d0-d9, ds, do, da-dd
Набор для детектора сигналов DTMF (DTMF Detection Package) Идентификатор: dd Пример синтаксиса: dd/	Цифры 0-9, A-F Кодирование, соответственно: d0-d9, da-df События Завершение плана нумерации (<i>ce</i>) Последовательность цифр (<i>ds</i>) Метод прекращения (<i>Meth</i>) UM – непротиворечивое соответствие PM – частичное соответствие FM – полное соответствие Отсутствуют характеристики, сигналы, статистика и процедуры
Набор для генератора акустических сигналов (Call Progress Tones Generator Package) Идентификатор: cg Пример синтаксиса: cg/	Сигналы 1. Ответ станции (<i>dt</i>) 2. КПВ (<i>rt</i>) 3. Зуммер «Занято» (<i>bt</i>) 4. Зуммер «Занято при перегрузке» (<i>ct</i>) 5. Указательный сигнал (<i>sit</i>) 6. Предупреждающий сигнал (<i>wt</i>) 7. Сигнал распознавания таксофона (<i>pt</i>) 8. Сигнал уведомления (<i>cw</i>) 9. Сигнал ожидания для вызывающего абонента (<i>cr</i>) Набор не определяет никаких характеристик, событий или статистических данных. Процедуры определены в E 180/Q.35

Окончание табл. 6.4

Название набора	Описание
Набор для контроля состояния аналоговых абонентских линий (Analog Line Supervision Package) Идентификатор: al Пример синтаксиса: al/	События 1. Трубка положена (<i>on</i>) 2. Трубка снята (<i>of</i>) 3. Калиброванный разрыв шлейфа (<i>fl</i>) Сигналы 1. Посылка вызова (<i>ri</i>) Не определено никаких свойств или статистики
Базовый набор для контроля целостности (Basic Continuity Package) Идентификатор: ct Пример синтаксиса: ct/	События 1. Завершение (<i>cmp</i>) 2. Результат (<i>res</i>) Сигналы 1. Сигнал контроля целостности (<i>ct</i>) 2. Ответный сигнал (<i>rsp</i>) Не определено никаких характеристик и статистических данных. Процедуры управляют взаимодействием контроллера (Softswitch) и транспортного шлюза для выбора метода контроля целостности соединения
Сетевой набор (Network Package) Идентификатор: nt Пример синтаксиса: nt/	Характеристики Максимальный размер джиттер-буфера (<i>jit</i>) События 1. Сетевой отказ (<i>netfail</i>) 2. Причина (<i>cs</i>) 3. Предупреждение об ухудшении качества (<i>qualert</i>) Статистические данные 1. Длительность соединения (<i>dur</i>) 2. Число переданных байтов (<i>oc</i>) 3. Число принятых байтов (<i>or</i>) Не определено никаких процедур или сигналов
Набор RTP (RTP Package) Идентификатор: rtп Пример синтаксиса: rtp	События 1. Передача полезной нагрузки (<i>pltrans</i>) Статистические данные 1. Число переданных пакетов 2. Число принятых пакетов 3. Коэффициент потерь пакетов 4. Джиттер 5. Задержка Не определено никаких процедур, сигналов и характеристик
Набор для каналов систем с временным уплотнением линий (TDM Circuit Package) Идентификатор: tdmc Пример синтаксиса: tdmc/	Свойства 1. Эхокомпенсация (<i>ec</i>) 2. Регулировка усиления (<i>gain</i>) Не определено никаких событий, сигналов, статистических данных или процедур

Наборы опций являются одним из способов расширения функциональных возможностей протокола. Все новые наборы, определяемые комитетом IETF, издаются в виде отдельных документов RFC, а наборы, определяемые ITU-T, – в виде соответствующих рекомендаций H.248.x.

6.5. Расширения Megaco/H.248

6.5.1. Развитие H.248

Рассмотрим расширения базовой версии протокола H.248, о которых говорилось в предыдущем разделе. На момент написания книги существовали следующие рекомендации.

- H.248.2 – в ней определяются наборы для факсимильной связи, для обмена текстовыми сообщениями и для услуги отклонения вызова с одного терминала на другой.
- H.248.3 – определяет элементы и действия в пользовательском интерфейсе. Могут регулироваться такие характеристики, как отображение текста, назначение клавиш и т.д.
- H.248.4 – определяет передачу сообщений H.248 поверх Stream Control Transmission Protocol (SCTP).
- H.248.5 – определяет передачу сообщений H.248 поверх ATM.
- H.248.6 – определяет набор, позволяющий динамически задавать тональные сигналы.
- H.248.7 – определяет набор общих извещений, позволяющий контроллеру управлять выдачей извещений шлюзом.
- H.248.8 – описывает коды ошибок и причины смены обслуживания.
- H.248.9 – определяет усовершенствованные наборы для медиа-сервера.
- H.248.10 – определяет набор средств обработки ситуаций соперничества за ресурсы.
- H.248.11 – определяет набор для управления при перегрузке MG.
- H.248.12 – определяет наборы для взаимодействия с сетями H.323 и H.324.
- H.248.13 – определяет набор, описывающий событие, которое MG использует для того чтобы указать контроллеру, что исчез аварийный сигнал недопустимого снижения качества в несущем канале.
- H.248.14 – определяет набор для таймера бездействия, позволяющего шлюзу обнаружить аварию в контроллере по отсутствию сообщений.
- H.248.15 – определяет новый атрибут SDP, позволяющий переносить свойства местного (local) и удаленного (remote) дескрипторов в текстовом кодировании H.248.
- H.248.16 – определяет усовершенствованные наборы функциональных средств и процедуры получения цифр номера.
- H.248.17 – определяет набор для проведения линейного теста.
- H.248.18 – определяет набор для поддержки множественных профилей.
- H.248.19 – определяет наборы для распределенного многоточечного управления, аудио- и видеоконференций, а также конференций с обменом данными.

- Н.248.20 – определяет использование местного (local) и удаленного (remote) дескрипторов с мультиплексированием Н.221 и Н.223.
- Н.248.21 – определяет набор для обслуживания полупостоянных соединений.
- Н.248.22 – определяет набор Shared Risk Group, позволяющий указать шлюзу, нужно или не нужно использовать при установлении соединений ресурсы, входящие в ту или иную группу равного риска. Группа равного риска – это группа ресурсов, имеющих одинаковую вероятность возникновения аварии.
- Н.248.23 – определяет усовершенствованные наборы для аварийных извещений.
- Н.248.24 – определяет наборы для многочастотного генератора и приемника.
- Н.248.25 – определяет базовый набор для систем сигнализации CAS.
- Н.248.26 – определяет усовершенствованные наборы для аналоговых линий связи.
- Н.248.27 – определяет наборы дополнительных тональных сигналов.
- Н.248.28 – определяет наборы для международных систем сигнализации CAS.
- Н.248.30 – определяет наборы расширенных метрик RTP.

6.5.2. Усовершенствования Megaco/Н.248

В IETF определен ряд дополнительных наборов сигналов и событий для поддержки услуг передачи в полосе тональных частот и расширенных услуг с помощью протокола Н.248/Megaco.

В табл. 6.5 описываются дополнительные наборы, их базовые возможности и базовый синтаксис. Наборы, в частности, обеспечивают обнаружение сигналов факсимильной, текст-телефонной и модемной связи. Этот аспект представляет большой интерес для правильного проектирования инфраструктуры сети IP-телефонии, которая должна поддерживать связь между рабочими станциями с качеством, по меньшей мере, не хуже, чем в сети ТФОП. По всем приведенным в табл. 6.5 наборам имеются соответствующие проекты RFC, выпущенные комитетом IETF.

6.6. Сценарий соединения между шлюзами

На рис. 6.6 приведен пример установления соединения с использованием протокола Megaco/Н.248 между двумя шлюзами типа Residential Gateway, управляемыми одним Softswitch. В этом

примере вызывающий шлюз MG1 имеет IP-адрес 212.86.42.1, адрес вызываемого шлюза MG2 – 218.68.122.41, адрес контроллера шлюзов Softswitch – 216.44.88.1. Порт для связи по протоколу Megaco для всех трех устройств по умолчанию имеет номер 55555.

Таблица 6.5. Дополнительные наборы

Набор	Возможности
Набор обнаружения тональных сигналов факсимильной/тексто-телефонной/модемной связи (FAX/Textphone/Modem Tones Detection Package) Идентификатор: ftmd Пример синтаксиса: ftmd/	Обеспечивает обнаружение тональных сигналов, передаваемых по стационарной телефонной линии, которые могут означать запрос перехода на один из режимов передачи данных, например на факсимильную или модемную связь. События: Те же, что и у набора для обнаружения тональных сигналов, с добавлением нового идентификатора сигнала (dtfm): tid=dtfm Поддерживаются основные тональные сигналы факсимильной связи, такие как CNG, V21, V23, V8bis, ANS, ANSAM, и т.д. Не определено никаких сигналов, статистики или процедур
Набор, позволяющий различать вызовы разного типа (Call Type Discrimination Package) Идентификатор: ctyp Пример синтаксиса: ctyp/	Позволяет установить, должен ли вызов обслуживаться как телефонный, факсимильный, тексто-телефонный или модемный, и выполняет начальное согласование режимов работы, параметров и т.д. Пример: <i>Ctyp/dtone{dt=cng}</i> (указывает на то, что обнаруженный сигнал – сигнал CNG)
Набор для текстовых телефонов (Text Telephone) Идентификатор: txp Пример синтаксиса: txp/	Обеспечивает связь с текстовыми телефонами. Пример: <i>txp/convmode=simultaneous</i> (разговорный режим — одновременная речевая связь и передача текста)
Набор для факсимильной связи (Fax) Идентификатор: fax Пример синтаксиса: fax/	Базовая факсимильная связь Пример: <i>fax/faxstate=prepare</i>
Набор для тексто-телефонной связи (Text Conversation) Идентификатор: txc Пример синтаксиса: txc/	Обеспечивает текстовую связь между терминалами разнородных сетей (текстовые телефоны имеются в одной из этих сетей, их поддерживает набор txp) Пример: <i>txc/bufftime=200</i> (время буферизации 200 мс)
Набор для факсимильной связи в IP-сетях (IP fax) Идентификатор: ipfax Пример синтаксиса: ipfax/	Факсимильная передача в IP-сетях с помощью процедур T.38 (в реальном времени) или T.37 (с промежуточной буферизацией). Пример: <i>ipfax/faxstate=negotiating</i>

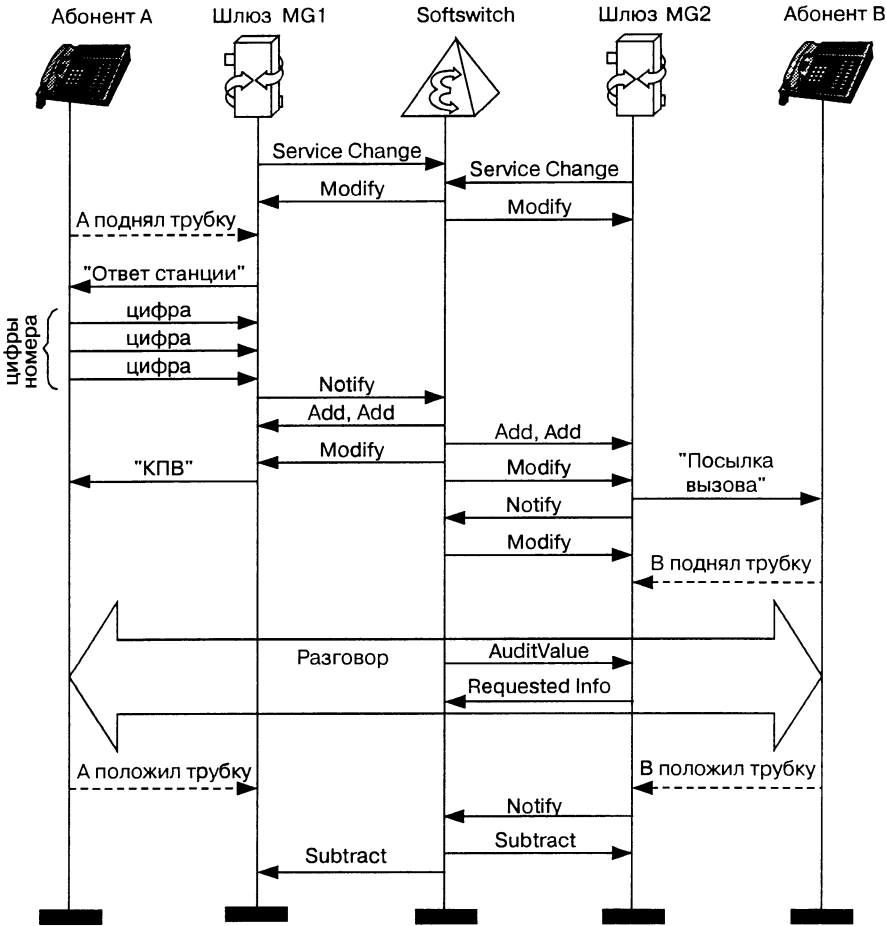


Рис. 6.6. Сценарий установления и разрушения соединения по протоколу Megaco/H.248

В самом начале шлюз MG1 регистрируется в Softswitch при помощи команды ServiceChange. Использование нулевого контекста означает, что порт в настоящий момент не участвует ни в каком соединении, а использование идентификатора порта ROOT означает, что команда относится ко всему шлюзу, а не к какому-нибудь определенному порту:

```
MG1 to Softswitch:
Megaco/1.0 [212.86.42.1]
Transaction = 9998 {
  Context = - {
    ServiceChange = ROOT {Services {
      Method=Restart, Port=55555, Profile=ResGW/1.0
    }
  }
}
```

```

}
Далее Softswitch подтверждает регистрацию шлюза:
Softswitch to MG1:
Megaco/1.0 [216.44.88.1]:55555
Reply = 9998 {
  Context = - {ServiceChange = ROOT { Services {
    Port=55555, Profile=ResGW/1.0}
  }
}
}

```

Шлюз имеет свободные аналоговые порты, которые должны быть запрограммированы для отслеживания изменения сопротивления абонентского шлейфа, когда абонент поднимет трубку, после чего шлюз должен передать абоненту акустический сигнал «Ответ станции».

Программирование производится при помощи команды Modify с соответствующими параметрами, причем программируется порт, находящийся в нулевом контексте. В команде указывается идентификатор порта (terminationId) – A4444, идентификатор информационного потока (streamId) – 1, транспортный адрес оборудования, передавшего команду – [216.44.88.1]:55555, специфицируется режим функционирования – дуплексный (SendReceive).

```

Softswitch to MG1:
Megaco/1.0 [216.44.88.1]:55555
Transaction = 9999 {
  Context = - {
    Modify = A4444 {
      Media {
        TerminationState {
          BufferedEventHandling{Step,Process}
        },
        Stream = 1 {
          LocalControl {
            Mode = SendReceive,
            g/GainControl=2, ; in dB,
            g/Encryption=xxx,
            g/EchoCancellation=G165,
            g/VoiceActDet=yes
          }
        }
      },
      Events = 2222 {glinesup/offhook}
    },
    Signals {g/PlayTone(tone=dialtone)}
  }
}
}

```

На этом же этапе в шлюз может быть загружен план нумерации в дескрипторе Digit Map. В этом случае, после того как абонент поднимет трубку, шлюз должен передать ему акустический сигнал «Ответ станции» и начинать прием сигналов DTMF в соответствии с планом нумерации. Однако в нашем примере план нумерации будет загружен только после того, как абонент поднимет трубку.

Шлюз MG1 подтверждает выполнение команды Modify:

```
MG1 to Softswitch:
Megaco/1.0 [212.86.42.1]:55555
Reply = 9999 {
    Context = - {Modify}
}
```

Аналогичным образом программируется аналоговый порт шлюза MG2, в нашем примере имеющий идентификатор A5555. Далее шлюз MG1 обнаруживает, что абонент А поднял трубку, и извещает об этом событии Softswitch при помощи команды Notify.

```
MG1 to Softswitch:
Megaco/1.0 [212.86.42.1]:55555
Transaction = 10000 {
    Context = - {
        Notify = A4444 {ObservedEvents =2222 {
            19990729T22000000:glinesup/offhook}}
    }
}
```

Softswitch подтверждает получение команды Notify:

```
Softswitch to MG1:
Megaco/1.0 [216.44.88.1]:55555
Reply = 10000 {
    Context = - {Notify}
}
```

На следующем шаге Softswitch дает шлюзу инструкцию накапливать цифры номера вызываемого абонента в соответствии с выбранным планом нумерации. Кроме того, после получения первой цифры номера необходимо остановить передачу акустического сигнала «Ответ станции».

```
Softswitch to MG1:
Megaco/1.0 [216.44.88.1]:55555
Transaction = 10001 {
    Context = - {
        Modify = A4444 {
            Events = 2223 {
                glinesup/onhook {
                    Action { DigitMap=Dialplan0 }
                }
            },
        },
    },
    Signals { g/StopTone},
    DigitMap= Dialplan0{
    (0T|00T|[17]xxx|8xxxxxxxx|#xxxxxxxx|*xx|91xxxxxxxxxxx|9011x.T)}
    }
}
```

Шлюз подтверждает получение и этой команды Modify:

```
MG1 to Softswitch:
Megaco/1.0 [212.86.42.1]:55555
Reply = 10001 {
    Context = - {Modify}
}
```

Цифры номера вызываемого абонента накапливаются шлюзом MG1, после чего они сравниваются с планом нумерации и передаются в Softswitch.

```

MG1 to Softswitch:
Megaco/1.0 [212.86.42.1]:55555
Transaction = 10002 {
  Context = - {
    Notify = A4444 {ObservedEvents =2223 {
      19990729T22010001:g/tonesdt{tones=«16135551212»}}}
  }
}

```

Полученное сообщение подтверждается шлюзом:

```

Softswitch to MG1:
Megaco/1.0 [216.44.88.1]:55555
Reply = 10002 {
  Context = - {Notify}
}

```

Далее Softswitch анализирует цифры номера вызываемого абонента, полученные от шлюза MG1, и определяет, что соединение должно проходить через шлюз MG2, к которому подключен вызываемый абонент. К вновь образованному контексту в шлюзе MG1 добавляются при помощи команды Add физическое окончание (аналоговый абонентский интерфейс) A4444 и виртуальный порт (RTP-порт). Так как в этот момент шлюз, к которому прикреплен вызывающий абонент, не имеет информации о шлюзе MG2 (такой как IP-адрес, номер RTP-порта и поддерживаемые алгоритмы декодирования принимаемой речевой информации), то контроллер Softswitch предписывает шлюзу MG1 только принимать информацию (режим ReceiveOnly). Кроме того, Softswitch специфицирует в команде Add предпочтительные для использования алгоритмы кодирования.

```

Softswitch to MG1:
Megaco/1.0 [216.44.88.1]:55555
Transaction = 10003 {
  Context = $ {
    Add = A4444 {
      Media {
        Stream = 1 {
          Events = 2224 {glinesup/onhook} }
        }
      },
    Add = $ {
      Media {
        Stream = 1 {
          LocalControl {
            Mode = ReceiveOnly,
            g/NetworkType = RTP/IP4, ;
            g/MaxJitterBuffer=40, ; in ms
            g/PreferredPacketization=30, ; in ms
            g/PreferredPacketization=30, ; in ms
            g/PreferredEncoders =[G723, PCMU],
            g/PreferredDecoders=[G723, PCMU],
            g/Gain=0 ; in dB
          }
        }
      }
    }
  }
}

```



```

        g/Gain=0 ; in dB
    },
    Remote=SDP{
v=0
c=IN IP4 212.86.42.1
m=audio 2222 RTP/AVP 4 0
a=sendrecv
    } ; RTP profile for G.723 is 4
    }
}
}
}

```

Создание контекста подтверждается, физический порт шлюза MG2 A5555 соединяется с UDP/RTP-портом, имеющим идентификатор A5556. Отметим, что RTP-порт имеет номер 1111, т.е. отличный от номера порта Megaco/H.248 – 55555.

MG2 to Softswitch:

```

Megaco/1.0 [212.86.42.1]:55555
Reply = 50003 {
    Context = 5000 {
Add,
Add = A5556{
    Media {
        Stream = 1 {
            Local = SDP {
v=0
c=IN IP4 218.68.122.411
m=audio 1111 RTP/AVP 4 0
a=sendreceive
        }
    } ; RTP profile for G723 is 4
    }
}
}
}
}

```

Контроллер предписывает шлюзу MG1 начать передачу вызывающему абоненту акустического сигнала контроля посылки вызова КПВ.

Softswitch to MG1:

```

Megaco/1.0 [216.44.88.1]:55555
Transaction = 10005 {
    Context = 2000 {
        Modify = A4444 {
            Signals {g/PlayTone{tone=ringback}}
        }
    }
}
}

```

Шлюз MG1 подтверждает передачу указанного акустического сигнала в порт A4444.

MG1 to Softswitch:

```

Megaco/1.0 [212.86.42.1]:55555
Reply = 10005 {
    Context = 2000 {Modify}
}

```

Контроллер Softswitch предписывает порту A5555 шлюза MG2 начать передачу вызывного сигнала.

Softswitch to MG2:

```
Megaco/1.0 [216.44.88.1]:55555
Transaction = 50004 {
  Context = 5000 {
    Modify = A5555 {
      Signals {glinesup/PlayTone{tone=ring}}
    }
  }
}
```

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

MG2 to Softswitch:

```
Megaco/1.0 [218.68.122.41]:55555
Reply = 50004 {
  Context = 5000 {Modify}
}
```

На этом этапе обоим абонентам, участвующим в соединении, посылаются соответствующие сигналы, и шлюз MG2 ждет, пока вызываемый абонент примет входящий вызов, после чего между двумя шлюзами будут организованы двунаправленные разговорные каналы.

Шлюз MG2 обнаружил, что вызываемый абонент поднял трубку, и извещает об этом контроллер Softswitch.

MG2 to Softswitch:

```
Megaco/1.0 [218.68.122.41]:55555
Transaction = 50005 {
  Context = 5000 {
    Notify = A5555 {ObservedEvents =1234 {
      19990729T22020002:glinesup/offhook}}
  }
}
```

Контроллер подтверждает получение команды Notify.

Softswitch to MG2:

```
Megaco/1.0 [216.44.88.1]:55555
Reply = 50005 {
  Context = - {Notify}
}
```

Далее контроллер Softswitch предписывает шлюзу MG2 прекратить передачу вызывного сигнала.

Softswitch to MG2:

```
Megaco/1.0 [216.44.88.1]:55555
Transaction = 50006 {
  Context = 5000 {
    Modify = A5555 {
      Events = 1235 {glinesup/onhook},
      Signals {g/StopTone} ; to turn off ringing
    }
  }
}
```

Шлюз MG2 подтверждает выполнение команды.

MG2 to Softswitch:

```
Megaco/1.0 [218.68.122.41]:55555
Reply = 50006 {
  Context = 5000 {Modify}
}
```

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

Softswitch to MG1:

```
Megaco/1.0 [216.44.88.1]:55555
Transaction = 10006 {
  Context = 2000 {
    Modify = A4445 {
      Media {
        Stream = 1 {
          LocalControl {
            Mode=SendReceive
          }
        }
      }
    },
    Modify = A4444 {
      Signals { g/StopTone}
    }
  }
}
```

Шлюз MG1 подтверждает выполнение команды.

MG1 to Softswitch:

```
Megaco/1.0 [212.86.42.1]:55555
Reply = 10006 {
  Context = 2000 {Modify, Modify}}
```

После этого начинается разговорная фаза соединения, в течение которой участники сеанса связи обмениваются речевой информацией. Следующим шагом контроллер Softswitch принимает решение проверить RTP-порт в шлюзе MG2.

Softswitch to MG2:

```
Megaco/1.0 [216.44.88.1]:55555
Transaction = 50007 {
  Context = - {AuditValue = A5556{
    Audit(Media, DigitMap, Events, Signals, Packages, Statistics )}
}
```

Шлюз MG2 выполняет команду. В ответе на команду AuditValue передается вся запрашиваемая информация, в том числе статистические данные, накопленные за время соединения. Кроме того, из ответа видно, что не произошло никаких событий и не передавалось никаких сигналов.

```

Megaco/1.0 [218.68.122.41]:55555
Reply = 50007 {
    Context = - {
        AuditValue {
            Media {
                TerminationState {
                    BufferedEventHandling{Process}
                },
                Stream = 1 {
                    LocalControl {
                        Mode = SendReceive,
                        g/MaxJitterBuffer=40, ; in ms
                        g/PreferredPacketization=30, ; in ms
                        g/PreferredEncoders=[G723, PCMU],
                        g/PreferredDecoders=[G723, PCMU],
                        g/Gain=0 ; in dB
                    },
                    Local = SDP {
v=0
c=IN IP4 218.68.122.41
m=audio 1111 RTP/AVP 4 0
a=sendrecv
                    },
                    Remote=SDP{
v=0
c=IN IP4 212.86.42.1
m=audio 2222 RTP/AVP 4 0
a=sendrecv
                    } ; RTP profile for G.723 is 4
                }
            },
        Packages {g, glinesup, RTPPkg},
        Statistics { RTPPkg/PacketsSent=1200,
                    RTPPkg/OctetsSent=62300,
                    RTPPkg/PacketsReceived=700,
                    RTPPkg/OctetsReceived=45100,
                    RTPPkg/PacketsLost=6,
                    RTPPkg/Jitter=20,
                    RTPPkg/AverageLatency=40 }
        }
    }
}

```

Вызываемый абонент первым разрушает связь, и шлюз MG2 извещает об этом Softswitch.

MG2 to Softswitch:

```

Megaco/1.0 [218.68.122.41]:55555
Transaction = 50008 {
    Context = 5000 {
        Notify = A5555 {ObservedEvents =1235 {
            19990729T24020002:glinesup/onhook}
        }
    }
}

```

Softswitch подтверждает получение сообщения Notify.

Softswitch to MG2:

```

Megaco/1.0 [216.44.88.1]:55555
Reply = 50008 {
    Context = - {Notify}
}

```

Получив информацию от любого из шлюзов о том, что один из абонентов положил трубку, Softswitch разрушает соединение. К обоим шлюзам передается команда Subtruct.

Алгоритм разрушения соединения предусматривает одинаковый обмен сигнальными сообщениями между контроллером и обоими шлюзами, поэтому здесь этот алгоритм рассматривается на примере шлюза MG2.

From Softswitch to MG2:

```
Megaco/1.0 [216.44.88.1]:55555
Transaction = 50009 {
  Context = 5000 {
    Subtract = A5555 {Audit{Statistics}},
    Subtract = A5556 {Audit{Statistics}}
  }
}
```

Каждый из портов шлюза MG2, участвующих в соединении (физический порт – A5555 и RTP-порт – A5556), передает статистические данные, накопленные за время соединения. В общем случае, Softswitch может запрашивать статистическую информацию только у одного из портов.

From MG2 to Softswitch:

```
Megaco/1.0 [218.68.122.41]:55555
Reply = 50009 {
  Context = 5000 {
    Subtract {
      Statistics { ; what are the stats for a TDM connection?
        TDMPkg/OctetsSent=45123,
        TDMPkg/Duration=40 ; in seconds
      }
    },
    Subtract {
      Statistics {
        RTPPkg/PacketsSent=1245,
        RTPPkg/OctetsSent=62345,
        RTPPkg/PacketsReceived=780,
        RTPPkg/OctetsReceived=45123,
        RTPPkg/PacketsLost=10,
        RTPPkg/Jitter=27,
        RTPPkg/AverageLatency=48
      }
    }
  }
}
```

После разрушения соединения Softswitch предписывает шлюзам MG1 и MG2 быть готовыми к тому, что кто-то из обслуживаемых ими абонентов поднимет трубку.

Отметим, что портам шлюза, отображаемым окончаниями в нулевом контексте, по умолчанию может быть предписано обнаруживать снятие трубки абонентом, при этом Softswitch не должен передавать шлюзам специальные команды, как это было в рассмотренном примере.

6.7. Сравнение протоколов VoIP

6.7.1. Megaco/H.248 и MGCP

О различиях Megaco/H.248 и MGCP уже говорилось выше в этой главе. Там отмечалось, что эти протоколы имеют различия в ряде областей. Прежде всего, Megaco имеет более общую модель обслуживания вызовов, что позволяет ему лучше работать с такими соединениями как TDM-TDM, TDM-ATM и TDM-IP, а также более гибко управлять конференциями. Еще одно различие касается транзакций. Megaco в транзакциях содержит команды отдельно друг от друга, в то время как MGCP позволяет использовать вложенные команды, что усложняет процесс поиска команды. Megaco может использовать в целях обеспечения безопасности заголовки аутентификации, которых нет у MGCP. Что касается мультимедиа, Megaco позволяет микшировать аудио/видео/данные и таким образом поддерживает мультимедийный трафик, а MGCP ориентирован только на поддержку аудиоинформации. Если шлюз обнаруживает аварию на управляющем им Softswitch, протокол Megaco позволяет назначить новый управляющий Softswitch при помощи команды ServiceChange. В MGCP это делается гораздо сложнее.

6.7.2. Megaco/H.248 и SIP

Megaco/H.248 и SIP не соперничают друг с другом, т.к. Megaco – это протокол, предназначенный для взаимодействия Softswitch и MG, а SIP – это протокол взаимодействия одноранговых устройств (Softswitch или SIP-phone). Взаимодействие транспортных шлюзов ограничено областью одного домена, т.к. они контролируются одним Softswitch. Таким образом, мы можем сказать, что Megaco не определяет систему связи целиком, ему нужен протокол для взаимодействия Softswitch, которым может быть SIP.

6.7.3. Megaco/H.248 и H.323

Как и SIP, протокол H.323 может дополнять Megaco/H.248, поскольку тоже является протоколом, обеспечивающим взаимодействие одноранговых устройств. В таком случае Megaco/H.248 позволит H.323 избавиться от присущих ему проблем с масштабируемостью, доступностью и возможностью взаимодействовать с ОКС7. В этих условиях H.323 будет протоколом терминалов для взаимодействия друг с другом и с сетью, а Megaco/H.248 будет использоваться привратниками для управления большими шлюзами, обеспечивающими взаимодействие IP-сети, построенной согласно H.323, с сетью ТфОП.

Глава 7

Группа Sigtran

*Не меняются только самые мудрые и самые глупые
Конфуций*

7.1. Система общеканальной сигнализации №7 в IP-сети

Речь в главе идет, разумеется, о первой из двух групп, указанных в приведенном в качестве эпиграфа изречении. Действительно, последняя и лучшая из двух региональных (R1 и R2) и семи международных систем сигнализации, стандартизованных МККТТ, – система общеканальной сигнализации №7 (ОКС7) – оказалась чрезвычайно удачной. Только мудростью разработчиков ОКС7 и созданной ими архитектурой стека протоколов ISUP, MAP, INAP, TCAP, SCCP, MTP 1, 2, 3 и др. можно объяснить долгую жизнь и сохраняющуюся перспективность этой системы сигнализации. И в сегодняшнем инфокоммуникационном мире, революционно изменяющемся в процессе конвергенции, роль ОКС7 практически не меняется.

Именно поэтому в рамках IETF и была создана *рабочая группа Sigtran (IETF SigTran Working Group)*, предназначенная для исследования транспортировки сигнальной информации ОКС7 в сетях IP и взаимодействия с другими сетями, в частности, ТфОП. С момента первого своего заседания в Орландо в 1998 этой рабочей группе удалось создать достаточно полную архитектуру ОКС7 (и не только ОКС7) поверх IP. Прежде чем приступить к ее обсуждению в этой книге, читателю, не знакомому со стеком протоколов ОКС7, было бы очень полезно пролистать параграф 8.4 учебника [6], или главу 10 книги [4], или более подробные источники [12].

Чтобы прояснить взаимодействие ОКС7 с протоколами сигнализации, описанными в предыдущих главах, рассмотрим в качестве примера сценарий на рис. 7.1, являющийся расширением сценария, изображенного на рис. 6.6 предыдущей главы. В этом

сценарии уже два Softswitch связываются друг с другом по протоколу SIP (глава 4) и управляют соответствующими транспортными шлюзами MG по протоколу Megaco (глава 6). Шлюзы сигнализации соединяют Softswitch непосредственно с пунктами сигнализации SP или транзитными пунктами сигнализации STP сети ОКС7. Поскольку Softswitch управляют обслуживанием вызовов в своих сетях, преобразованные в SG сигнальные сообщения ISUP направляются в Softswitch.

Пересылка сигнальной информации ISUP от SP/STP к SG и от SG к SP/STP помечается на рис. 7.1 как ISUP (в трактовке [®]_{ITU-T}), а пересылка той же сигнальной информации от SG к Softswitch или от Softswitch к SG помечается как принадлежащая IP, т.е. [®]_{Sigtran}. Содержание сообщений при этом не изменяется, а единственное отличие состоит в том, что сообщения ISUP передаются к Softswitch и от него поверх IP, а не поверх стандартного протокола MTP (Message Transfer Part) стека ОКС7. Таким образом, все, что делает SG, – это получает сообщение ISUP из сети ОКС7 и доставляет его к соответствующему объекту в сети IP.

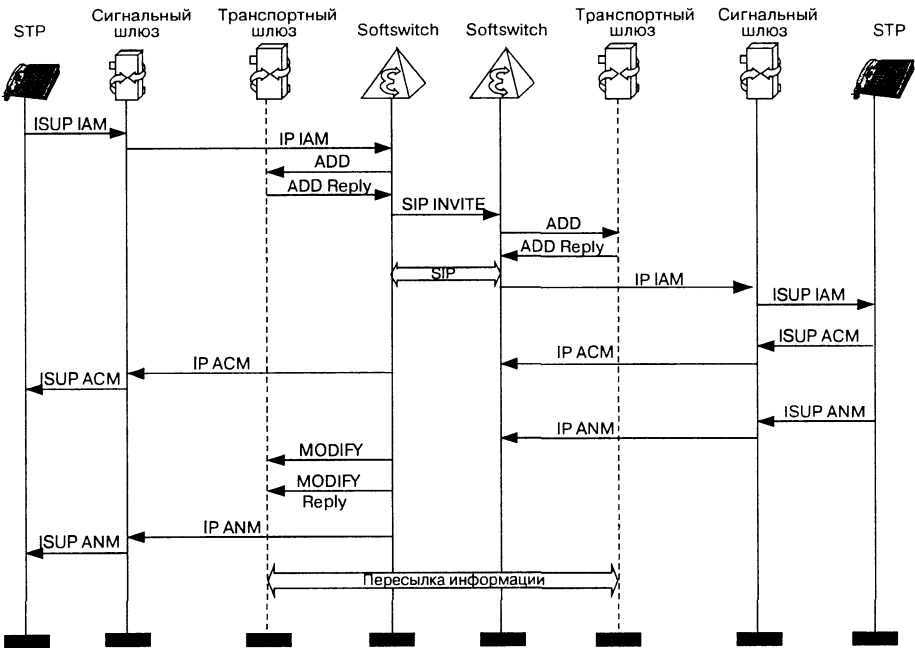


Рис. 7.1. Сценарий установления соединения SIP/Megaco /ISUP

В некоторых реализациях сообщения ISUP просто помещаются в пакеты UDP или TCP и передаются из SG в Softswitch, т.е. вместо [®]_{Sigtran} используются [®]_{UDP} или [®]_{TCP}. Однако оба этих подхода ущербны с точки зрения характерных для ОКС7 строгих требований к парамет-

рам потерь сообщений и к соблюдению очередности следования сообщений. Эти требования не позволяют всерьез использовать UDP, поскольку он ненадежен в своей основе. Гораздо больше надежд возлагалось на протокол TCP, но и он не подходит по своим временным характеристикам: хотя TCP может гарантировать строгую очередность доставки сообщений, доставка происходит недостаточно быстро. Это связано с тем, что блокировка несвоевременно пришедших данных, предлагаемая протоколом TCP, вносит ненужную задержку. Поясним подробнее и другие проблемы, связанные с использованием TCP.

Протокол TCP отслеживает переданные байты и подтверждает принятые байты. Этот характер протокола TCP, ориентированный на передачу байтов, часто причиняет неудобства, когда приложение желает отслеживать переданные сообщения в целом. Чтобы гарантировать, что все сообщение передано в приемлемое время, приложение должно добавлять собственную маркировку для очерчивания границ своих сообщений и использовать в явном виде средство форсированной отправки **push** протокола TCP.

Ограниченная область действия TCP-портов усложняет задачу переноса данных с множественной адресацией – весьма важное обстоятельство, обсуждающееся ниже в этой главе. Менее важный аспект, связанный с протоколом TCP, – его уязвимость к атакам злоумышленников, приводящим к отказу в обслуживании, например, к SYN-атакам, которые могут засорить сеть и сделать законный доступ практически невозможным (атака TCP-SYN – это когда злонамеренный объект постоянно пытается открыть TCP-соединения с атакуемым объектом с целью истощить его ресурсы). Несмотря на то, что такие атаки трудно полностью исключить, могут быть введены методы, позволяющие ограничить их последствия.

Разработкой средств доставки сообщений ISUP поверх IP, свободных от недостатков UDP и TCP, и занимается рабочая группа Sigtran. Предложенные ею общий подход и методология для транспортировки сигналов OKC7 по сетям IP изложены в документе RFC 2719 «Framework Architecture for Signaling Transport». Но – обо всем по порядку.

7.2. Архитектура Sigtran

Архитектура Sigtran, определенная вышеупомянутым RFC 2719, предусматривает следующие уровни:

- стандартный протокол IP,
- общая транспортировка сигналов, обеспечивающая доставку сообщений без ошибок и в должном порядке, независимо от капризов нижележащей сети IP, по протоколу SCTP (*Stream Control*

Transmission Protocol), который рассматривается в следующем параграфе главы,

- уровень адаптации, обеспечивающий интерфейс с протоколами и приложениями верхнего уровня, так что эти приложения не ощущают, что нижележащая транспортировка осуществляется в IP-среде, а не по традиционным протоколам переноса сообщений МТР стека ОКС7, например.

Заметим сразу, что протокол SCTP предоставляет возможность использовать его для надежной доставки сигнального трафика других типов, не входящего в стек ОКС7. В область интересов Sigtran включены также адаптационные уровни разных протоколов, что дает возможность пересылать по SCTP сигнальные сообщения не только ОКС7, а например, Q.931 ISDN или V5.2. Архитектура Sigtran подробно показана на рис. 7.2. В этой архитектуре, благодаря пересылке независимых последовательностей сообщений в отдельных потоках SCTP (что обсуждается ниже в этом параграфе), гарантируется свободная от ошибок доставка сообщений с соблюдением очередности их следования, обеспечивается быстрая доставка сообщений и уменьшается влияние повторной передачи потерянного сообщения на своевременность доставки сообщений из других последовательностей за счет так называемой *блокировки с относительным приоритетом (head-of-line blocking)*, что делает SCTP более подходящим протоколом, чем TCP.

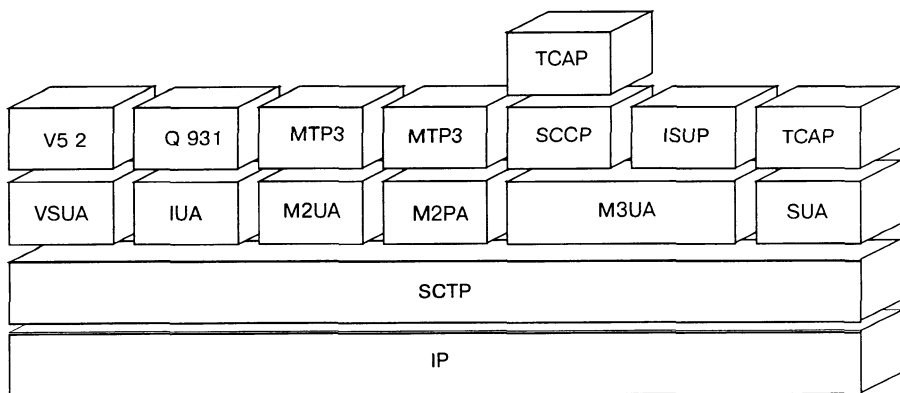


Рис. 7.2. Архитектура протокола Sigtran

Протокол SCTP рассматривается в следующем параграфе. Вслед за этим описываются уровни адаптации, которые обеспечивают сопряжение SCTP с протоколами верхнего уровня. Большинство из них ориентировано на ОКС7, в первую очередь, на протокол ISUP, но два относятся к сигнализации других типов. В число работающих поверх SCTP модулей адаптации входят следующие.

M2UA (MTP2-User Adaptation Layer) обеспечивает адаптацию SCTP к MTP3 таким образом, чтобы стандартный протокол MTP3 мог использоваться в сети IP, реализуя транспортировку сообщений через SCTP и IP вместо MTP2. Например, реализованное в Softswitch стандартное приложение MTP3 может обмениваться управляющими сообщениями сетевой сигнализации с внешней сетью ОКС7. Таким же образом, как в сети ОКС7 MTP2 предоставляет свои услуги MTP3, M2UA предоставляет свои услуги MTP3 в сети IP. M2UA имеет зарегистрированный номер порта 2904. Описанию M2UA посвящен параграф 7.5.

M2PA (MTP2 Peer-to-Peer Adaptation Layer) также обеспечивает адаптацию SCTP к MTP3, но уже в другой области. Аналогично случаю с M2UA, уровень MTP3 в узле сети IP (Softswitch, в частности) обменивается информацией с M2PA, как если бы он был обычным MTP2. Различия между M2UA и M2PA определяются их ролями в сетевой архитектуре: если Softswitch соединяется с сетью ОКС7 просто на правах терминала сигнализации ОКС7, то достаточно применение M2UA. Шлюз SG, который использует M2PA, сам фактически является транзитным пунктом сигнализации STP на базе IP, у него есть собственный код пункта сигнализации, он может также выполнять функции сигнализации верхнего уровня, такие как функции SCCP. Подробнее это обсуждается в посвященном M2PA параграфе 7.6.

M3UA (MTP3-User Adaptation Layer) обеспечивает интерфейс между SCTP и теми протоколами ОКС7, которые используют услуги MTP3, например, ISUP и SCCP. Благодаря M3UA эти протоколы не ощущают, что вместо типичной транспортировки MTP3 используется транспортировка SCTP поверх IP. Однако M3UA – просто адаптационный уровень между протоколами верхнего уровня и SCTP, он не является полной копией MTP3 в IP-сети и не реализует некоторые стандартные управляющие сообщения сетевой сигнализации MTP3, такие как TFA, TFP и пр. Этот момент важен, и с него мы начнем рассмотрение M3UA в параграфе 7.4.

SUA (SCCP-User Adaptation Layer) – параграф 7.7 – обеспечивает интерфейс между протоколом SCCP стека ОКС7 и SCTP, благодаря чему такие прикладные подсистемы-пользователи SCCP как TCAP используют услуги SUA точно так, как они используют услуги SCCP в сети ОКС7, даже не подозревая, что все это происходит в IP-сети.

IUA (ISDN Q.921-User Adaptation Layer) тоже работает поверх SCTP и обеспечивает для сигнализации DSS1 по рекомендации Q.931 прозрачную транспортировку сообщений по сети IP точно так, как они передаются уровнем звена данных Q.921 в сети ISDN. Освежить знания о протоколах ISDN второго (Q.921) и третьего (Q.931) уровней можно в [5], а описанию IUA посвящен параграф 7.8.

V5UA (*V5.2-User Adaptation Layer*) имеет ряд схожих с протоколом IUA черт и может рассматриваться как расширение IUA. Про универсальный интерфейс V5.2 сети доступа можно прочитать в [5] и [11], а его Sigtran-версия рассматривается в параграфе 7.9 этой главы.

7.3. Транспортный протокол с управлением потоками

7.3.1. Основные функциональные возможности SCTP

Протокол передачи с управлением потоками SCTP (*Stream Control Transmission Protocol*) специфицирован в документе RFC 2960 и является протоколом семейства IP за номером 132. Основанием для его разработки послужила уже обсуждавшаяся выше неспособность как UDP, так и TCP обеспечить скорость и надежность, необходимые для транспортировки сигнальных сообщений протоколов верхнего уровня, называемых *Upper-layer Protocol (UPL)*, которые не требуют полного набора функциональных возможностей протокола TCP, но продолжают предпочитать ориентированный на соединение протокол транспортного уровня с сохранением данных о состояниях. Эти задачи и призван решить SCTP. По смыслу протокол SCTP аналогичен TCP, но он усовершенствует операции переноса данных, сохранение данных о состояниях и обновление этих данных в отношении тех действий, которые необходимы для надежной и устойчивой транспортировки потоков сообщений UPL между портами. В связи с этим в предлагающемся на смену TCP протоколе SCTP реализуются следующие принципы:

- подтверждаемая, достоверная, свободная от ошибок и не дублируемая пересылка пользовательских данных в *потоках сообщений (message streams)*, при которой устраняется необходимость в обеспечении строгого порядка следования сообщений, и сообщения пересылаются на вышележащий уровень, как только они получены;
- сегментация данных для адаптации к размеру максимального пересылаемого блока данных, что, впрочем, является обязательным условием в мире IP и предусматривает сборку блоков данных в сообщения на дальнем конце;
- отсутствие обязательного мультиплексирования сообщений в SCTP-дейтаграммы;
- отказоустойчивость на сетевом уровне;
- исключение перегрузок и противодействие лавинам сообщений и нелегальным проникновениям в систему, вызывающим перегрузки;

- функции эксплуатационного управления трактом передачи, позволяющие установить доступность адресата в режиме реального времени посредством периодических контрольных сообщений, и если обнаруживается, что текущий транспортный адрес получателя недоступен, выбирается другой адрес из списка возможных транспортных адресов этого получателя.

Несмотря на то, что протокол SCTP является ориентированным на соединение в том смысле, что порты терминалов устанавливают между собой соединение перед тем, как начать передачу данных, он, по сравнению с протоколом TCP, является в некоторых областях применения более простым (причем не за счет надежности и устойчивости транспортного уровня), однако в других областях таковым не является. Он использует некоторые из алгоритмов, которые были разработаны в последние годы, а также накопленный опыт оптимального использования пропускной способности для максимального повышения производительности протокола TCP в глобальных и в высокоскоростных локальных вычислительных сетях. Рассмотрим основные термины протокола SCTP.

7.3.2. Множественная адресация

Оконечный пункт SCTP представляет собой логический передатчик или приемник пакетов SCTP и представляет собой комбинацию одного или нескольких адресов и номера порта, причем SCTP позволяет оконечному пункту иметь несколько IP-адресов и быть, таким образом, *multihomed* – распределенным по нескольким физическим платформам, – обеспечивая тем самым устойчивость к повреждениям. Даже имея несколько IP-адресов, оконечный пункт SCTP может использовать только один номер порта. Таким образом, если у оконечного пункта несколько IP-адресов, к каждому из них применяется один и тот же номер порта SCTP.

Комбинация IP-адреса и номера порта называется *транспортным адресом получателя (Active Destination)*, используемым передающим портом для пользовательских сообщений. Когда активный транспортный адрес недоступен, пробуются другие адреса удаленного порта из списка возможных транспортных адресов. Заметим, что любой транспортный адрес может применяться только к одному оконечному пункту SCTP, хотя оконечный пункт может иметь несколько транспортных адресов.

SCTP работает путем установления связей между оконечными пунктами SCTP. Такую связь называют *ассоциацией* или, менее точно, но более привычно, – *соединением*, причем оно определяется участвующими в нем оконечными пунктами SCTP и текущим состоянием протокола. Т.о., *SCTP-соединение (SCTP association)* – это протокольная связь между двумя SCTP-портами, содержащая протокольную информацию о состоянии, включая тэги верификации и активный

в данный момент набор порядковых номеров передачи TSN. Два SCTP-порта в любой момент времени не должны иметь между собой более одного SCTP-соединения. Прежде чем приложения двух оконечных пунктов смогут обмениваться информацией, необходимо установить соединение. Когда коммуникация закончена, соединение можно прекратить. Заметим, что протоколы верхнего уровня ISUP, SCCP, TCAP и др. не осведомлены о таких соединениях, более того, они не обнаруживают того факта, что сигнальные сообщения передаются не стандартной MTP, а чем-то иным.

Множественная адресация позволяет устанавливать соединение между двумя оконечными пунктами через несколько адресов IP и/или сетевых интерфейсов. Пример множественной адресации SCTP показан на рис. 7.3, где оба оконечных пункта А и В имеют два интерфейса для SCTP-соединений. Эти оконечные пункты имеют каналы двух типов: спутниковый в верхней части рисунка и ATM в нижней части. Один из адресов определен как основной, а другой может использоваться в качестве резервного при отказе основного адреса или в случае, если приложение верхнего уровня требует использовать исключительно резервный адрес.

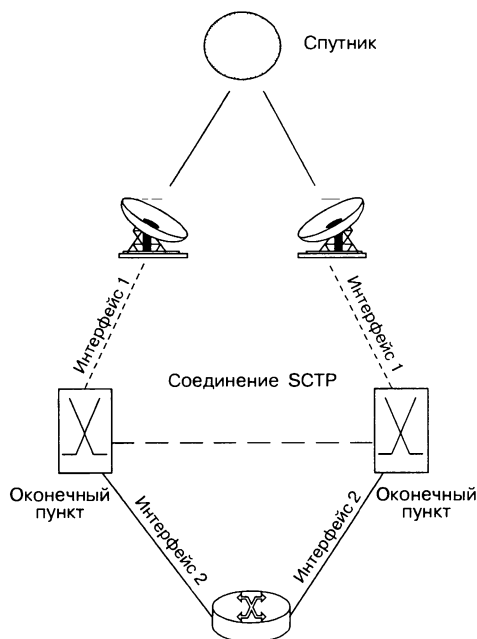


Рис. 7.3. Соединение SCTP для оконечных пунктов с множественной адресацией

Встроенная поддержка протоколом SCTP оконечных пунктов с множественной адресацией особенно полезна в среде, которая требует высокой доступности приложений, как в случае транспор-

тировки сигналов ОКС7. Соединение SCTP с множественной адресацией может также ускорять восстановление после отказов канала без прерывания текущей пересылки данных.

7.3.3. Соединения для нескольких потоков

Когда устанавливается соединение между оконечными пунктами, нужно учитывать количество потоков, которые это соединение должно поддерживать. Д. Коллинз в [39] приводит наглядную аналогию: если представить себе соединение как одностороннюю автомобильную магистраль между оконечными пунктами, то отдельные потоки, которые оно поддерживает, будут аналогичны отдельным полосам движения на этой магистрали.

Возвращаясь от этой наглядной аналогии к практическому применению принципа, приведем рис. 7.4, иллюстрирующий возможность мультиплексировать данные приложения верхнего уровня в одном SCTP-соединении [106].

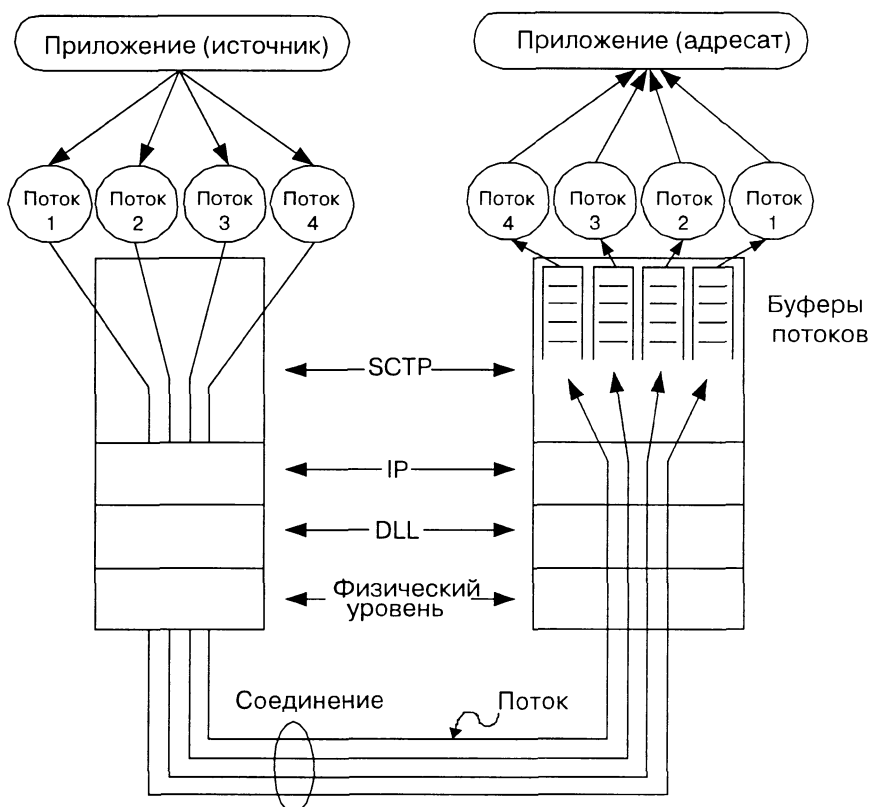


Рис. 7.4. SCTP-соединение для четырех потоков данных одного приложения

В каждом потоке производится упорядочение данных. Если фрагмент пакета, принадлежащего некоторому потоку потерян, то фрагменты этого пакета, следующие за потерянным, будут сохраняться в буфере приемника потока, пока потерянный фрагмент не будет передан источником повторно. Однако фрагменты пакетов из других потоков могут по-прежнему проходить в приложение верхнего уровня. Этим исключается блокировка *head-of-line*, которая имеет место в TCP, где данные из всех приложений верхнего уровня пересылаются в одном потоке. Иначе говоря, эффект блокировки *head-of-line* ограничен пределами отдельных потоков, но не проявляется для соединения в целом. Проще говоря, каждый поток обрабатывается отдельно, так что доставка сообщений одного потока не задерживается из-за ожидания следующего по порядку сообщения другого потока.

В заключение этого раздела напомним, что для передачи сообщения пользователя (*user message*), получаемого от протокола верхнего уровня ULP, SCTP передает в IP так называемый пакет SCTP, а тот маршрутизирует его к месту назначения. Пакет SCTP состоит из общего заголовка и нескольких фрагментов (*chunks*), как показано на рис. 7.5.

7.3.4. Фрагменты

Фрагмент (chunk – небольшой кусок) – это часть информации внутри SCTP-пакета, состоящая из заголовка и содержимого, зависящего от приложения. Общий заголовок SCTP-пакета на рис. 7.5 включает в себя номера портов источника и пункта назначения, которые в сочетании с IP-адресами источника и пункта назначения однозначно определяют оконечные пункты. Далее в состав заголовка входит тэг верификации, который используется для подтверждения данных об отправителе пакета. Тэг верификации еще будет описан в этой главе подробнее.

Общий заголовок содержит также контрольную сумму Adler-32, которая образуется особым подсчетом значений всех октетов пакета. Эта контрольная сумма служит для того, чтобы гарантировать отсутствие повреждений в полученном пакете, и обеспечивает еще один уровень защиты в дополнение к контрольной сумме заголовка IP.

За общим заголовком следуют несколько фрагментов. Каждый фрагмент содержит свой заголовок плюс некоторое содержимое. Это содержимое может быть либо управляющей информацией SCTP, либо информацией пользователя SCTP. В случае пользовательской информации SCTP из ULP значение идентификатора ID фрагмента равно 0, обозначая данные полезной нагрузки пользователя. В ином случае идентификатор фрагмента будет иметь значение, указывающее тип управляющей информации SCTP. Возможные значения флагов и длины зависят от идентификатора фрагмента.

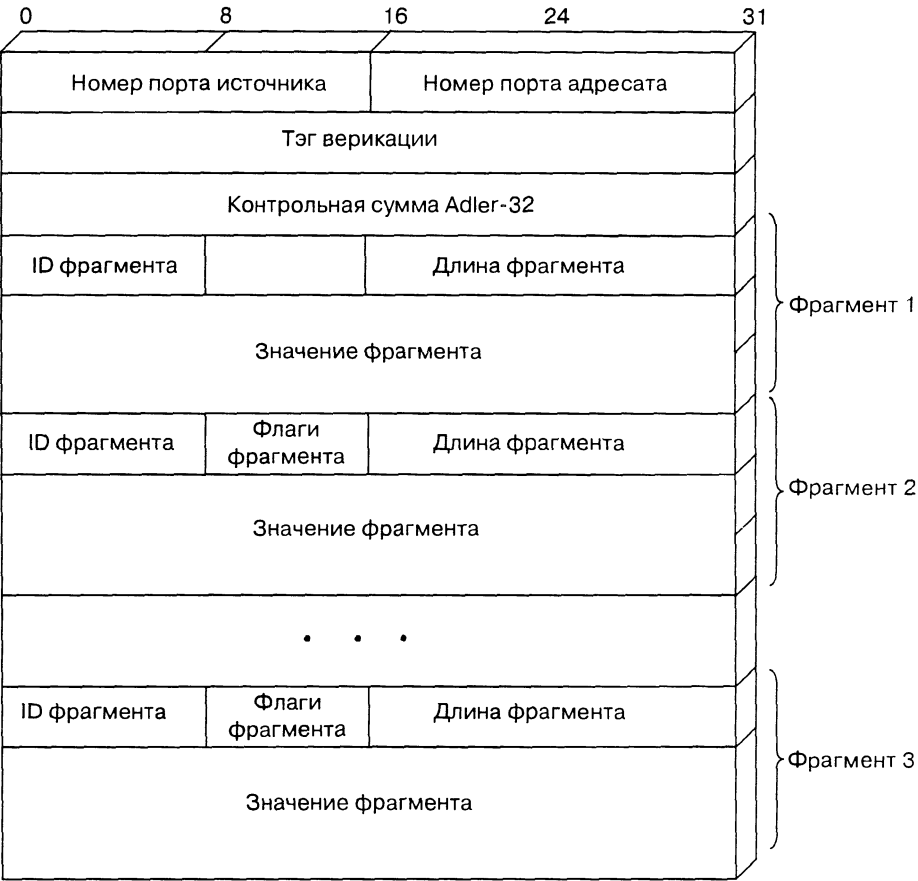


Рис. 7.5. Формат пакета SCTP

Хотя всего может быть до 256 разных идентификаторов фрагмента, существуют четыре основные их категории: идентификаторы переноса данных пользователя SCTP, идентификаторы переноса управляющей информации SCTP, идентификаторы, которые резервированы IETF, и идентификаторы переноса расширений, определенных IETF. Типы фрагментов описываются в табл. 7.1.

Таблица 7.1. Фрагменты пакетов протокола SCTP

Имя фрагмента	Описание применения
DATA (0)	Фрагменты с данными, передаваемыми портами терминалов после того, как между ними установлено SCTP-соединение. Чтобы обеспечить раннюю передачу данных, фрагменты DATA могут объединяться в группы с управляющими фрагментами COOKIE-ECHO и COOKIE-ACK, пока управляющие фрагменты идут в сообщении первыми. Сообщения могут сегментироваться, чтобы не превышался заданный максимальный размер передаваемого блока информации MTU. Если это имеет место, то флаг фрагмента указывает начало и конец сегмента исходного сообщения. Фрагменты DATA могут доставляться в порядке их приема (и тогда они могут быть неупорядоченными), или же перед доставкой сообщения к протоколу верхнего уровня может производиться полная сборка исходного сообщения. Тип обслуживания, запрашиваемый потоком, указывается флагом фрагмента
INIT (1)	Это первый фрагмент, который инициирует установление SCTP-соединения между двумя терминалами. Он переносит такие параметры, как транспортный адрес соединения (может быть более одного адреса и может быть адрес протокола IPv4, IPv6 или их сочетание), количество входящих потоков, которое может поддерживать отправитель, и количество исходящих потоков, которое желает поддерживать получатель в данном SCTP-соединении. Здесь же удаленному порту сообщается о резервировании ресурсов отправителем (размер входного буфера в байтах)
INIT ACK (2)	Подтверждает прием фрагмента INIT и содержит переменную состояния cookie. Может также идентифицировать неопознанные параметры в сообщении INIT и, подобно INIT, задает количество выходных и входных потоков для SCTP-соединения с портом терминала, а также транспортные адреса, которые могут использоваться в этом соединении
SACK (3)	Подтверждает получение фрагментов DATA или информирует о том, что в последовательности принятых фрагментов DATA имеется разрыв
HEARTBEAT REQUEST (4)	Передается периодически для подтверждения доступности порта получателя
HEARTBEAT ACK (5)	Подтверждает запрос HEARTBEAT ACK. Должен передаваться на исходный IP-адрес отправителя фрагмента HEARTBEAT REQUEST
ABORT (6)	Немедленно закрывает SCTP-соединение и может содержать параметры, которые указывают причину
SHUTDOWN (7)	Передается, чтобы инициировать постепенное закрытие SCTP-соединения
SHUTDOWN ACK (8)	Получатель сообщения SHUTDOWN передает это сообщение как подтверждение
ERROR (9)	Указывает разные неисправности на порте. Ошибки могут быть внутренними или ошибками протокола, такими как некорректные параметры при управлении фрагментами DATA
COOKIE ECHO (10)	Используется только в фазе установления SCTP-соединения и завершает процесс установления соединения у отправителя данных. Может объединяться в группу с фрагментом DATA, но должен быть первым фрагментом в такой связке
COOKIE-ACK (11)	Подтверждает получение COOKIE-ECHO в фазе установления SCTP-соединения. Может объединяться в группу с фрагментом DATA, но должен быть первым фрагментом в такой связке
ECNE (12) и CWR (13)	Уведомление о явной перегрузке и уменьшенное окно перегрузки, резервированы для будущего использования
SHUTDOWN COMPLETE (14)	Подтверждает получение SHUTDOWN ACK

Значения ID фрагментов кодируются двумя старшими битами, определяющими действие, которое нужно выполнить в случае, если обрабатывающий оконечный пункт не узнает тип фрагмента. Возможные значения этих битов и их смысл:

- **00** – остановить обработку этого пакета SCTP и отбросить его; остальные фрагменты в этом пакете не обрабатывать;
- **01** – остановить обработку этого пакета SCTP и отбросить его; остальные фрагменты в этом пакете не обрабатывать. Отправить сообщение о неопознанном параметре Unrecognized Parameter Type (в фрагменте ERROR или INIT ACK);
- **10** – пропустить этот фрагмент и продолжить обработку;
- **11** – пропустить этот фрагмент и продолжить обработку, но отправить сообщение в фрагменте ERROR с использованием Unrecognized Parameter Type в качестве причины ошибки.

Фрагмент INIT используется для инициирования соединения SCTP между двумя оконечными пунктами. В отличие от многих других, фрагмент INIT не должен делить пакет SCTP с другими фрагментами. Иначе говоря, пакет SCTP, содержащий фрагмент INIT, не должен содержать никаких других фрагментов.

Фрагмент INIT ACK используется для подтверждения инициирования соединения SCTP. Как и фрагмент INIT, фрагмент INIT ACK не должен делить пакет SCTP с другими фрагментами.

Фрагмент SACK служит для подтверждения приема фрагментов DATA (полезной нагрузки) и уведомления отправителя о пропусках в последовательности принятых фрагментов. Не каждый принятый фрагмент заслуживает передачи в ответе фрагмента SACK. Фрагмент SACK работает как указатель места пропуска. Предположим, что приемник получил фрагменты с 1 по 5, а также фрагменты 8 и 9. Сообщение SACK информирует об отсутствии фрагментов 6 и 7. Нужно повторно передать только эти фрагменты. Такой метод эффективнее механизма повторной передачи в TCP.

Фрагмент HEARTBEAT используется для проверки досягаемости определенного оконечного пункта. Предположим, что в течение некоторого отрезка времени никакие фрагменты передавать из оконечного пункта А в оконечный пункт В не нужно. В этом случае оконечный пункт А будет периодически передавать в оконечный пункт В сообщения HEARTBEAT, чтобы убедиться в работоспособности оконечного пункта В. Фрагмент HEARTBEAT содержит специальную информацию отправителя. Получатель фрагмента HEARTBEAT должен ответить фрагментом HEARTBEAT ACK, который содержит информацию, скопированную из принятого фрагмента HEARTBEAT.

Фрагмент ABORT передается оконечным пунктом, чтобы резко прекратить соединение. Этот фрагмент может содержать инфор-

мацию о причине прекращения соединения и может быть передан в одном пакете с другими управляющими фрагментами SCTP. Однако в таких случаях он должен быть последним фрагментом в пакете. Если он передается не последним в пакете, то следующие за ним фрагменты игнорируются. Фрагменты DATA не должны входить в состав пакета, содержащего фрагмент ABORT.

Фрагмент SHUTDOWN используется для плавного прекращения соединения. Если приложение верхнего уровня или управляющее приложение хочет закрыть соединение, то окончательный пункт прекращает передачу новых данных на дальний конец. Он будет ждать, пока не получит подтверждения всех переданных данных, а затем передаст на дальний конец фрагмент SHUTDOWN, чтобы закрыть соединение. SHUTDOWN будет указывать последний фрагмент DATA, принятый от дальнего конца. Если это необходимо, окончательный пункт может повторно передать данные пользователя на дальний конец и только потом передать фрагмент SHUTDOWN.

После приема фрагмента SHUTDOWN окончательный пункт может убедиться, что все данные пользователя, которые он передал, подтверждены, и, если необходимо, повторно передать данные на дальний конец. Если действительно все, что окончательный пункт передавал прежде, получено, он должен передать фрагмент SHUTDOWN ACK.

После получения SHUTDOWN ACK отправитель SHUTDOWN должен ответить фрагментом SHUTDOWN COMPLETE и может стереть все сведения о соединении. Когда дальний конец принимает фрагмент SHUTDOWN COMPLETE, он тоже может стереть все сведения о соединении. В этот момент соединение разрушено.

Фрагмент ERROR передается для уведомления об обнаруженных окончательным пунктом ошибочных ситуациях. В состав фрагмента обычно входит извещение о причине ошибки, чтобы обеспечить возможность дальнейшей ее обработки. Например, окончательный пункт мог получить фрагмент несуществующего потока или фрагмент, в котором отсутствуют некоторые обязательные параметры. Получение фрагмента ERROR само по себе не указывает на непоправимое состояние. Переданный фрагмент ERROR просто может дать возможность приемнику исправить ошибочное состояние. Если ясно, что ошибочное состояние непоправимо, фрагмент ERROR может быть передан в той же дейтаграмме, что и фрагмент ABORT.

Фрагмент COOKIE ECHO используется только во время иницирования соединения. Когда окончательный пункт получает фрагмент INIT и отвечает фрагментом INIT ACK, он включает в состав INIT ACK параметр cookie. Этот параметр содержит особую для окончательного пункта и для его представления соединению информацию, временную метку, и значение времени жизни параметра cookie (рекомендуется 5 секунд). Когда на дальний конец приходит INIT ACK, копия

cookie вводится в фрагмент COOKIE ECHO, который передается в обратном направлении. COOKIE ECHO может передаваться в пакете, который содержит также фрагменты DATA. Однако в таком случае фрагмент COOKIE ECHO должен быть первым фрагментом в пакете.

Фрагмент COOKIE ACK передается в ответ на фрагмент COOKIE ECHO. Поэтому COOKIE ACK используется только во время установления соединения. Поскольку содержимое фрагмента COOKIE ACK такое же, какое было передано в INIT ACK, отправитель INIT ACK может убедиться, что инициатор соединения принял информацию cookie правильно. Если фрагмент COOKIE ECHO был принят без ошибок и в течение указанного для cookie времени жизни, приемник COOKIE ECHO передает фрагмент COOKIE ACK. В противном случае передается фрагмент ERROR. Фрагмент COOKIE ACK может передаваться в той же дейтаграмме, что и фрагменты DATA, но должен быть первым фрагментом в этой дейтаграмме.

7.3.5. Фрагмент полезной нагрузки DATA

Фрагмент DATA используется для переноса к и от UPL информации пользователя. Он имеет формат, показанный на рис. 7.6.

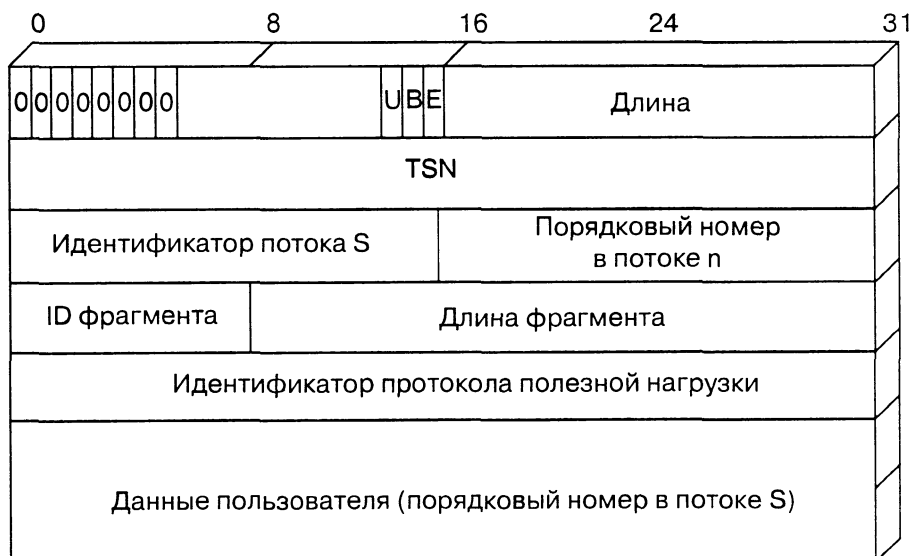


Рис. 7.6. Формат фрагмента DATA

Есть вероятность того, что протоколу SCTP придется разделить сообщение на сегменты. Такое может произойти, если MTU тракта меньше размера сообщения, которое необходимо передать. Из-за возможной сегментации в формат фрагмента введены биты *Начало* (B) и *Конец* (E). Бит B указывает, что фрагмент содержит часть

первого сегмента сообщения пользователя, а бит Е – что фрагмент содержит часть последнего сегмента сообщения. Если сообщение полностью уместается в один фрагмент, оба бита, В и Е, имеют значение 0. Если сообщение содержит более 2 сегментов, первый фрагмент первого сегмента должен иметь бит В, равный 1, а бит Е – равный 0, в то время как последний фрагмент последнего сегмента должен иметь бит В, равный 0, а бит Е равный – 1. Фрагменты всех сегментов в промежутке между первым и последним должны иметь оба бита, Е и В, равными 1.

Бит U указывает, что фрагмент принадлежит неупорядоченному потоку данных. Другими словами, порядок сообщений пользователя в потоке не играет роли, и порядковый номер в потоке следует игнорировать. В таком случае SCTP пропускает данные в верхний уровень без анализа порядка поступления сообщений. Однако SCTP все-таки должен гарантировать, что сегментированные сообщения прошли восстановительную сборку до отправки данных в верхний уровень.

Порядковый номер передачи (TSN) представляет собой 32-битовое целое число, которое идентифицирует фрагмент в контексте соединения. Этот номер не зависит от порядкового номера фрагмента в потоке и назначается SCTP, а не каким-нибудь пользователем SCTP. Когда оконечный пункт передает фрагмент INIT, в его состав входит TSN, соответствующий первому фрагменту DATA, который этот пункт планирует передать. Таким образом, первый передаваемый фрагмент DATA всегда содержит тот же TSN, что и фрагмент INIT. После этого TSN увеличивается для каждого нового фрагмента DATA, передаваемого оконечным пунктом в этом соединении.

Идентификатор потока (S) является 16-битовым целым числом, определяющим поток, которому принадлежат данные. Порядковый номер в потоке (n) – это 16-битовое целое число, указывающее положение сообщения внутри потока. Порядковые номера сообщений в каждом потоке начинаются с 0. Номер увеличивается для каждого передаваемого в этом потоке сообщения. Заметим, что сегментированное сообщение должно иметь в каждом сегменте один и тот же порядковый номер в потоке.

Идентификатор протокола полезной нагрузки передается от пользователя-отправителя к SCTP на передающем конце и пропускается от SCTP к пользователю-адресату на приемном конце. Он доступен пользователям для пропуска дальнейшей информации о фрагменте, но SCTP не проверяет этот идентификатор и не воздействует на него.

7.3.6. Установление соединения

Установление соединения обычно инициирует протокол верхнего уровня, который приказывает SCTP установить соединение. Соединение может быть установлено заблаговременно перед передачей какого-либо трафика данных. Например, если сетевой администратор организует пучок соединительных линий ISUP в Softswitch, и Softswitch использует M3UA, действия, связанные с определением пучка соединительных линий, могут заставить M3UA запросить в SCTP установление соединения. Подобным же образом, соединение может быть установлено, когда в обслуживание вводится новое звено OKC7 в SG, или когда вводится в обслуживание новый диапазон CIC. Этот процесс изображен на рис. 7.7.

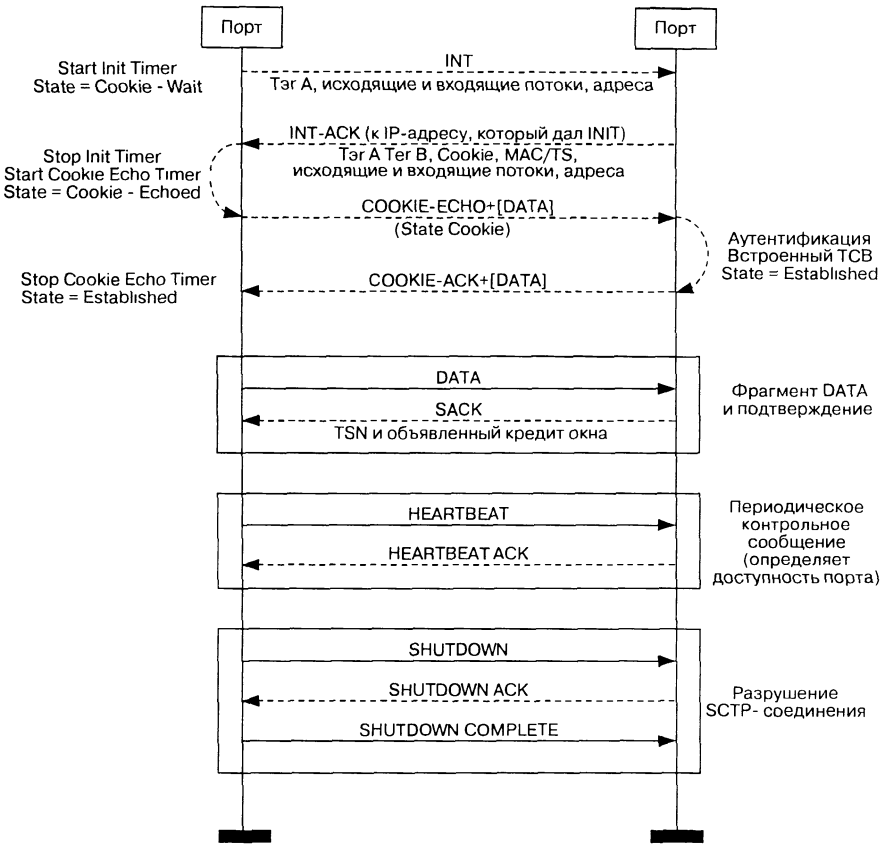


Рис. 7.7. Сценарий установления и разрушения SCTP-соединения

Он начинается передачей на транспортный адрес удаленного порта пакета SCTP, содержащего фрагмент INIT, инициируя тем самым установление SCTP-соединения. Отправитель запускает таймер и переходит в состояние cookie-wait (ожидание cookie).

Помимо обязательных параметров фрагмент INIT может содержать также ряд дополнительных параметров и/или параметров с варьируемой длиной. Например, фрагмент INIT может содержать один или несколько адресов IPv4 и IPv6, или имя разрешенного хоста.

Удаленный порт, который принимает INIT, генерирует фрагмент INIT-ACK и передает его на IP-адрес отправителя INIT. INIT-ACK содержит данные о cookie-состояниях, и как только он принимается, отправитель INIT останавливает таймер и передает фрагмент COOKIE-ECHO. Запускается новый таймер, а отправитель переходит в состояние cookie-wait. Фрагмент INIT ACK тоже может содержать ряд адресов IPv4 и IPv6. Принимая во внимание то, что фрагмент INIT ACK тоже содержит некоторое количество входящих и исходящих потоков, оба конца соединения знают максимальное количество потоков, которые может передавать и принимать другая сторона. Каждый оконечный пункт должен соблюдать требования другого и не должен передавать больше, чем другой оконечный пункт может обработать. После приема фрагмента INIT ACK инициатор соединения передает фрагмент COOKIE ECHO, содержимое которого скопировано из параметра cookie принятого фрагмента INIT ACK. Когда на дальний конец соединения приходит COOKIE-WAIT и от него поступает фрагмент COOKIE-ACK, оба порта переходят в состояние *соединение установлено (established)*.

Надежная пересылка данных пользователя достигается путем использования двух фрагментов. Первый – это фрагмент DATA, который был описан в п. 7.3.5, а второй – фрагмент SACK. Прием фрагментов DATA подтверждается фрагментами SACK, которые указывают также на пропуски в последовательности передачи данных потока. Периодически происходит обмен фрагментами HEARTBEAT для поддержания соединения между портами на действующих маршрутах между транспортными адресами. Пара сообщений HEARTBEAT/HEARTBEAT-ACK полезна и для определения времени двойного пробега (задержки подтверждения приема) RTT между портами, которое, в свою очередь, используется для вычисления размеров окон для передачи. Многочисленные неудачные попытки передать на порт фрагмент определенного типа (или неоднократные срабатывания таймера при ожидании SACK в ответ на DATA) могут означать, что текущий транспортный адрес недоступен.

SCTP-соединения могут разрушаться немедленно (с помощью сообщения ABORT) или постепенно (с помощью сигнальной процедуры SHUTDOWN/SHUTDOWN-ACK/SHUTDOWN COMPLETE), как показано в представленном сценарии. Заметим, что, в отличие от протокола TCP, протокол SCTP не поддерживает «полуоткрытое» состояние, при котором одна сторона может продолжать передачу данных, в то время как другая сторона уже закрыта.

также и к другим адаптационным уровням. Прежде всего, подчеркнем различие между термином *сервер приложений AS* (*Application Server*), использованным ранее в этой книге в контексте VoIP и Softswitch, и тем же термином в понимании рабочей группы Sigtran для протоколов адаптационного уровня. В последнем случае под *сервером приложений AS* понимается логический объект, который обрабатывает сигнализацию в определенной области. Например, AS может быть логическим объектом в Softswitch, обрабатывающим сигнализацию ISUP для конкретного диапазона ОКС7 DCP/OPC/CIC. В равной степени, AS может быть логическим объектом в приложении базы данных, обрабатывающим сигнализацию.

Процесс сервера приложений ASP (*Application Server Process*) представляет собой экземпляр AS, что напоминает концепцию процессов в языке спецификаций и описаний SDL, обсуждающуюся в [4]. Сервер AS содержит набор *процессов сервера приложений*. Фактически, AS можно рассматривать как список процессов ASP, часть которых активна, а часть находится в резерве. ASP может быть, например, процессом в Softswitch, который в это время обрабатывает сигнализацию ISUP. В устойчивой сети должен быть, по крайней мере, один активный ASP и, по крайней мере, один резервный ASP для каждого приложения. Один ASP может обслуживать несколько серверов AS. Например, Softswitch может иметь несколько серверов AS, каждый из которых соответствует уникальной комбинации OPC/DPC. Этот же самый Softswitch может иметь только один ASP, обрабатывающий всю сигнализацию ISUP (или два процесса ASP для резервирования или для разделения нагрузки).

Ключ маршрутизации (Routing Key) представляет собой набор таких параметров ОКС7, как SLS, DPC, OPC или диапазон CIC, которые определяют сигнализацию для некоторого AS. Например, если какой-то AS должен обрабатывать сигнализацию ISUP для определенной комбинации OPC/DPC/диапазон CIC, то эта комбинация и является ключом маршрутизации для такого AS. В пределах SG каждый ключ маршрутизации обычно указывает на один определенный AS. Иначе говоря, между ключами маршрутизации и AS, как правило, существует однозначное соответствие.

Отображение сети (Network Appearance) – это такое ее представление, которое позволяет отделить часть сигнального трафика, нужную для связи между SG и ASP, от всего трафика, использующего одно и то же соединение SCTP. Представим себе, например, международный SG. Этот SG будет иметь, по крайней мере, один национальный и один международный код пункта сигнализации. SG использует национальный вариант MTP для связи в национальной сети и вариант ITU-T MTP – для связи в международной сети, а потому он должен видеть и различать соответствующие сигнальные потоки. Для связи между SG и Softswitch передаваемые и принимаемые сообщения

должны помещаться в контексте правильного отображения сети, чтобы можно было оперировать соответствующей группой линий на не-IP-стороне SG.

7.4.3. Код пункта сигнализации

Каждый ASP необходимо ассоциировать с кодом пункта сигнализации. Однако назначение кодов пунктов для процессов ASP является абсолютно гибким. Например, все ASP, подсоединенные к определенному SG, могут совместно использовать тот же код пункта, что и этот SG. В таком случае комбинация SG и процессов ASP видна сети ОКС7 как единый оконечный пункт сигнализации. Или же все ASP, подсоединенные к одному SG, могут иметь один и тот же код пункта, который отличается от кода пункта сигнализации, присвоенного этому SG. В таком случае SG будет виден сети ОКС7 как STP, а объединенные общим кодом ASP – как единый оконечный пункт сигнализации, расположенный за этим STP.

Еще одним вариантом назначения кодов может быть присвоение каждому ASP своего кода пункта, или группам ASP – разных общих кодов, отличных от кода, присвоенного SG. В этом случае SG виден как STP, а каждый ASP (или группа процессов ASP) – как один оконечный пункт сигнализации. Дело в том, что если некий ASP или некая группа ASP может связываться с сетью ОКС7 не через один, а через два SG, то этот ASP или эта группа ASP должны иметь код пункта, который отличается от кодов этих двух SG. В таком сценарии шлюзы SG работают как транзитные пункты сигнализации STP.

7.4.4. Примитивы

Чтобы предоставлять услуги верхнему уровню прозрачно (так, чтобы приложение не ощущало факт использования функций MTP3, встроенных в SG, вместо функций локальной MTP), M3UA должен предоставлять верхнему уровню те же самые примитивы, которые предоставляет MTP3. Это следующие примитивы:

- *MTP-Transfer request* передается из верхнего уровня в M3UA, чтобы запросить перенос сообщения в определенный пункт назначения.
- *MTP-Transfer indication* используется M3UA, чтобы пропустить входящее сообщение в верхний уровень.
- *MTP-Pause indication* передается M3UA в верхний уровень, чтобы указать, что передача сигналов в определенный пункт назначения должна быть приостановлена. Этот примитив используется, например, когда пункт назначения недостижим.
- *MTP-Resume indication* передается M3UA в верхний уровень, чтобы указать, что передачу сигналов в пункт назначения можно возобновить.

- *MTP-Status indication* передается M3UA в верхний уровень, чтобы информировать этот уровень о некоторых изменениях, возникших в сети OKC7, таких как перегрузка или недоступность подсистемы-пользователя в пункте назначения.

Рассмотрим пример приложения ISUP в Softswitch, которому требуется передать сообщение в сеть OKC7. Приложение передает запрос MTP-Transfer request в M3UA, а M3UA передает его в SCTP как фрагмент DATA, который необходимо передать по определенному соединению SCTP и в определенном потоке. SCTP обеспечивает поступление фрагмента DATA в SG, где содержимое этого фрагмента проходит в M3UA, который передает его к функции взаимодействия в SG. Функция взаимодействия пропускает его в MTP3 на стороне сети OKC7 шлюза SG, который берет на себя корректную маршрутизацию сообщения дальше в сеть OKC7.

В противоположном направлении процесс проходит аналогично. Сообщение приходит в SG и проходит от MTP3 к функции взаимодействия, а от функции взаимодействия поступает в M3UA. На основе параметров DPC/OPC/диапазон CIC сообщения OKC7 выбираются подходящий AS и подходящий ASP. Если активны более одного ASP, то выбирается один из них (в соответствии с алгоритмом разделения нагрузки). M3UA формирует сообщение для передачи SCTP как фрагмента DATA по соответствующему соединению SCTP и в соответствующем потоке. В пункте назначения фрагмент DATA проходит в M3UA, который пропускает информацию этого фрагмента в приложение, используя примитив MTP-Transfer indication.

7.4.5. Сообщения M3UA

В состав M3UA входит ряд сообщений между одноуровневыми объектами M3UA, общий формат которых показан на рис. 7.9. Формат содержит заголовок и содержимое сообщения. Заголовок является общим для всех уровней адаптации. Для уровня M3UA версия протокола равна 0000 0001. Класс сообщения может быть следующим:

- **00** Сообщение управления;
- **01** Сообщение пересылки;
- **02** Сообщение эксплуатационного управления сетью сигнализации OKC7 (SSNM);
- **03** Сообщения эксплуатационного управления состоянием ASP (ASPSM);
- **04** Сообщение эксплуатационного управления трафиком ASP (ASPTM);
- **05** Резерв для класса сообщений, относящихся к IUA и обеспечивающих транспортировку пограничных примитивов Q.921/Q931;

- **06** Резерв для класса сообщений адаптации пользователя, относящихся к M2UA;
- **07** Резерв для класса сообщений без установления соединения, относящихся к SUA;
- **08** Резерв для класса сообщений, ориентированных на соединение и относящихся к SUA;
- **09** Сообщение эксплуатационного управления ключом маршрутизации (RKM);
- **10** Резерв для класса сообщений эксплуатационного управления идентификатором интерфейса M2UA;
- **11** Резерв для класса сообщений M2PA;
- от **12** до **127** резервированы комитетом IETF;
- от **128** до **255** резервированы для определяемых IETF расширений класса сообщений.



Рис. 7.9. Общий формат сообщения M3UA

Когда M3UA пересылает информацию пользователя между SG и Softswitch, как было описано ранее, он выполняет это путем передачи сообщений M3UA DATA. Эти сообщения формируются как фрагменты SCTP DATA. При передаче сообщения DATA поле класса сообщения имеет значение 1, и тип сообщения имеет значение 1, как это показано в табл. 7.2.

Помимо упаковки сообщений пользователя в формат сообщений M3UA DATA, M3UA предусматривает другие сообщения между одноуровневыми M3UA-объектами, так что эти объекты могут обмениваться информацией, относящейся к сети OKC7 в целом. Например, если пункт назначения становится недоступным, то SG уведомляется об этом с помощью сообщений эксплуатационного управления сетью сигнализации OKC7. Приложение ISUP в Softswitch

тоже должно уведомляться об этом событии, чтобы оно не пыталось передавать сообщения, которые не могут достичь своего пункта назначения. МЗUA в Softswitch может предупреждать о таком событии с помощью примитива MTP-Pause indication. Но МЗUA – не МТРЗ, и сообщения эксплуатационного управления сетью сигнализации не проходят прямо от SG к SG. Поэтому МЗUA в Softswitch узнает, что пункт назначения недоступен, с помощью другого сообщения МЗUA, помимо сообщения DATA. В табл. 7.2 приводится список типов сообщений МЗUA.

Таблица 7.2. Сообщения МЗUA

Имя сообщения	Класс сообщения	Код класса сообщения	Код типа сообщения
Error (ERR)	MGMT	00	00
Notify (NTFY)	MGMT	00	01
Data	Transfer	01	01
Destination Unavailable (DUNA)	SSNM	02	01
Destination Available (DAVA)	SSNM	02	02
Destination State Audit (DAUA)	SSNM	02	03
SS7 Network Congestion State (SCON)	SSNM	02	04
Destination User Part Unavailable (DUPU)	SSNM	02	05
Destination Restricted (DRST)	SSNM	02	06
ASP Up (ASPUP)	ASPSM	03	01
ASP Down (ASPDN)	ASPSM	03	02
Heartbeat (BEAT)	ASPSM	03	03
ASP Up Acknowledgment (ASPUP ACK)	ASPSM	03	04
ASP Down Acknowledgment (ASPDN ACK)	ASPSM	03	05
Heartbeat Acknowledgment (BEAT ACK)	ASPSM	03	06
ASP Active (ASPAC)	ASPTM	04	01
ASP Inactive (ASPIA)	ASPTM	04	02
ASP Active Acknowledgment (ASPAC ACK)	ASPTM	04	01
ASP Inactive Acknowledgment (ASPIA ACK)	ASPTM	04	02
Registration Request (REG REQ)	RKM	09	01
Registration Response (REG RSP)	RKM	09	02
Deregistration Request (DEREG REQ)	RKM	09	03
Deregistration Response (DEREG RSP)	RKM	09	04

К сообщениям эксплуатационного управления (*Management Messages*) относится сообщение *ERR-ошибка (Error)* о том, что принято непредвиденное сообщение или сообщение с неверным содержанием, а также сообщение *NTFY-уведомление (Notify)* для передачи информации об определенных событиях, относящихся к МЗUA. Например, сообщение NTFY можно использовать, чтобы информировать об изменении состояния в ASP. В состав сообщений эксплуатационного управления сетью сигнализации

(*Signaling Network Management Messages*) M3UA входят: сообщение *DUNA* – адресат недоступен (*Destination Unavailable*), передаваемое из SG во все заинтересованные процессы ASP, чтобы уведомить их о недоступности пункта назначения в сети ОКС7, сообщение *DAVA* – адресат доступен (*Destination Available*), которое в ASP преобразуется в примитив MTP-Resume indication, сообщение *DAUD* – проверка состояния пункта назначения (*Destination State Audit*), сообщение *SCON* о перегрузке сети ОКС7 (*SS7 Network Congestion*), сообщение *DUPU* – подсистема-пользователь в пункте назначения недоступна (*Destination User Part Unavailable*), которое в ASP отображается в примитив MTP-Status indication, и сообщение *DRST* – доступ к пункту назначения ограничен (*Destination Restricted*).

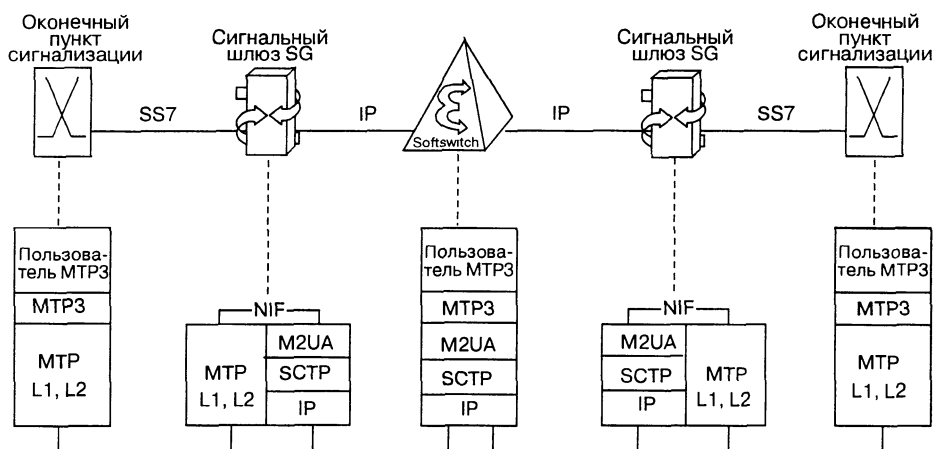
В состав сообщений M3UA входят следующие *сообщения эксплуатационного управления состоянием ASP (ASP State Management Messages)*: *ASPUP* – ASP включен (*ASP Up*) и *ASPUP ACK* – подтверждение включения ASP (*ASP Up Acknowledgment*), *ASPDN* – ASP выключен (*ASP Down*) и *ASPDN ACK* – подтверждение выключения ASP (*ASP Down Acknowledgment*), *BEAT* и *BEAT ACK* – сообщения о работоспособности (*Heartbeat messages*), а также *сообщения эксплуатационного управления трафиком ASP (ASP Traffic Management Messages)*, с помощью которых организуется передача трафика между SG и одним или несколькими ASP (распределение нагрузки), а также *сообщения эксплуатационного управления ключами маршрутизации (Routing Key Management Messages)*.

7.5. Протокол M2UA

Использование M2UA иллюстрирует рис. 7.10. В этом сценарии два сигнальных шлюза SG обеспечивают интерфейс с внешней сетью ОКС7. Оба шлюза подсоединены к Softswitch. На стороне Softswitch шлюзов SG мы имеем M2UA поверх SCTP поверх IP, а на стороне ОКС7 – стандартную MTP стека ОКС7. В Softswitch мы имеем стандартный протокол MTP3, работающий поверх M2UA и IP. В обычной сети ОКС7 MTP3 использует услуги протокола MTP2. Однако в изображенном на рис. 7.10 сценарии MTP3 в Softswitch использует услуги MTP2, который расположен в SG, не сознавая того, что тот не является локальным. Функция M2UA – обеспечить прозрачный доступ из стандартного MTP3, находящегося в Softswitch к стандартному MTP2, находящемуся в SG.

Поясним это еще подробнее. В предыдущем параграфе наше внимание было сосредоточено на ситуации, в которой Softswitch поддерживает функции ISUP, но не реализует функции нижних уровней стека ОКС7. В частности, MTP3 в самом Softswitch не реализован, что приводит к тому, что Softswitch «не видит» сеть ОКС7, как это может делать любой логический объект, непосредственно

реализующий MTP3. В том числе, он не передает и не принимает сообщения эксплуатационного управления сетью сигнализации. Если же желательно, чтобы Softswitch был вовлечен в эксплуатационное управление сетью сигнализации, то одной из возможностей является реализация MTP3 в Softswitch и использование M2UA поверх SCTP для доступа к функциям MTP2 в SG. Это позволило бы Softswitch лучше «видеть» сеть OKC7, а также теснее взаимодействовать со шлюзом сигнализации SG. Фактически SG становится в таком случае удаленным терминалом сигнализации, составляющим, с точки зрения сети OKC7, логический элемент Softswitch.



NIF = узловая функция взаимодействия

Рис. 7.10. Функции M2UA в Softswitch

В примере на рис. 7.10 приложение MTP3 в Softswitch может принимать такие сигнальные сообщения эксплуатационного управления сетью, как *Transfer Allowed (TFA)* и *Transfer Prohibited (TFP)*. Протокол MTP3 может использовать эту информацию при определении того, каким образом маршрутизировать сообщения такого пользователя MTP3 верхнего уровня, как ISUP.

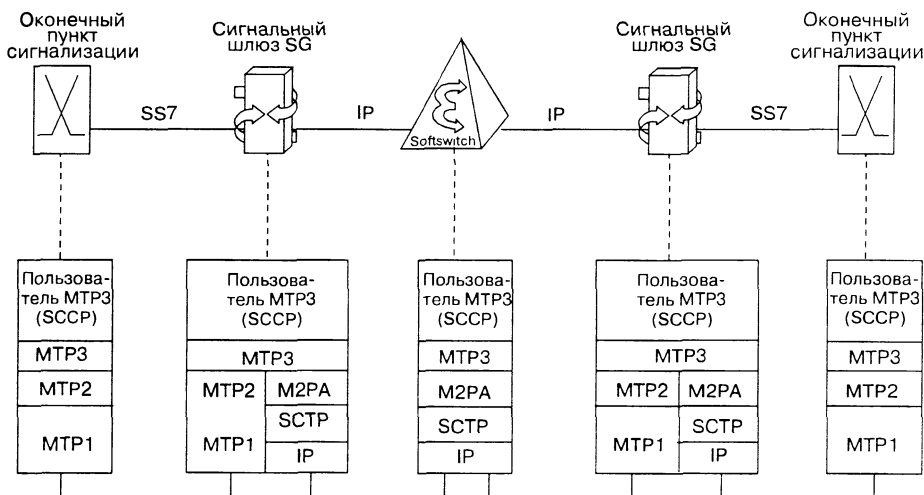
M2UA использует концепции, аналогичные обсуждавшимся в предыдущем параграфе для M3UA. В их число входят понятия AS и ASP. Он предусматривает также аналогичные сообщения, такие как ASPUP, ASPDN, ASPAC, SPIA, NTFY, BEAT, ERR, и соответствующие подтверждения. Эти сообщения используются точно таким же образом, как они используются в M3UA, с той лишь разницей, что протоколы ASP в M2UA выполняют другие функции. В M3UA протокол ASP может иметь отношение к характеристикам, подобным DPC/OPC/диапазон CIC, или другому набору характеристик; а в M2UA протокол ASP является отдельным случаем MTP3 в таком узле, как Softswitch.

Сообщения, которые передаются между одноранговыми объектами M2UA, имеют тот же формат, что и сообщения M3UA (см. рис. 7.9); отличается только поле Message Type общего заголовка. Для M2UA эти сообщения имеют другие коды класса – коды 6 и 10, а сообщения эксплуатационного управления состоянием ASP и трафиком ASP являются общими для всех уровней адаптации. Все эти соображения оправдывают решение авторов сэкономить здесь место на описании сообщений M2UA, функции которых вполне очевидно вытекают из вышеизложенного.

7.6. Протокол M2PA

По уже сложившейся в этой главе традиции, рассмотрим рисунок 7.11, который иллюстрирует область применения M2PA. Идея M2PA – в прозрачном со стороны протокола MTP3 и вышележащих протоколов транзите сигнальных единиц через IP, т. е. для MTP3 протокол M2PA не отличается от традиционного MTP2. Неизменными остаются все функции сетевого уровня ОКС7: балансировка нагрузки между звеньями одного пучка с помощью поля селектора сигнального звена (SLS), обнаружение неисправностей, процедуры переключения на альтернативный маршрут (change-over) и возврата на первоначальный (change-back), контроль перегрузки звена с помощью задаваемых порогов и т. д.

M2PA имеет регистрационный номер порта 3565.



NIF = узловая функция взаимодействия

Рис. 7.11. Функции M2PA в Softswitch

Несмотря на некоторое сходство M2UA и M2PA, между ними есть принципиальные различия. Хотя протокол M2UA и позволяет Softswitch использовать стандартный MTP2 в удаленном сигнальном шлюзе SG, но M2PA более строго соответствует версии MTP2. И показанное на рис. 7.11 соединение SG – Softswitch фактически является звеном ОКС7, тогда как аналогичное соединение на рис. 7.10 таковым не является.

Прямым следствием этой разницы является то, что SG, который использует M2UA, фактически служит для показанного на рис. 7.10 Softswitch удаленным терминалом сигнализации. В то же время SG, который использует M2PA, уже сам по себе является узлом сигнализации; у него есть собственный код пункта сигнализации, и он фактически представляет собой STP на базе IP. Это означает, что SG может выполнять такие функции сигнализации верхнего уровня, как SCCP. Например, SG, использующий M2PA, может выполнять преобразование глобального адреса – Global Title Translation (GTT), – а сигнальный шлюз SG на базе M2UA такие функции выполнять не может.

Выбор между M2UA и M2PA целиком предоставляется проектировщику или Оператору сети. Все зависит от функций, которые должны выполняться в определенных узлах сети. Если, например, SG должен выполнять такие функции, как GTT, то подходящим выбором будет M2PA. С другой стороны, если SG предназначен просто в качестве терминала сигнализации ОКС7 для узла IP-сети (такого как Softswitch), то достаточно будет M2UA.

Теперь несколько слов о реализации этих функций в M2PA. В главе 10 [4] описываются три типа сигнальных единиц ОКС7 на уровне MTP2: значащие сигнальные единицы MSU, которые переносят полезную нагрузку пользователя; единицы LSSU, которые переносят информацию о состоянии сигнального звена, и заполняющие сигнальные единицы FISU, которые передаются, когда другой информации для передачи нет. Протокол M2PA поддерживает сообщения аналогичных типов в IP-сети, за исключением FISU. Отсутствие в M2PA эквивалента FISU объясняется принципами функционирования IP-сети, что же касается корректной работы трактов сигнализации в IP-сети, то для этого используется вышеупомянутое сообщение SCTP BEAT, а сообщения M2PA для пересылки данных включают в себя функции подтверждения. Т.о., в M2PA имеются два сообщения: сообщение User Data и сообщение Link Status.

Сообщение User Data в M2PA является просто сигнальной единицей MSU, из которой исключено несколько стандартных полей ОКС7, и содержит индикатор длины LI (Length Indicator), октет служебной информации SIO (Service Information Octet) и поле сигнальной информации SIF (Signaling Information Field). Поля Flag, Backward Sequence Number (BSN), Backward Indicator Bit (BIB),

Forward Sequence Number (FSN), Forward Indicator Bit (FIB) и Check Bits в состав User Data не входят. LI включен в состав User Data только потому, что некоторые национальные варианты ОКС7 используют два резервных бита LI в качестве указателя приоритета.

Сообщениями Link Status обмениваются одноранговые объекты M2PA, чтобы информировать друг друга о текущем состоянии тракта. Link Status аналогично LSSU в ОКС7 и тоже содержит поле status (состояние), которое может принимать следующие значения:

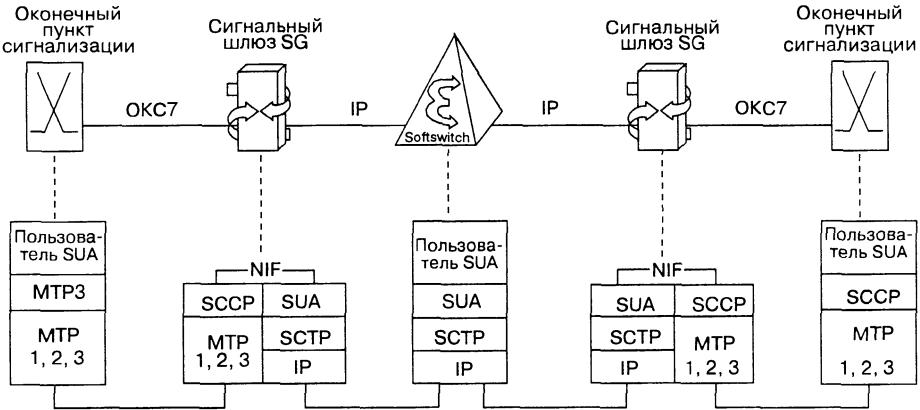
- Alignment (фазирование);
- Proving Normal (подтверждение нормального состояния);
- Proving Emergency (подтверждение аварийного состояния);
- Ready (готовность);
- Processor Outage (повреждение процессора);
- Processor Outage Ended (восстановление процессора);
- Busy (занят);
- Busy Ended (освободился);
- Out of Service (выведен из обслуживания);
- In Service (введен в обслуживание).

7.7. Протокол SUA

SUA – протокол транспортировки информации SCCP через сеть IP (Transporting SCCP over IP) определен рабочей группой Sigtran для транспортировки по сети IP с использованием SCTP сигнальных сообщений подсистемы SCCP стека ОКС7 (несущих, в первую очередь, информацию TCAP и RANAP). В сущности, SUA дублирует услуги SCCP путем поддержки надежной пересылки сообщений пользователя SCCP, включая поддержку услуг как без соединения (класс 0 и 1), так и ориентированных на соединение (класс 2 и 3). SUA поддерживает также услуги эксплуатационного управления SCCP, предназначенные для управления состоянием удаленных пунктов назначения и подсистем SCCP. Кроме того, в некоторых конфигурациях SUA выполняет еще и функции преобразования адреса и маршрутизации.

Таким образом, протокол SUA обеспечивает взаимодействие с сетью ОКС7 на более высоком уровне, чем это делает M3UA (и, тем более, M2UA, M2PA). В сигнальном шлюзе завершают работу (терминируются) протоколы MTP и SCCP, а до ASP передается лишь полезное содержимое сообщений SCCP. Протокол SUA имеет зарегистрированный IANA номер порта 14001. Он имеет также зарегистрированный IANA идентификатор протокола полезной нагрузки SCTP, равный 4.

Для транспортировки сообщений без соединения SCCP и SUA сопрягаются в шлюзе SG. Именно там (с точки зрения пункта сигнализации ОКС7) расположен пользователь SCCP. Сообщения ОКС7 маршрутизируются к SG на основе кода пункта сигнализации и номера подсистемы SCCP, а затем шлюз сигнализации маршрутизирует сообщения SCCP к удаленному оконечному пункту IP. Если существуют резервные оконечные пункты IP, шлюз сигнализации может поделить нагрузку между активными оконечными пунктами IP, используя циклический метод.



NIF = узловая функция взаимодействия

Рис.7.12. Функции SUA в Softswitch

Заметим, что при распределении нагрузки, создаваемой сообщениями TCAP, выбор оконечного пункта пересылки происходит только для первого сообщения в диалоге TCAP. Следующие сообщения в том же диалоге TCAP всегда передаются в оконечный пункт, который выбран для первого сообщения, пока не будет получена информация о состоянии оконечных пунктов, и сигнальный шлюз не будет информирован о стратегии распределения сообщений оконечных пунктов IP.

Формат общего заголовка сообщения и TLV, ранее определенный для M3UA, в равной мере применяется и для SUA. В табл. 7.3 приводится список классов и типов сообщений SUA.

Таблица 7.3. Классы и типы сообщений SUA

Код класса сообщения	Наименования класса и типа сообщения	Код типа сообщения
0	Management (MGMT) messages	
	Error message	0
	Notify message	1
2	SS7 Signaling Network Management (SSNM) messages	
	Destination Unavailable (DUNA)	1
	Destination Available (DAVA)	2
	Destination State Audit (DAUD)	3
	Signaling Congestion (SCON)	4
	Destination User Part Unavailable (DUPU)	5
	Destination Restricted	6
3	ASP State Maintenance (ASPSM) messages	
	ASP Up	1
	ASP Down	2
	Heartbeat	3
	ASP Up Acknowledge	4
	ASP Down Acknowledge	5
	Heartbeat Acknowledge	6
4	ASP Traffic Maintenance (ASPTM) messages	
	ASP Active	1
	ASP Inactive	2
	ASP Active Acknowledge	3
7	Connectionless (CL) Messages	
	Connectionless Data Transfer (CLDT)	1
	Connectionless Data Response (CLDR)	2
8	Connection-oriented (CO) messages	
	Connection Request (CORE)	1
	Connection Acknowledge (COAK)	2
	Connection Refused (COREF)	3
	Release Request (RELRE)	4
	Release Complete (RELCO)	5
	Reset Confirm (RESCO)	6
	Reset Request (RESRE)	7
	Connection-oriented Data Transfer (CODT)	8
	Connection-oriented Data Acknowledge (CODA)	9
	Connection-oriented Error (COERR)	10
9	Inactivity Test (COIT)	11
	Routing Key Management (RKM) messages	
	Registration Request	1
	Registration Response	2
	Deregistration Request	3
	Deregistration Response	4

Сообщения без соединения используются для трафика класса 0 и класса 1 протокола.

Существуют два сообщения без соединения: CLDT и CLDR:

- Сообщение Connectionless Data Transfer соответствует сообщениям unitdata (UDT), extended unitdata (XUDT) и long unitdata (LUDT) в SSCP. Оно используется для пересылки данных между одноранговыми SUA для трафика класса 0 и класса 1.
- Сообщение Connectionless Data Response соответствует сообщениям услуги unitdata (UDTS), услуги extended unitdata (XUDTS) и услуги long unitdata (LUDTS) в SSCP. Оно передается как ответ в CLDT, чтобы информировать об ошибках в сообщении CLDT, если используется соответствующая опция.

Сообщения, ориентированные на соединение, используются для трафика протокола класса 2 и класса 3:

- Connection Request (CORE) используется, чтобы запросить сигнальное соединение между двумя оконечными пунктами. Это сообщение соответствует сообщению Connection Request (CR) в SSCP.
- Connection Acknowledgement (COAK) используется для положительного ответа на Connection Request. Это сообщение соответствует сообщению Connection Confirm (CC) в SSCP.
- Connection Refusal (COREF) используется для отрицательного ответа на запрос Connection Request. Это сообщение соответствует сообщению Connection Refusal (CREF) в SSCP.
- Connection-oriented Data Transfer (CODT) используется для передачи данных по сигнальному соединению. Оно соответствует сообщениям Data Form 1 (DT1), Data Form 2 (DT2), и Expedited Data (ED) в SSCP.
- Connection-oriented Data Acknowledgement (CODA) используется одноранговым оконечным пунктом для подтверждения получения данных. Это сообщение используется только для сообщений протокола класса 3. Оно соответствует сообщению Data Acknowledgement (AK) в SSCP.
- Release Request (RELRE) используется для запроса разрушить сигнальное соединение. Это сообщение соответствует сообщению Connection Released (RLSD) в SSCP.
- Release Complete (RELCO) используется для подтверждения разрушения сигнального соединения. Все ресурсы, отведенные соединению, должны быть освобождены. Это сообщение соответствует сообщению Release Complete (RLC) в SSCP.

- Reset Request (RESRE) используется для запроса начать заново присвоение порядковых номеров сообщениям в пункте-отправителе и в пункте-получателе, которые ассоциированы с сигнальным соединением. Это сообщение соответствует сообщению Reset Request (RSR) в SCCP.
- Connection-oriented Error (COERR) используется для того, чтобы указать, что в протокольном блоке данных была ошибка. Это сообщение соответствует сообщению Protocol Data Unit Error (ERR) в SCCP.
- Connection-oriented Inactivity Test (COIT) соответствует сообщению Inactivity Test (IT) в SCCP.

SUA поддерживает те же сообщения *MGMT*, что и M3UA, но предоставляет также информацию о состоянии подсистемы SCCP. Сообщения DUNA, DAVA, DRST, SCON и DAUD могут опционально содержать номер подсистемы SubSystem Number (SSN). Кроме того, сообщения DUNA, DAVA, DRST и SCON могут опционально содержать параметр SubSystem Multiplicity Indicator (SMI).

SUA поддерживает те же сообщения *RKM*, что и M3UA, но параметр Routing Key отличается тем, что он содержит опции для адресов источника и пункта назначения и для диапазонов адресов.

В заключение отметим, что, с одной стороны, за счет терминирования в сигнальном шлюзе «лишнего» протокола достигается более эффективное использование полосы пропускания IP-сети, но, с другой стороны, по этой же причине теряется возможность передачи через SUA информации протокола ISUP, так как для адресации SUA использует уровень MTP3 ОКС7.

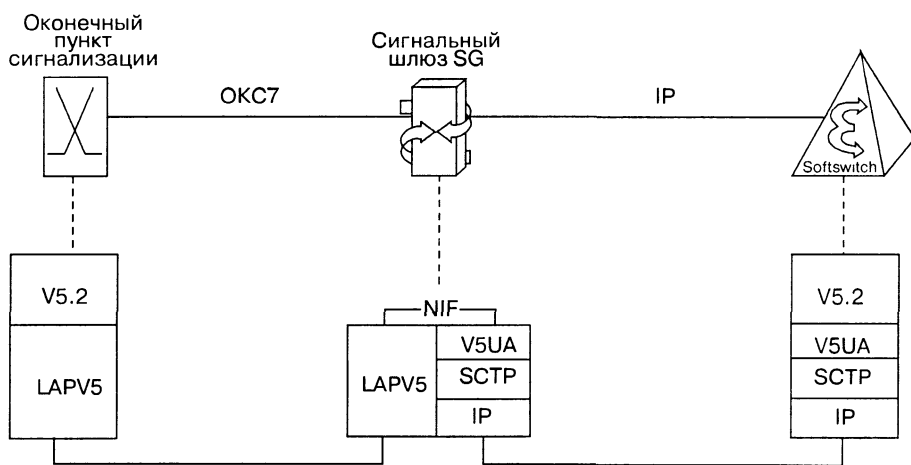
Сигнальный шлюз может выполнять *преобразование глобальных адресов GTT (Global Title Translation)* для определения пункта назначения сообщения SCCP. Сигнальный шлюз маршрутизирует сообщения по глобальному адресу, который представляет собой такие цифры, присутствующие во входящем сообщении, как номер вызываемой стороны или идентификационный номер мобильного абонента. Для транспортировки сообщений, ориентированной на соединение, SCCP и SUA сопрягаются в сигнальном шлюзе, чтобы объединить два участка соединения, необходимых при ориентированной на соединение пересылке данных между окончательным пунктом сигнализации ОКС7 и окончательным пунктом IP. Маршрутизация сообщений производится сигнальным шлюзом к сигнальным пунктам ОКС7 на основе кода пункта назначения (в поле адреса MTP3) и к окончательным пунктам IP на основе IP-адреса (в заголовке SCTP).

7.8. Протокол IUA

В ISDN сигнальную информацию пользователя, например, сообщения Q.931, переносит звеньевой уровень Q.921. Эквивалентной спецификацией Sigtran в сети IP является IUA. Кадры Q.921 могут пропускаться из ISDN в сеть IP с идентичными реализациями Q.931 в каждой сети, причем ни одна из них не распознает никаких различий в лежащей в основе транспортировке. Протокол IUA определен в документе RFC 3057 для поддержки протоколов Q.931 и QSIG, причем, эта поддержка распространяется как на доступ ISDN на первичной скорости (PRA), так и на базовый доступ ISDN (BRA). Предложены также расширения IUA для DPNSS/DASS2. Регистрационный номер порта для IUA равен 9000.

7.9. Протокол V5UA

Универсальный интерфейс сети доступа V5.2 поддерживает подключение к местной АТС аналоговых телефонных линий, доступ ISDN на базовой скорости, доступ ISDN на первичной скорости и абонентский доступ других типов, как это описано в [5] и, более детально, в [11]. Т.к. в процессе конвергенции сетей связи и перехода к NGN местные АТС заменяются управляемыми Softswitch медиа-шлюзами, то между системой доступа и Softswitch понадобится SG, как показано на рис. 7.13. Протокол V5UA дает возможность приложениям V5.2 в Softswitch использовать в шлюзе SG на стороне сети доступа собственные функции V5.2. Протокол V5UA имеет регистрационный номер порта 5675.



NIF = узловая функция взаимодействия

Рис. 7.13. Функции V5UA в Softswitch

Глава 8

Протокол ВІСС

*Теории ничего не доказывают, зато позволяют выиграть
время и отдохнуть, если ты совсем запутался,
стараясь найти то, что найти невозможно.*
Марк Твен

8.1. Стандартизация ВІСС

Для взаимодействия Softswitch между собой теоретически должен применяться именно протокол *BICC* (*Bearer independent call control protocol*), разработанный Международным союзом электросвязи ITU-T. И хотя на практике более популярным становится второй протокол – SIP (SIP-T), разработанный IETF и рассмотренный в главе 4 книги, протокол ВІСС успешно используется до сих пор, например, в весьма удачных Softswitch платформы ENGINE компании Ericsson, о чем мы еще поговорим в главе 10.

Работа над созданием протокола управления обслуживанием вызова независимо от носителя (несущего канала) *BICC* была начата Исследовательской комиссией 11 (ИК-11) ITU-T в марте 1999 года. Обязательным требованием была поддержка сигнальных сообщений ISUP, поскольку протокол должен был облегчить Операторам переход к мультисервисным сетям и обеспечить взаимодействие новой мультисервисной сети с существующими сетями ISDN. Фактически протокол ВІСС рассматривался как еще одна прикладная подсистема общеканальной сигнализации ОКС7, обеспечивающая экономичный переход к мультисервисной сети с сохранением большей части сигнального оборудования ISUP сетей с временным разделением каналов TDM.

Как подчеркивает эпиграф к этой главе, протокол ВІСС, равноправие которого с SIP сегодня носит, в основном, теоретический характер, в свое время позволил выиграть время при решении проблемы нехватки сетевых ресурсов, возникшей перед рядом Операторов, не желавших вкладывать инвестиции в дальнейшее

развитие TDM-сетей. Для них протокол BICC должен был (и сумел) обеспечить возможность предоставлять уже существующие услуги ТФОП/ISDN в пакетных сетях, а также поддерживать взаимодействие имеющихся узлов коммутации TDM с узлами пакетной сети и взаимодействие узлов коммутации TDM через пакетную сеть.

По этой причине протокол BICC должен был базироваться исключительно на подсистеме ISUP стека ОКС7. Чтобы не пришлось разрабатывать две отдельные технологии, одна из которых переносила бы ISUP в IP-окружение, а другая обеспечивала взаимодействие между пакетной и TDM-сетью, для BICC было принято требование полной совместимости протокола с существующей сетью коммутации каналов, но, в то же время, способности работать с любой транспортной технологией, которая может обеспечить приемлемое качество передачи речевого трафика. Были сформированы основные принципы разрабатываемого протокола BICC:

- протокол основан на ISUP, чтобы быть полностью совместимым с существующими услугами и сетями TDM;
- протокол независим от транспортной технологии;
- протокол использует уже существующие сигнальные протоколы для установления соединений в транспортных сетях.

Единственной доработкой протокола ISUP для BICC стало усовершенствование обслуживания вызовов абонентов мобильных сетей, сделанное из-за того, что многие Операторы стационарной связи предоставляют свои сети для передачи трафика Операторов мобильной связи. Ранее качество передачи речевой информации при этом ухудшалось из-за кодирования и декодирования трафика, соответственно, на входе и на выходе проводной сети. Возможность сигнализировать об используемом кодеке и согласовать выбор наилучшего кодека для обслуживаемого вызова оказалось легко добавить в BICC, не ухудшая при этом его совместимости с ISUP.

Подготовленные ИК-11 рекомендации BICC имеют индексы Q.1900 – Q.1999, причем стандартизация протокола BICC проходила в несколько этапов, начиная с набора возможностей *CS1 (Capability Set 1)*, ориентированного на взаимодействие узлов ISDN через сети ATM. Основная рекомендация для BICC – Q.1901 – представляет собой так называемый delta-документ, т.е. документ, описывающий отличия от существующих рекомендаций ISUP Q.761 – Q.764.

Следующий за ним CS2 уже ориентировался на сети IP, для чего в рекомендации Q.1970 был предложен новый протокол *IPBCP (IP Bearer Control Protocol)*, и появилась еще одна рекомендация Q.1990, посвященная туннелированию сигнальной информации в IP-сети. Сам набор возможностей CS2 описывается рекомендацией Q.1902 (Q.1902.1 – Q.1902.6). Кроме того, потребовалось внести дополнения в другие, уже существующие рекомендации, в частности,

в Q.765, описывающую Application Transport Mechanism. Благодаря тому, что все процедуры, связанные с преобразованием транспортлируемых сообщений, были удалены из протокола и переданы функциональной единице, получившей название *Signaling Transport Converter (STC)*, была достигнута полная независимость BICC от транспортной технологии. Варианты STC для транспорта каждого вида описываются дополнительными рекомендациями ITU-T и документами других стандартизирующих организаций. Так, например, конвертер для транспортных услуг MTP частично рассмотрен в приложении к рекомендации Q.1901. Конвертер для транспортной технологии ATM описан руководящими документами ATM-форума (AF-CS-VMOA-0146.000). В принципе, ничто не мешает дополнять BICC новыми наборами возможностей, что позволяет этому протоколу работать с любой транспортной технологией. Так, например, набор возможностей CS3 обеспечивает поддержку новых инфокоммуникационных услуг и взаимодействие с протоколом SIP-T.

Как сказано выше, одним из принципов BICC является использование существующих сигнальных протоколов, следовательно, принимая во внимание три поддерживаемые технологии, BICC умеет взаимодействовать с сигнализацией:

- ATM Forum UNI4.0 и ITU-T DSS2 для доступа ATM;
- ITU-T B-ISUP, ATM Forum PNNI и AINI для магистральной сети ATM;
- AAL Type 2 – для управления носителем в ATM;
- SDP – для IP сетей.

8.2. Архитектура протокола BICC

Начнем рассмотрение архитектуры BICC с узлов обслуживания сети *Serving Nodes (SN)* и разберемся со связанной с ними терминологией. Архитектура BICC подразумевает, что вызовы будут входить в сеть и выходить из нее с поддержкой BICC через интерфейсные узлы обслуживания – *Interface Serving Nodes (ISN)*, – предоставляющие сигнальные интерфейсы между узкополосной ISUP (сетью ТфОП/ISDN с коммутацией каналов) и одноранговым узлом ISN (находящимся в пакетной сети).

Кроме функции интерфейса между двумя подсистемами ISUP через домен BICC имеется возможность взаимодействия двух разных Операторов связи, у каждого из которых свой BICC-домен. Узел, исполняющий роль шлюза в каждом из доменов BICC, получил название пограничный узел обслуживания – *Gateway Serving Node (GSN)*. Он обеспечивает соединение двух областей BICC, принадлежащих разным Операторам, и это соединение состоит из двух узлов GSN, непосредственно связанных друг с другом.

Если два оператора могут взаимодействовать друг с другом, то должно быть также возможным, чтобы каждый из них мог предоставлять услуги ТфОП/ISDN внутри своей сети. Узел, который будет это выполнять, аналогичен по своим функциям транзитной АТС и называется транзитным узлом обслуживания – *Transit Serving Node (TSN)*.

На рис. 8.1 представлены узлы всех рассмотренных типов. Имеются также промежуточные коммутаторы, через которые тракт проключается при помощи сетевой сигнализации. Эти коммутаторы характерны для сетей АТМ и в терминах BICC называются узлами ретрансляции носителя – *Bearer Relay Nodes (BRN)* или коммутирующими узлами – *Switching Nodes (SWN)*, но не все сетевые технологии требуют их наличия.

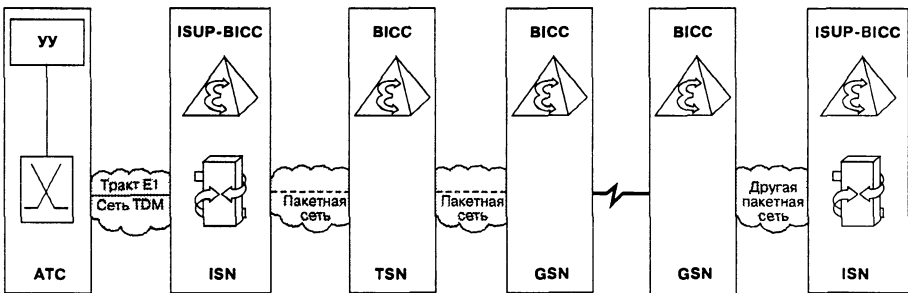


Рис. 8.1. Узлы обслуживания BICC

Структура каждого из вышеупомянутых узлов соответствует модели протокола BICC, представленной на рис. 8.2.

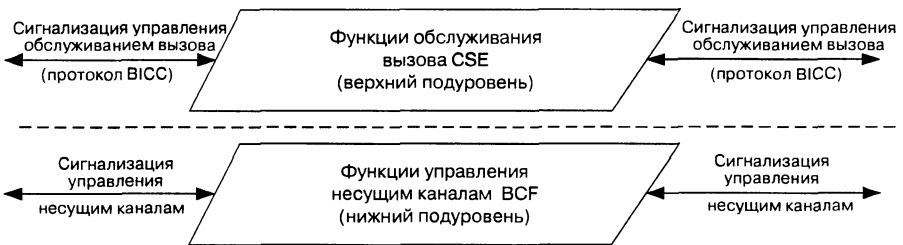


Рис. 8.2. Структура узла обслуживания в соответствии с CS1

На нижней плоскости размещены отделенные от BICC-протокола сигнализации управления обслуживанием вызова и, следовательно, не рассматриваемые в нем, функции подуровня управления носителем *BCF (Bearer Control Function)*, которые подразделяются на 4 типа: *BCF-N*, *BCF-T*, *BCF-G* и *BCF-R*. Первые три обеспечивают управление функцией коммутации несущего канала, содержат средства для взаимодействия с ассоциированной с ними *CSF (Call*

Service Function) и средства сигнализации, необходимые для организации несущего канала к другой одноранговой *BCF* и для разрушения этого канала. *BCF-R* обеспечивает управление коммутацией несущего канала и передает запросы управления несущим каналом к следующей *BCF* для сквозного обмена сигнальной информацией. Что же касается верхней плоскости обслуживания вызова, т.е. подуровня, на котором функционирует сигнализация BICC, то здесь присутствуют функции обслуживания вызовов *CSF* четырех типов:

- узловая функция обслуживания вызова *CSF-N (Nodal)*, которая реализует действия узла, связанные с управлением узкополосными услугами, и поддерживает взаимодействие между сигнализацией ISDN и BICC, передавая одноранговой функции *CSF* данные о вызове и обращаясь к функции *BCF-N*, необходимой для переноса трафика узкополосной услуги к/от опорной сети;
- транзитная функция обслуживания вызова *CSF-T (Transit)*, которая реализует действия, требующиеся для создания и поддержания сеанса связи и необходимого для него носителя в опорной сети, ретранслируя сигналы между одноранговыми *CSF* и обращаясь к функции *BCF-T*, обеспечивающей перенос трафика узкополосной услуги в опорной сети;
- шлюзовая функция обслуживания вызова *CSF-G (Gateway)*, которая реализует действия, нужные при предоставлении услуги через шлюз и требующиеся для установления и поддержания сеанса связи и необходимого для него носителя в опорной сети, ретранслируя сигналы между одноранговыми *CSF* и обращаясь к функции *BCF-G*, обеспечивающей перенос трафика узкополосной услуги между разными опорными сетями;
- функция координации обслуживания вызовов *CSF-C (Coordination)*, которая реализует координацию действий по обслуживанию вызова и посреднические действия, необходимые для установления и поддержания сеанса связи в опорной сети, ретранслируя сигналы между одноранговыми *CSF*. *CSF-C* не имеет никакой связи с какой-либо *BCF*, а является только функцией управления обслуживанием вызова.

В узлах BICC формируется функция взаимодействия несущих каналов *BIWF (Bearer InterWorking Function)* – функциональная единица, поддерживающая функции управления несущим каналом (*BCF*) и функции мэйпинга/коммутации в SN. *BIWF* содержит один блок *BCF*.

Оперируя имеющейся у нас теперь терминологией, можно посмотреть, что представляют собой три описанных ранее типа узлов обслуживания SN с точки зрения протокола BICC.

Функциональный объект *Interface Serving Node (ISN)* содержит блок узловой функции обслуживания вызовов *CSF-N* и один или

более блоков функций взаимодействия несущих каналов *BIWF*, которые взаимодействуют с сетью коммутации каналов *SCN* (*Switched Circuit Network*) и одноранговыми блоками в опорной сети.

Функциональный объект *Transit Serving Node* (*TSN*) содержит функцию обслуживания вызовов *CSF-T* и поддерживает один или более блоков функций взаимодействия несущих каналов *BIWF*. *TSN* взаимодействуют с другими *TSN*, *GSN* и *ISN* в собственном домене базовой сети.

Функциональный объект *Gateway Serving Node* (*GSN*) содержит функцию обслуживания вызовов *CSF-G* и один или более блоков межсетевого взаимодействия несущих каналов *BIWF*. *GSN* взаимодействуют с другими *GSN* в других доменах базовой сети и с другими *ISN* и *TSN* в собственном домене базовой сети.

Узлы *SWN* содержат единственную функцию – функцию коммутации *BCF-R*.

Одним из основных требований к протоколу *BICC* является поддержка всех существующих узкополосных услуг, поэтому архитектура *BICC* должна обеспечить предоставление услуг Интеллектуальных сетей (*IN*) точно так, как они предоставляются в ТФОП/*ISDN*. Для поддержки функций Интеллектуальной сети [7] вводится узел архитектуры *BICC* еще одного типа – так называемый *Call Mediation Node* (*CMN*). Фактически *CMN* – это частный случай узла *TSN*, а именно *TSN*, не имеющий пользовательского подуровня (или «пользовательской плоскости»), т.е. на него не поступает и через него не проходит транзитом пользовательский трафик. Пользуясь введенной выше терминологией *BICC*, можно сказать, что *CMN* – это узел, который выполняет функцию управления обслуживанием вызова *CSF*, но не имеет связанной с ней *BCF*.

Прежде чем перейти к последовательному рассмотрению двух специфицированных наборов возможностей *CS1* и *CS2*, приведем структуру протокола *BICC* (рис. 8.3), которая должна чуть больше разъяснить общую картину функционирования протокола. Блок процедур *BICC* включает в себя функции элемента *CSF*. Функции протокольного элемента *BCF* распределены между блоками функций мэппинга и блоками управления несущим каналом. Блок функций мэппинга используется блоками *BCF* при получении/передаче сигнальных сообщений управления несущим каналом для их преобразования, при этом используется универсальный интерфейс.

Для получения/передачи сообщений *BICC* используется универсальный интерфейс с конвертером транспортировки сигнализации *STC* (*Signaling Transport Converter*). Поскольку посредством этого конвертера протокол *BICC* обеспечивает свою независимость от транспортной технологии, необходимо определять интерфейсы *STC* с разными системами транспортировки сигнальных сообщений и с блоками функций управления носителем.

8.3. Capability Set 1

Прежде чем начать рассмотрение структурно-архитектурных особенностей CS1, приведем список услуг, которые, исходя из требований, предъявляемых к BICC, должны поддерживаться им уже в первой реализации, то есть в CS1. Предусмотренные протоколом BICC CS1 возможности базового обслуживания вызова представлены в табл. 8.1. Протоколом BICC CS1 поддерживаются также дополнительные услуги, приведенные в табл. 8.2.

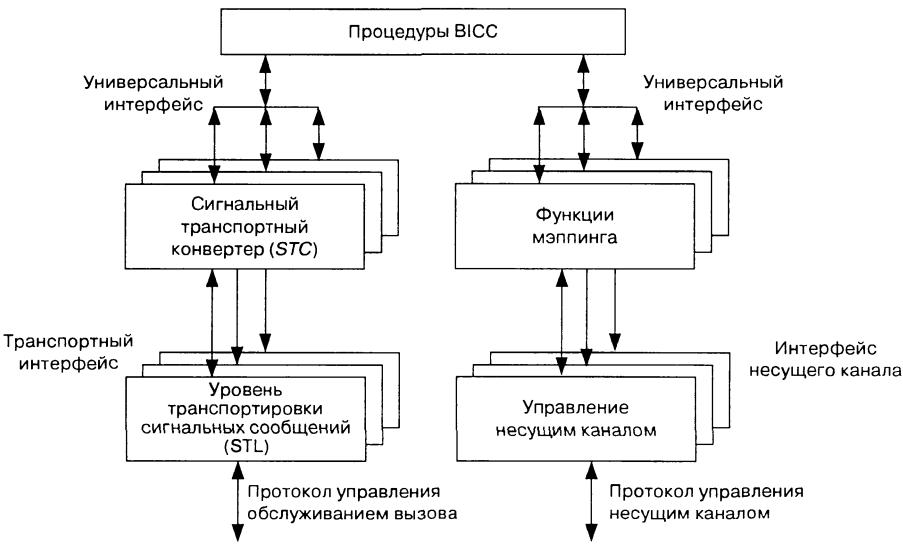


Рис. 8.3. Структура протокола BICC

Как уже подчеркивалось выше, BICC CS1 проектировался для того, чтобы позволить традиционным Операторам, эксплуатирующим сети ОКС7 с передачей информации ISUP поверх MTP3 в TDM-трактах, довольно просто перейти к использованию альтернативных пакетных технологий. В частности, BICC CS1 позволяет поместить ATM-сегмент в существующую узкополосную сеть ISUP без ущерба для функциональных возможностей или услуг ISUP и IN. Будучи преемником ISUP, протокол BICC перенял все его функции и услуги, которые применимы в архитектуре с отделенным носителем. Те же сигналы, которые не относятся к BICC, могут прозрачно передаваться между двумя узлами ISDN, соединенными посредством BICC. Таким образом, при предоставлении услуг не происходит потерь.

Таблица 8.1. Возможности базового обслуживания вызова

Функция/Услуга	Националь- ное приме- нение	Междуна- родное при- менение
Речь/аудио 3.1 КГц	√	√
Доступ 64 Кбит/с	√	√
Мультискоростное подключение	√	√
Подключение N × 64 Кбит/с	√	√
Блочная передача адресной информации	√	√
Передача адресной информации с перекрытием	√	√
Выбор транзитной сети	√	—
Проверка целостности	Примеч. 1	Примеч. 1
Прямая передача	—	√
Простая сегментация	√	√
Речевые объявления и акустические сигналы	√	√
Доставка информации доступа	√	√
Передача пользовательской информации	√	√
Прерывание и возобновление	√	√
Сигнальные процедуры для перехода на аварийный режим	√	√
Процедура определения задержки	√	√
Расширенные сигнальные процедуры echo control	—	—
Упрощенные сигнальные процедуры echo control	√	√
Попытка автоматического повторения	√	√
Блокировка/Отмена блокировки	√	√
Запрос группы каналов	√	—
Двойное занятие	√	√
Обработка вызывного сигнала для цифровых межстанцион- ных линий	—	—
Возврат в исходное состояние	√	√
Получение не подходящей (не по контексту) сигнальной ин- формации	√	√
Процедуры совместимости	√	√
Временная блокировка магистральной линии	—	—
Контроль перегрузки сигнализации ISUP	Примеч. 2	Примеч. 2
Автоматический контроль перегрузки	√	√
Взаимодействие N-ISDN и INAP	√	√
Не поддерживаемое значение circuit identification code	√	—
Контроль доступности ISUP	Примеч. 3	Примеч. 3
Пауза/прекращение паузы MTP	Примеч. 2	Примеч. 2
Поддержка сообщений с длиной, большой максимальной	√	√
Временный альтернативный маршрут (TAR)	√	√
Процедура подсчета межузловых переприемов	√	√
Процедура Collect call request	√	√
Hard-to-reach	√	√
Запрос информации о географических координатах вызыва- емого абонента	√	√

ПРИМЕЧАНИЕ 1 — функция проверки целостности не поддерживается, но это не препятствует правильному выполнению операций процедуры проверки целостности в предшествующей или в последующей SCN.

ПРИМЕЧАНИЕ 2 — Если BICC развернут на уровне MTP3 или MTP3B, то эти функции обеспечиваются подуровнем STC.

ПРИМЕЧАНИЕ 3 — Если BICC развернут на уровне MTP3 или MTP3B, эквивалентная процедура обеспечивается подуровнем STC.

Таблица 8.2. Дополнительные услуги базового обслуживания вызова

Дополнительные услуги	Аббревиатура
Прямой набор номера абонента УАТС	DDI
Множественный абонентский номер	MSN
Идентификация вызывающей линии	CLIP
Запрет идентификации вызывающей линии	CLIR
Идентификация подключенной линии	COLP
Запрет идентификации подключенной линии	COLR
Идентификация злонамеренного вызова	MCID
Субадресация	SUB
Переадресация при занятости абоненте	CFB
Переадресация при отсутствии ответа абонента	CFNR
Безусловное переадресация	CFU
Отклонение вызова на другой номер	CD
Переключение связи	ECT
Вызов на ожидании	CW
Удержание	HOLD
Завершение установления соединения при занятости абонента	CCBS
Завершение установления соединения при отсутствии ответа	CCNR
Возможность переноса терминала	TP
Конференцсвязь	CONF
Трехсторонняя связь	3PTY
Замкнутая группа пользователей	CUG
Многоуровневый приоритет	MLPP
Услуга глобальной виртуальной сети	GVNS
Международные карты оплаты	ITCC
Возможность относить начисление платы за связь на входящую сторону	REVC
Сигнализация пользователь-пользователь	UUS

Обмен сигнальной информацией между двумя разными интерфейсами сигнализации должна выполняться так, как если бы ISN был промежуточным узлом ISUP. Более того, так как оба протокола (BICC и ISUP) используют сигнальную информацию, описанную рекомендацией ITU-T Q.763, то поддерживается и совместный мэппинг. Как уже упоминалось, в BICC были добавлены новые опции, отсутствовавшие в ISUP: согласование характеристик кодека (*codec negotiation*) и модификация кодека (*codec modification*). Это избавило BICC от необходимости транскодирования в опорной сети, что улучшило качество передачи речевой информации при транзите трафика между двумя сетями TDM.

Взаимодействие BICC с ISUP внутри узла изображено на рис. 8.4.

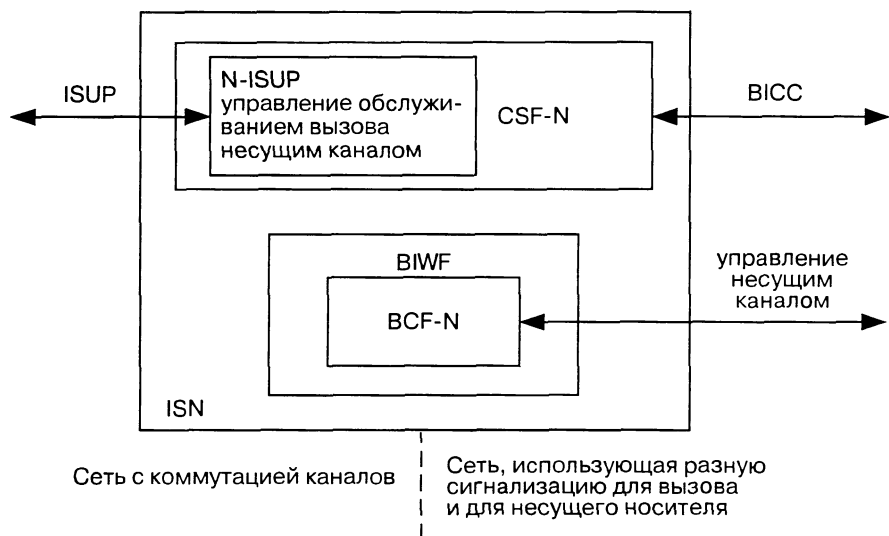


Рис. 8.4. Функциональная модель ISUP/ISN

Рассмотрим более подробно функциональную структуру узла BICC CS1 (рис. 8.5). Для этого еще раз, но уже более строго, опишем задачи, возлагаемые на компоненты узла.

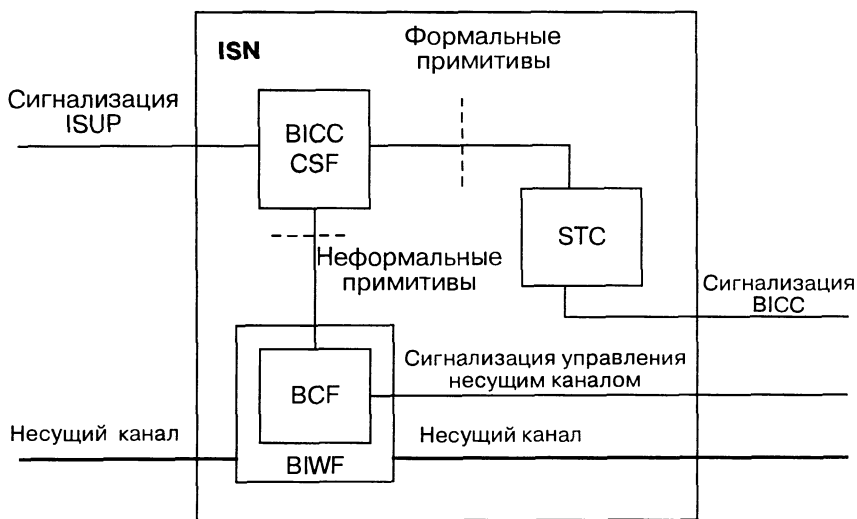


Рис. 8.5. Функциональные компоненты узла ISN в BICC CS1

Функция CSF обеспечивает взаимодействие с традиционной сигнализацией ISUP TDM-области, предоставляет интерфейс с транспортно-зависимым сигнальным конвертером (STC), предоставляет общий интерфейс с функциями BIWF/BCF. Сигнальный транспортный конвертер STC производит привязку общих сообщений BICC к сигнализации транспортной сети. В BICC CS1 определены STC для трех систем сигнализации: MTP3/3B, SSCOP и SSCOPMCE.

Функция BIWF обеспечивает взаимодействие между различными транспортными технологиями (например, TDM и ATM). BCF предоставляет средства соответствующей системы сигнализации транспортной сети для организации несущих каналов, которые впоследствии будут использоваться при обслуживании вызовов BICC.

Для управления BIWF/BCF функцией CSF в BICC CS1 служит общий интерфейс, обмен информацией через который происходит посредством примитивов, рассматриваемых ниже. Чтобы обеспечить корректное взаимодействие узлов ISN разных модификаций и производителей, необходимо специфицировать привязку BICC к каждой технологии транспортной сети. В CS1 такая привязка была определена комитетом ITU-T для интерфейсов:

- AAL1, использующего сигнализацию DSS2;
- AAL1, использующего сигнализацию B-ISUP;
- AAL2, использующего сигнализацию AAL2 (CS1).

В дополнение к этому, ATM-форум определил привязки BICC для интерфейсов:

- AAL1, использующего сигнализацию ATM-F UNI;
- AAL1, использующего сигнализацию ATM-F PNNI;
- AAL1, использующего сигнализацию ATM-F AINI.

Материал этого и предыдущего параграфов позволяет нам перерисовать рис. 8.1 в более строгом виде, соответствующем общей архитектуре сети BICC для CS1, как это представлено на рис. 8.6.

8.4. Система транспорта сигнализации

Продолжая обсуждение архитектуры BICC CS1, рассмотрим подробнее систему транспорта сигнализации, т.к. она будет использоваться и в CS2, и в CS3. К тому же, она является одной из главных составляющих протокола BICC.

Система транспорта сигнализации находится, так сказать, на границе протокола BICC. Предусматривается по одному уже рассматривавшемуся выше объекту STC (*signaling transport converter*) на каждую сигнальную связь. Протокол BICC передает или принимает сообщения этой сигнальной связи, используя соответствующую точку доступа к услуге SAP (*Service Access Point*).

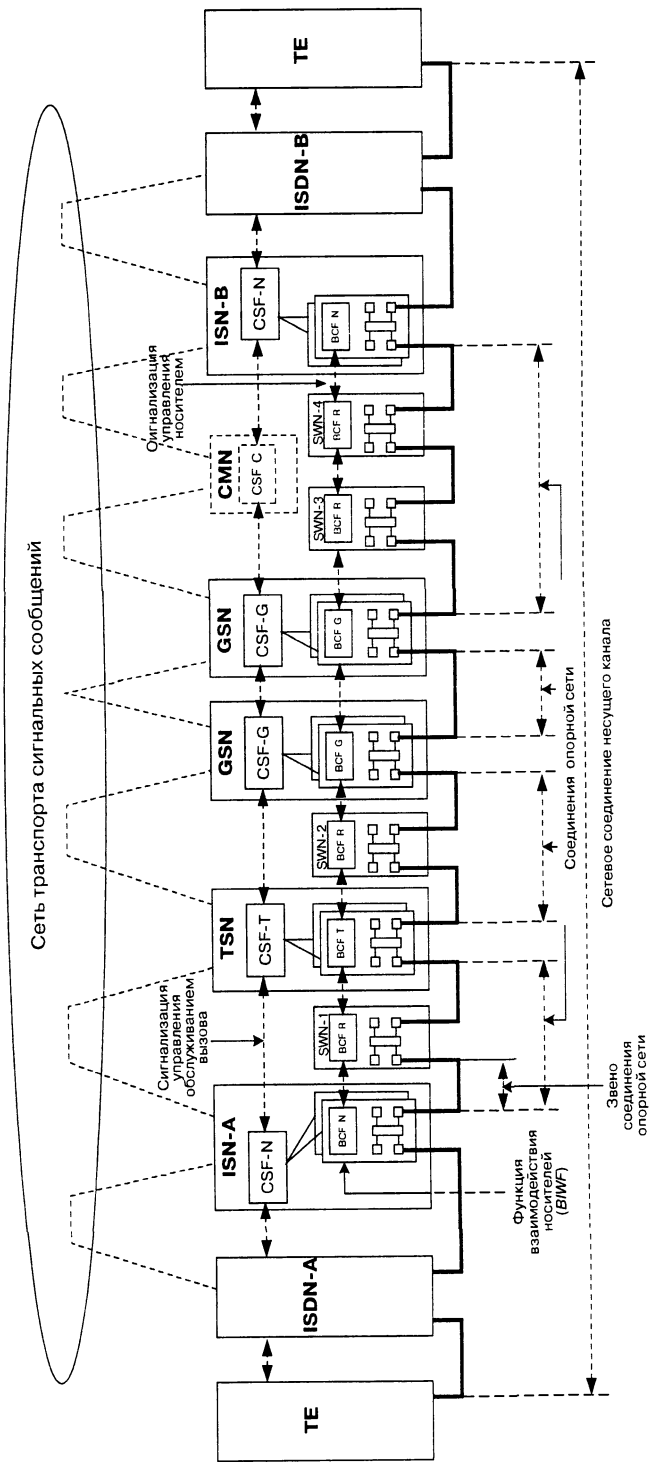


Рис. 8.6. Архитектура сети BICC CS1

Два равнозначных блока CSF для уверенной передачи информации между ними и индикации доступности услуг используют услугу транспорта сигнальной информации *BICC* (*BICC Signaling Transport service*). Таким образом, обмен сообщениями BICC между одноранговыми протокольными единицами BICC происходит с использованием этой услуги, как показано на рис. 8.7.



Рис. 8.7. Функциональная архитектура системы транспорта сигнализации

Сигнальные транспортные конвертеры выполняют процедуры адаптации примитивов, определенных для взаимодействия ISUP и MTP3 в базовой сигнализации OKC7, к специфическим примитивам для той или иной системы транспорта сигнализации. Таким образом, сигнальный обмен между функцией обслуживания вызовов и сигнальным транспортным конвертером производится с использованием общих примитивов, а между конвертером и той или иной системой транспорта сигнализации – посредством специфических примитивов этой системы.

Примитивы переносят сообщения BICC (создаваемые функцией CSF), а также выполняют другие функции. Приведем описание общих примитивов, используемых системой транспорта сигнализации BICC:

- примитив *IN-SERVICE.indication* указывает, что сигнальный транспорт способен предоставить возможность обмена сообщениями между одноранговыми объектами. Эта индикация поддерживается через SAP независимо от сигнального протокола BICC. Примитив содержит индикатор *level*, определяющий уровень перегрузки;
- примитив *OUT-OF-SERVICE.indication* указывает, что сигнальный транспорт не способен предоставить возможность обмена сообщениями между одноранговыми объектами. Эта индикация также поддерживается через SAP;

- примитив *TRANSFER.request* используется протоколом BICC для передачи сообщений к одноранговому объекту.
- примитив *TRANSFER.indication* используется для предоставления сигнального сообщения от однорангового объекта сигнальному протоколу BICC.
- примитив *CONGESTION.indication* используется для передачи информации о перегрузке;
- примитив *START-INFO.indication* сообщает протоколу BICC максимальную длину *SDU (Service Data Unit)*, которые может передавать *STC*, и является ли узел ведущим в процедуре установления соединения.

Таблица 8.3. Общие примитивы системы сигнального транспорта BICC

Универсальное название примитива	Тип			
	Запрос	Индикация	Подтверждение	Отклик
START-INFO	–	Max_Length CIC_Control	–	–
IN-SERVICE	–	Level	–	–
OUT-OF-SERVICE	–	*	–	–
CONGESTION	–	Level	–	–
TRANSFER	Sequence Control BICC Data Priority**	BICC Data Priority **	–	–
– Эти примитивы не определены * – Примитив не имеет параметров ** – Этот параметр – национальная опция				

Теперь перечислим параметры рассмотренных выше примитивов:

- параметр *BICC Data* содержит законченное сообщение BICC; оно представляется посредством *SDU STC*;
- параметр *level* указывает уровень перегрузки; значение параметра *level* зависит от реализации сети;
- параметр *Sequence Control* указывает для *STC* значение, которое может использоваться нижележащим сигнальным транспортом *STC* для разделения нагрузки и/или доставки сообщений с сохранением очередности их следования (*in-sequence*);
- параметр *Max_Length* указывает максимальную длину сообщений, которые могут транспортироваться через используемую сигнальную связь;
- параметр *CIC_Control* указывает блоку BICC, является ли тот контрольным для четных или нечетных CIC текущей сигнальной связи;
- параметр *Priority* указывает приоритет сообщения BICC.

Более детальное рассмотрение примитивов здесь не приводится, т.к. описание специфических примитивов для разных технологий очень громоздко и разнообразно. Приведенная же выше информация об основных примитивах не является справочными данными, а предназначена помочь читателю более полно увидеть процессы, происходящие в протоколе BICC.

Уже не раз упоминалось, что основой для BICC является протокол ISUP, и, соответственно, BICC наследует его сообщения и процедуры. Сообщения BICC поступают от блока CSF к STC и имеют формат, представленный на рис. 8.8.

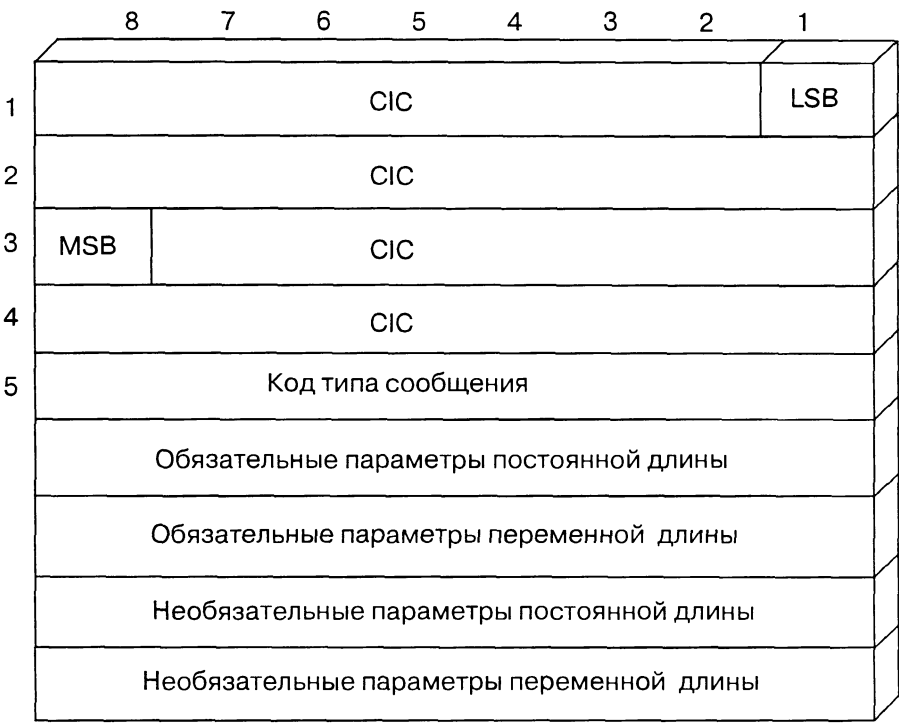


Рис. 8.8. Формат сообщения BICC

Приведенная ниже табл. 8.4 содержит минимальный набор сообщений, поддержка которых должна быть реализована для международного интерфейса BICC. Все эти сообщения не содержат индикаторы инструкций совместимости сообщений (*Message Compatibility Instruction Indicators*), которые применяются, чтобы обеспечить совместимость разных версий BICC и, следовательно, должны быть распознаны SN самостоятельно.

Таблица 8.4. Сообщения протокола BICC

ID	Сообщение	Значение сообщения
1	Address complete	Принятый адрес достаточен
2	Answer	Ответ
5	Call Progress	Особенности маршрута соединения
6	Circuit Group Blocking	Блокировка пучка
7	Circuit Group Blocking Acknowledgement	Подтверждение блокировки пучка
8	Circuit Group Reset	Возврат каналов пучка в исходное состояние
9	Circuit Group Reset Acknowledgement	Подтверждение возврата каналов пучка в исходное состояние
10	Circuit Group Unblocking	Разблокировка пучка
11	Circuit Group Unblocking Acknowledgement	Подтверждение разблокировки пучка
12	Connect	Ответ – соединить
13	Continuity	Целость (индикация проключения несущего канала)
14	Confusion	Несоответствие – прием нераспознанного сообщения/параметра
16	Facility Accepted	Подтверждение приема запроса услуги
17	Facility Reject	Отклонение этого запроса
18	Facility Request	Запрос услуги
19	Forward Transfer	Переключение связи
20	Initial Address	Начальное адресное сообщение
21	Release	Запрос разъединения
22	Release Complete	Подтверждение разъединения
23	Reset Circuit	Возврат канала в исходное состояние
24	Resume	Возобновление связи
25	Subsequent Address	Дополнительное адресное сообщение
26	Suspend	Временное прерывание связи
29	User-to-user information	Сообщения для обмена информацией между пользователями

В табл. 8.4 пропущены сообщения, которые непосредственно не применяются в BICC, однако должны быть правильно распознаны для обеспечения взаимодействия с другими сетями. Эти сообщения приведены в табл. 8.5.

Таблица 8.5. Сообщения, распознаваемые в протоколе BICC

ID	Сообщение	Значение сообщения
3	Blocking	Блокировка
4	Blocking Acknowledgement	Подтверждение блокировки
15	Continuity Check Request	Запрос проверки целостности
27	Unblocking	Разблокировка
28	Unblocking Acknowledgement	Подтверждение разблокировки

Как следует из формата сообщений BICC (рис. 8.8), каждое такое сообщение составляется из нескольких обязательных и необязательных параметров. В табл. 8.6 приведены лишь те параметры, которые необходимы для международного интерфейса.

Таблица 8.6. Параметры протокола BICC

Код	Параметр	Значение параметра
1	Access transport	Транспорт в доступе
2	Automatic congestion level	Уровень перегрузки
3	Backward call indicator	Обратные индикаторы условий обслуживания вызова
4	Called party number	Номер вызываемого абонента
5	Calling party number	Номер вызывающего абонента
6	Calling party's category	Категория вызывающего абонента
7	Cause indicators	Индикаторы причины
8	Circuit group supervision message type indicators	Индикаторы сообщения наблюдения за группой каналов (для BICC – только эксплуатационные)
9	Closed user group interlock code	Код закрытой группы пользователей
10	Connected number	Подключенный номер
11	Continuity indicators	Индикаторы проверки целостности
12	End of optional parameters indicator	Индикатор конца необязательного параметра
13	Event information	Информация о событии
14	Facility indicator	Индикатор дополнительной услуги
15	Forward call indicators	Индикаторы особенностей обслуживания вызова, передаваемые в прямом направлении
16	Nature of connection indicators	Индикаторы типа соединения
17	Optional backward call indicators	Необязательные индикаторы, передаваемые в обратном направлении
18	Optional forward call indicators	Необязательные индикаторы, передаваемые в прямом направлении
19	Original called number	Исходный номер вызываемого абонента
20	Range and status	Диапазон и статус (число и статус каналов пучка)
21	Redirecting number	Номер, на который заказана переадресация
22	Redirection information	Информация о переадресации
23	Redirection number	Номер, на который произведена переадресация
24	Subsequent number	Продолжение номера (в сообщении SAM)
25	Suspend/Resume indicators	Индикаторы прерывания/возобновления связи
26	Transmission medium requirement	Требования к среде передачи
27	User service information	Информация об услуге для пользователя
28	User-to-user indicators	Индикаторы пользователь-пользователь
29	User-to-user information	Информация пользователь-пользователь

Практически все приведенные в табл. 8.6 параметры (как и сообщения BICC) заимствованы из сигнализации ISUP, но есть ряд особенностей при их использовании в протоколе BICC. Так, параметр *Continuity Indicators* не указывает, в отличие от ISUP, на успешное завершение проверки целостности на текущем участке маршрута, но указывает на успешное завершение проверки целостности на предшествующем канале ISUP и/или на успешную организацию несущего канала на участке маршрута, предшествующем BICC-сети.

Имеются некоторые различия и в используемых понятиях. Например, в параметре *hop counter*, передаваемом в прямом направлении и убывающем при прохождении сообщения через транзитные узлы (для подсчета длины маршрута) нужно заменить значение *ISUP interexchange circuits* значением *call control associations*. Таким образом, параметр позволяет подсчитать не количество узлов, при помощи которых образован канал, а число сигнальных связей.

Одним из главных терминологических различий является *Circuit Identification Code (CIC)*, имевший в ISUP значение идентификатора физического канала между парой узлов, а в BICC использующийся, чтобы обозначить сигнальный сеанс для управления обслуживанием определенного вызова *Call Instance Code (CIC)*. В [12] отмечено, что *CIC (Circuit Identification Code)* в ISUP вместе с комбинацией *OPC/DPC/NI* выполняет две задачи: идентификацию физических каналов и идентификацию сигнального сеанса между одноранговыми объектами ISUP. В протоколе BICC же *CIC (Call Instance Code)* используется только для второй задачи. Размер поля *CIC* увеличен с 12 битов в ISUP до 4 октетов, чтобы увеличить количество вызовов, одновременно обслуживаемых протоколом. Поскольку информация *DPC/OPC/NI* не используется в BICC (при необходимости STC формирует эти значения для MTP3, MTP3b), *CIC* идентифицирует сигнальные связи между узлами. Для BICC число значений *CIC*, выделяемых для пары взаимодействующих узлов, представляет собой максимальное число сигнальных сеансов, которые могут существовать между ними.

Routing Label, содержащая информацию, которая передается к MTP для маршрутизации сообщений, а в BICC не используется. Если BICC развернут на MTP3 или MTP3b, то *Routing Label* формируется на подуровне STC.

Вместе с набором параметров и сообщений BICC унаследовал от ISUP и набор процедур, определенных в рекомендации Q.764, который, правда, подвергся частичному изменению. Был определен ряд дополнительных процедур, связанных с отделением носителя. Их рассмотрение потребовало бы значительного увеличения размеров главы и усложнения ее структуры, но для понимания принципов протокола BICC знать эти процедуры не обязательно.

8.5. Capability Set 2

BICC CS2 базируется на принципах, заложенных в CS1, продолжает поддерживать большинство услуг ISUP, но ориентирован уже на работу в IP-сети. К тому же, в CS2 архитектура протокола включает в себя функции оконечной АТС. Из-за этого ИК11 ИТУ-Т пришлось определить базовый процесс обслуживания вызова уже не в виде

delta-документа, как это было сделано в CS1, а в виде полных спецификаций. Все следующие доработки ISUP будут отныне включать в себя новые версии Q.761 и Q.764 с добавлением новых определений, параметров и сообщений из Q.1902.2 и Q.1902.3. Таким образом, протоколы ISUP и BICC оказываются неразрывно связанными через рекомендации ITU-T Q.7xx и Q.19xx, как это представлено в табл. 8.7.

Таблица 8.7. Рекомендации, описывающие базовый процесс обслуживания вызова в CS2

Рекомендация BICC	Эквивалент в ISUP	Что описывает	Комментарий
Q.1902.1	Q.761	Обзор	Отдельный текст
Q.1902.2	Q.762	Определения	Совместно с ISUP
Q.1902.3	Q.763	Форматы и коды	Совместно с ISUP
Q.1902.4	Q.764	Процедуры	Отдельный текст

Поскольку BICC CS2 включает в себя функции оконечной АТС, он должен, помимо обмена входящей/исходящей информацией, поддерживать дополнительные услуги ISUP. Это достигается посредством взаимодействия подсистемы BICC с ISUP так, как показано на рис. 8.9.

Помимо того, что реализация многих услуг ISUP в BICC имеет свои особенности, в BICC CS2 появились и новые, не существовавшие в ISUP услуги и возможности. Это может использоваться в BICC-сети при взаимодействии с услугами Интеллектуальной сети, например, при предоставлении услуги телеголосования или карт предоплаты услуг связи. В число процедур создания несущего канала были добавлены сигнальные процедуры, учитывающие методы организации носителя, например, в прямом направлении, в обратном направлении или создание свободного несущего канала. Это несколько усложнило сигнальные процедуры, но они по-прежнему базируются на сигнализации ISUP. Поскольку некоторые из процедур организации несущего канала требуют подтверждения того, что на каждом из SN, находящемся вдоль маршрута, пользовательская плоскость активна, это может привести к тому, что узел назначения надолго задержит передачу исходящего сообщения IAM, что, в свою очередь, даст неприемлемую задержку в установлении сеанса связи. Чтобы преодолеть описанный недостаток, в окружение BICC была внедрена процедура проверки целостности соединения.

Сам тест целостности соединения, как он определен в ISUP, в BICC не проводится, но сообщение *COT (Continuity)* используется, чтобы показать, что несущий канал проключен, и IAM может выйти из области BICC.

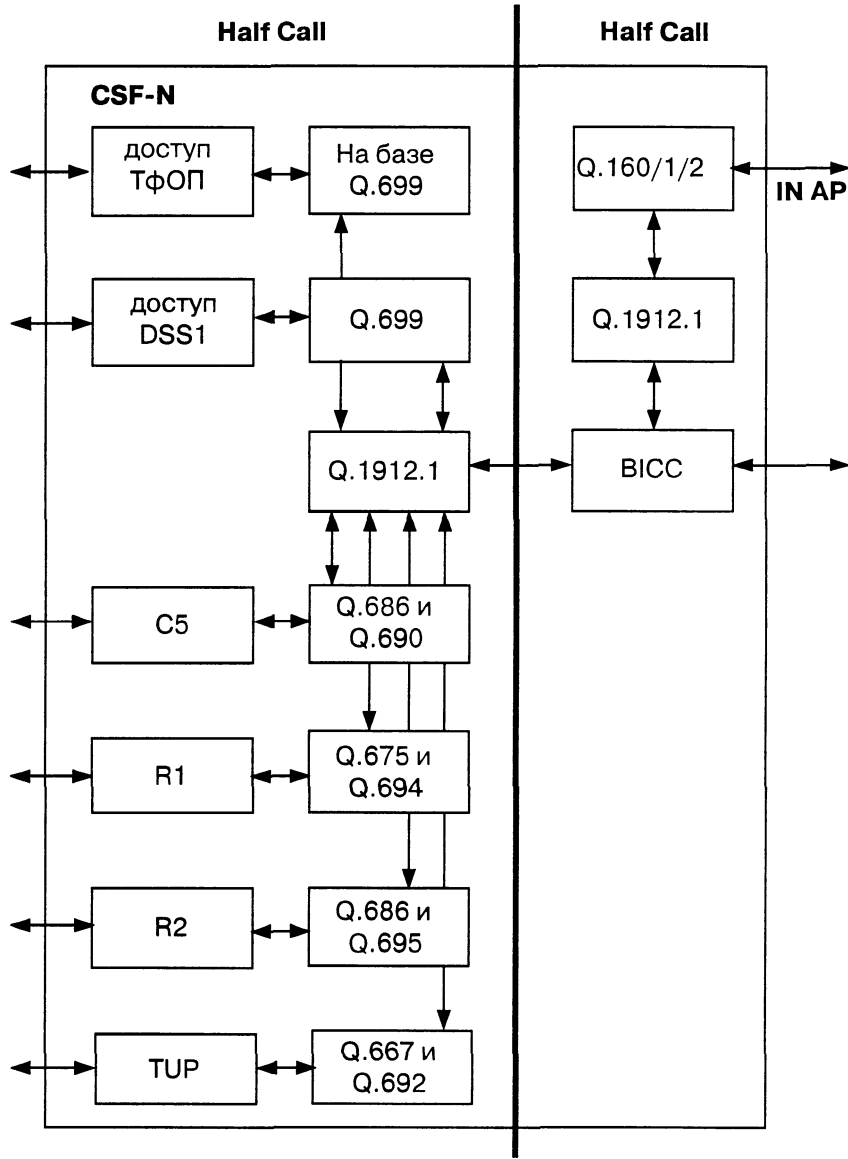


Рис. 8.9. Архитектура сигнального взаимодействия BICC с ISUP

Важной особенностью BICC CS2 является то, что модель этой версии позволяет одной функции CSF управлять более чем одной BIWF, а также одной BIWF быть управляемой несколькими CSF. Это значит, что количество информации, которую необходимо перенести от исходного SN до следующего узла на маршруте, увеличилось. Дополнительная информация связана с корреляцией вызова/несущего канала и с идентификацией. Для того чтобы более полно осветить вышесказанное, рассмотрим подробнее функциональную модель узла согласно BICC CS2.

Напомним рассмотренную в двух первых главах концепцию декомпозиции шлюза, составляющую основу архитектуры Softswitch. Декомпозиция шлюза предполагает, что он состоит из двух основных частей: медиа-шлюза MG, который преобразует данные из одного формата (например, TDM) в другой (например, IP), и Softswitch или контроллера транспортного шлюза MGC, который управляет медиа-шлюзом. Третий компонент шлюза после его декомпозиции – шлюз сигнализации SG – часто объединяется с MGC или входит в состав Softswitch. Вернувшись к архитектуре и терминологии BICC и принимая во внимание необходимость для BICC функционировать именно в этом окружении, целесообразно разделить функциональную модель единого узла SN, как он определен в CS1, на части, которые могут быть наложены на архитектуру MG/MGC. Требования к сетям IP-телефонии, на которые ориентировалась ИК11 при создании функциональной модели BICC CS2, предусматривающей физическое разделение функций управления обслуживанием вызова и управления несущим каналом, были взяты из проекта *TIPHON ETSI* и *MSF (Multiservice Switching Forum)*. Функциональная модель узла SN, физически разделенного на части согласно BICC CS2, представлена на рис. 8.10.

Функция CSF обеспечивает выполнение процедур BICC для каждого из вызовов, BCF выполняет общие управляющие функции в MGC. Простые же функции медиа-шлюза MG, без какой-либо управляющей составляющей, поддерживаются функцией мэппинга и коммутации *MMSF (Media mapping and switching function)*.

В предыдущих параграфах подчеркивалось, что при разработке BICC основные усилия были сконцентрированы на том, чтобы поддерживать предоставление уже устоявшихся узкополосных услуг (ISDN, Интеллектуальной сети и т.п.), используя широкополосную технологию. В частности, и по этой причине функции BCF и MMSF логически объединяются вместе, чтобы сформировать функцию BIWF.

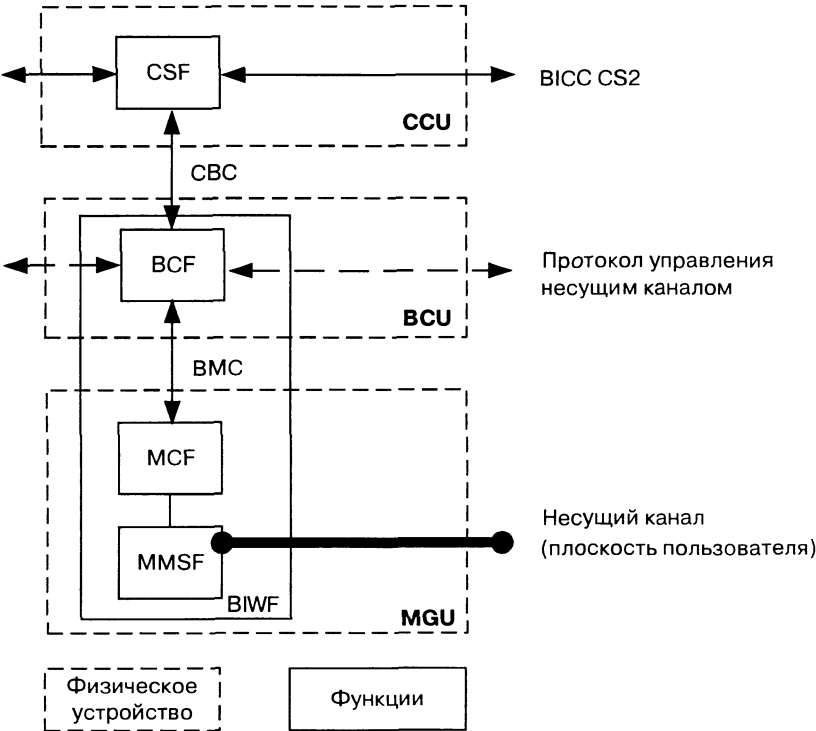


Рис. 8.10. Декомпозиция узла обслуживания SN (CS2)

Разумеется, архитектура BICC позволяет сделать интерфейс между BCF и MCF открытым, но разделение функций между BCF и MMSF не рассматривалось ИК11 при стандартизации BICC CS2. Более развитая функциональная структура позволяет одному серверу вызовов управлять несколькими медиа-шлюзами, что отражено на рис. 8.11.

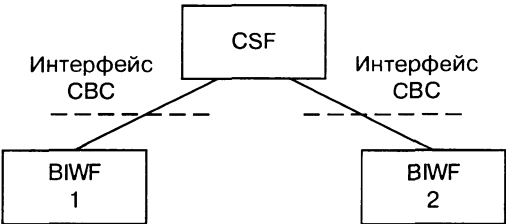


Рис. 8.11. Управление несколькими BIWF

С другой стороны, требования к поддержке мобильных приложений, о которых говорилось выше, вылились в создание возможности управлять одним BIWF несколькими CSF. Это сделано для того, чтобы, доведя до сети подвижной связи (СПС) вызов и несущий канал, довести до конечного терминала только вызов.

На этом этапе может быть использована тональная сигнализация, управляемая сервером вызовов СПС, но при помощи уже существующей функции BIWF, как это показано на рис. 8.12.

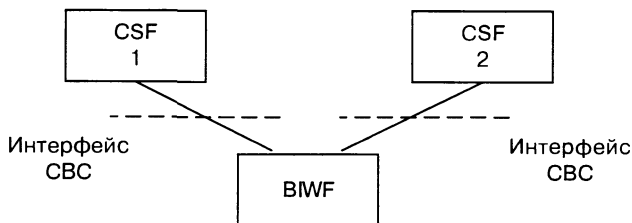


Рис. 8.12. Управление BIWF несколькими CFS

Важным нововведением в функциональной структуре узлов (как SN, так и CMN) стало использование так называемой модели *half call*, когда блок CSF разделяется на исходящие и входящие процедуры. Сказанное иллюстрирует рис. 8.13.

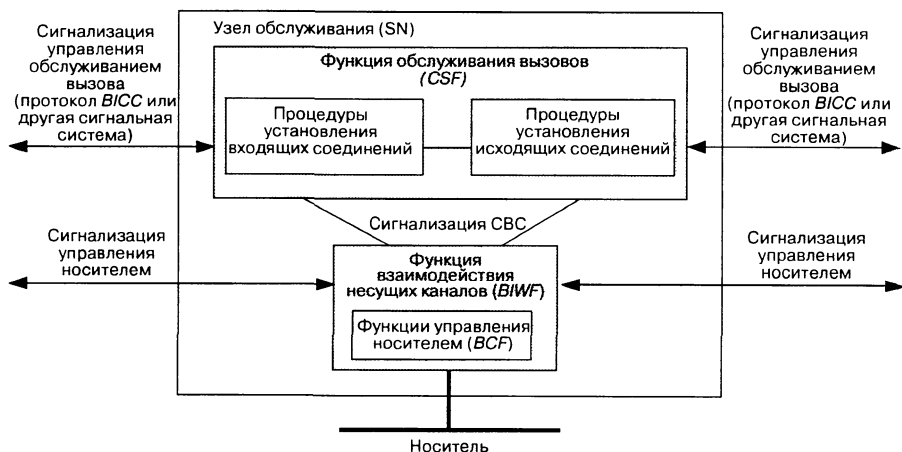


Рис. 8.13. Модель узла SN в соответствии с CS2

Информационный обмен через интерфейс между CSF и BIWF (CBC) в BICC CS2 стандартизирован и ведется по протоколу MEGACO/Н.248. Таким образом, еще раз учитывается использование в BICC CS2 принципа декомпозиции шлюза. Как это было сделано для BICC CS1, приведем на рис. 8.14 архитектуру сети на базе BICC CS2.

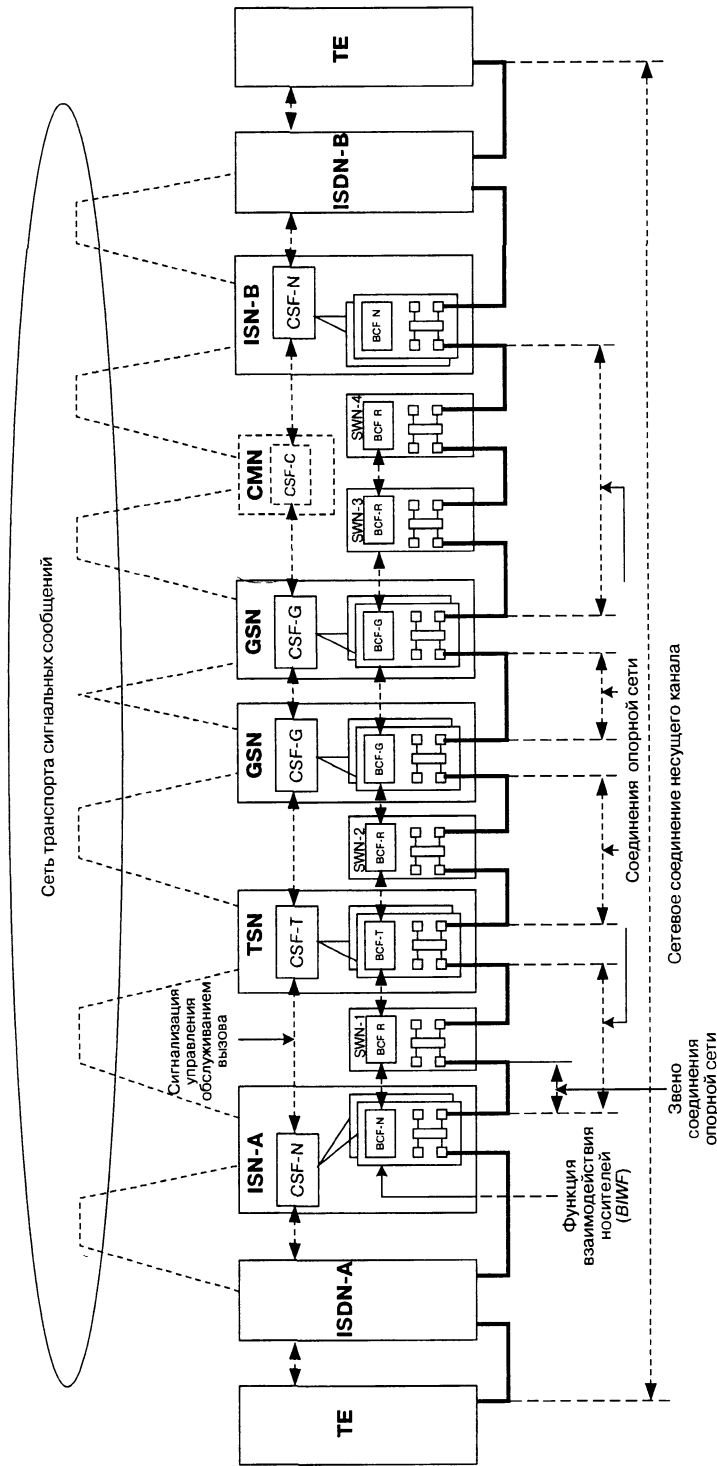


Рис. 8.14. Архитектура сети BICC CS2

8.6. Протокол IPBCP

Между IP-сетями и такими сетями, как TDM или АТМ, существует различие, заключающееся в том, что для обеспечения взаимодействия пользователей сигнальные сообщения не обязательно должны восприниматься всеми сетевыми элементами. Если шлюзы или взаимодействующие узлы обмениваются IP-адресами и номерами портов, то для IP-сети этого достаточно, чтобы обеспечить передачу между ними пользовательского трафика. Такой принцип вполне подходит для обслуживания трафика по модели *best effort*, но IP-сеть с гарантированным уровнем обслуживания должна функционировать поверх некоего типа соединения.

Так как BICC всего лишь использует уже существующие протоколы внутри IP-сети, ИК11 при разработке BICC CS2 и BICC CS3 пришлось сосредоточить усилия на вопросе обеспечения качества. Запрос соединения просто перераспределяет полосу пропускания в шлюзе, получившем этот запрос. К тому же, IP-сети не устанавливают двунаправленные соединения автоматически, и чтобы обеспечить это, требуется передача служебной информации в каждом направлении. К счастью, обмен информацией может быть очень простым – обмен IP-адресами, номерами портов и некоторыми сведениями, описывающими тип пользовательских данных.

В IP-сетях с протоколом SIP информация о пользовательском трафике описывается отдельно в протоколе описания сеанса *SDP* (*Session Description Protocol*), о чем говорилось в главе 4. Хотя SDP там и назывался протоколом, фактически он определяет только формат и значение передаваемых данных. SDP не определяет своих собственных сообщений и поэтому переносится протоколом SIP. Для того чтобы сделать протокол BICC максимально совместимым с SIP, сообщения BICC были расширены так, чтобы они могли опционально переносить данные протокола SDP. Эта информация создается функцией MMSF и через интерфейс CBC передается вертикально блоку управления обслуживанием вызова BICC, а затем пересылается горизонтально, как информация, туннелируемая внутри BICC. Эта возможность позволяет обмениваться данными SDP, чтобы открыть соединение на пользовательской плоскости, и обойтись без спецификации в BICC всей информации, которая уже определена в SDP. Здесь использован термин туннелирование потому, что протокол BICC не просматривает, не проверяет и не понимает информацию, которую он передает. Для того чтобы механизм туннелирования был универсальным, ITU-T выпустил отдельную рекомендацию Q.1990 – Bearer Control Tunneling Protocol, – определяющую заголовок туннелируемой информации, который нужен для того, чтобы идентифицировать протокол и номер версии.

Такой обмен информацией между двумя BIWF, с использованием кодирования SDP и с туннелированием согласно Q.1990, был определен как работа по протоколу *IP Bearer Control Protocol*, который, в свою очередь, специфицирован в рекомендации Q.1970.

Для передачи информации протокол IPBCP использует четыре сообщения:

- *Request message* передается BIWF, чтобы инициировать процесс создания или модификации IP-носителя. BIWF, передавший это сообщение, называется *I-BIWF (Initiating BIWF)*.
- *Accepted message* передается в ответ на сообщение запроса. BIWF, передавший это сообщение, называется *R-BIWF (Receiving BIWF)*.
- *Confused message* передается в ответ на сообщение запроса в случае, если его невозможно обработать.
- *Rejected message* передается в ответ на сообщение запроса в случае, если его невозможно удовлетворить.

8.7. Обслуживание вызова в BICC

На рис. 8.15 представлен сценарий взаимодействия и обмен сообщениями между вертикальными и горизонтальными интерфейсами BICC для организации несущего канала в прямом направлении. Там же показано, как область BICC взаимодействует с ТФОП-окружением. Исходящий узел ISN получает сообщение IAM и сам генерирует и отправляет исходящее сообщение IAM к следующему узлу. Это сообщение IAM переносит в параметре «транспортировка приложения» *APP (Application Transport Parameter)* инкапсулированные характеристики несущего канала *BNC (Backbone Network Connection)*, которые генерируются на основе принятых параметров «информация об услугах для пользователя» *USI (User Service Information)* и содержат сведения о средствах доставки информации, затребованных вызывающим абонентом, и «требование к среде передачи» *TMR (Transmission Medium Requirement)*, указывающее тип информации, доставку которой должна обеспечить среда передачи. После приема сообщения «Транспортировка приложения» *APM (Application Transport)* с информацией об адресе носителя (у) функция CSF передает функции BIWF запрос создать носитель и снабжает ее полученной адресной информацией. Как только функция BIWF создаст носитель, она сразу же извещает об этом CSF, а та, в свою очередь, передает это извещение следующему узлу в аналогичном сообщении APM. В задачи CSF узла назначения входит передача предыдущему узлу сообщения APM с адресной информацией, необходимой для создания носителя. Если этот узел является TSN, он также генерирует и передает сообщение IAM, содержащее индикацию «COT on previous» и свои характеристики BNC.

После этого TSN будет ждать сообщения APM с информацией об адресе носителя. Если же узел является ISN назначения, выполняется та же процедура передачи APM предыдущему узлу, но исходящее сообщение IAM с индикацией «COT on previous» передается подсистеме ISUP сети TDM. Дальнейший обмен сообщениями APM является опциональным и зависит от того, применяется ли согласование кодеков или туннелирование информации в BICC.

TSN передает сообщение COT (целость) после того как обнаружит, что носитель между ним и предыдущим узлом организован, то есть либо когда создан носитель в прямом направлении от исходящего ISN к TSN, либо после приема сообщения APM от исходящего ISN (в примере на рис. 8.15).

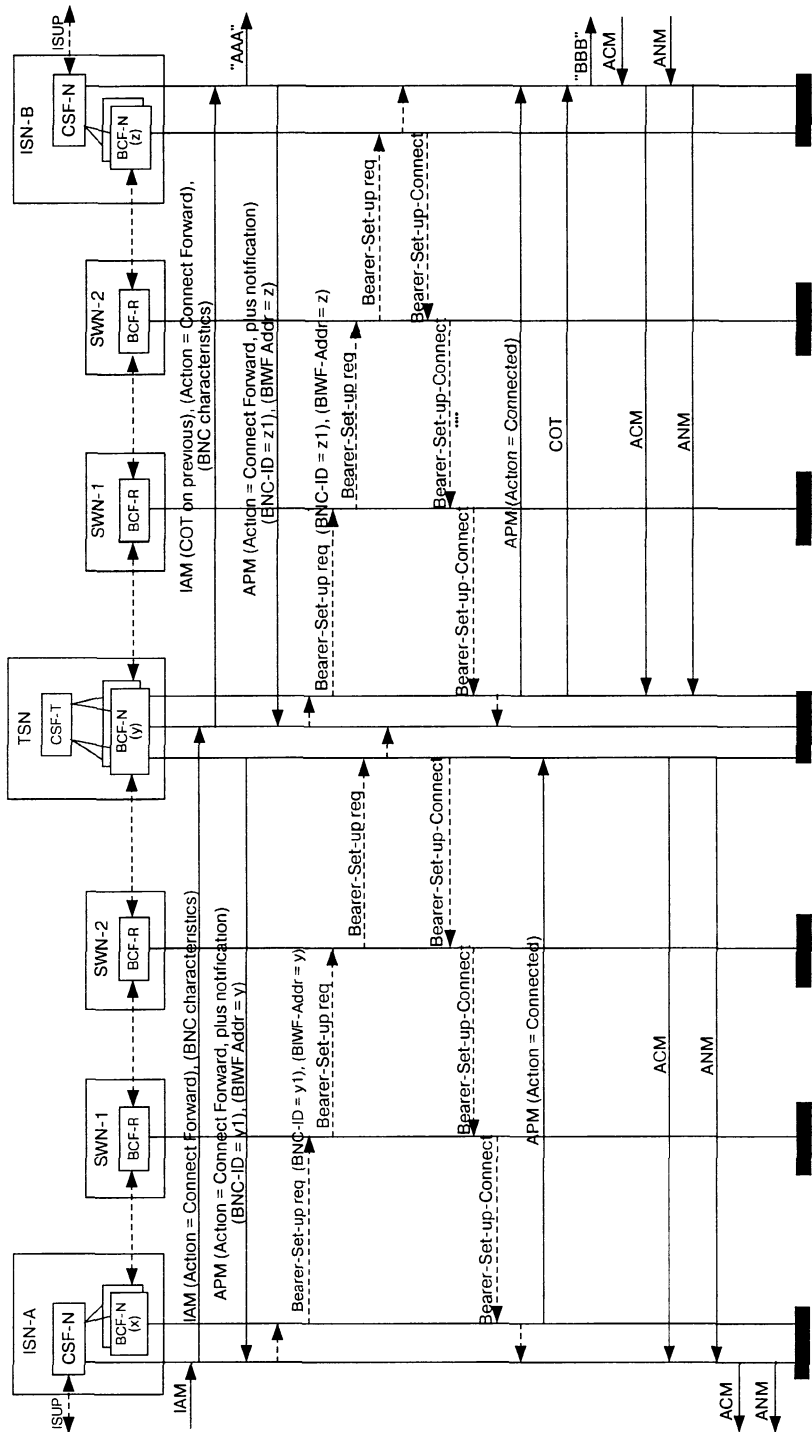
Поток сообщений ACM (*Address Complete Message*) и ANM (*Answer Message*) идентичен процедурам ISUP. Процедуры разъединения также не отличаются от тех же процедур ISUP, за исключением того, что CSF информирует BWF о необходимости освободить носитель. При создании носителя в обратном направлении используются те же потоки сообщений, за исключением того, что характеристики носителя и туннелируемая информация генерируются BWF узла назначения и передаются обратно в первом сообщении APM. Приведенное описание сценария ориентировано на BICC CS1. Отличием случая с BICC CS2 будет лишь то, что исходящий и входящий узлы ISN могут быть конечными адресатами сигнализации ISUP, а не транзитными, поскольку обладают функциями оконечной ATC.

8.8. Сценарии взаимодействия Softswitch

Поскольку протокол BICC изначально задуман для работы в мультисервисной конвергентной сети, важно рассмотреть его работу в смешанном окружении, как это может оказаться в реальной сети NGN. Как следует из всего, написанного выше, начиная с названия книги, основным элементом такой NGN является Softswitch, поэтому в представленном на рис. 8.16 примере рассматриваются три Softswitch, которые взаимодействуют друг с другом по протоколам BICC и SIP. Таким образом, здесь Softswitch реализуют функции *Interface Serving Node (ISN)* протокола BICC и функции прокси-сервера SIP.

SIP-NNI (Network-Network Interface) – это модуль SIP, устанавливаемый на пограничном узле сигнализации SIP, взаимодействующем с внешними сетями. В примере на рис. 8.16, а также в показанных на рис. 8.17 и 8.18 сценариях этот модуль реализован в составе Softswitch и обозначен, соответственно, как SIP-NNI.

В этом примере сеанс связи устанавливается между абонентом TDM-сети, включенным в PBX, и абонентом сети IP-телефонии с SIP-телефоном, причем в обслуживании вызова участвует еще один транзитный Softswitch. Так как первый абонент включен в учрежденческую ATC, то ее взаимодействие с Softswitch1, реализующим функции *Interface Serving Node BICC*, обеспечивает протокол DSS1.



T11107780-00

Рис. 8.15. Организация носителя в прямом направлении

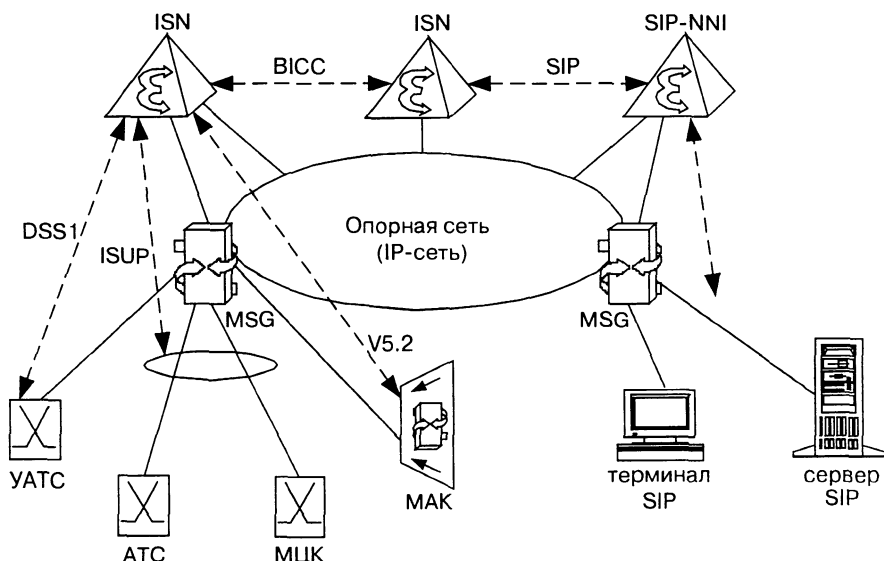


Рис. 8.16. Пример сети NGN под управлением трех Softswitch

Сделано это для разнообразия, чтобы дать читателю возможность отдохнуть от протокола ОКС7, постоянно присутствовавшего в этой главе, но взаимодействие Softswitch по DSS1 происходит точно по тем же правилам, что и в случае ISUP. Набор передаваемых сигналов остается неизменным.

Для взаимодействия с SIP необходима новая функциональная единица – модуль взаимодействия *IWU* (*Interworking Unit*). Этот модуль может быть отдельной физической единицей, а может входить в состав узла BICC. Отметим, что при взаимодействии протоколов BICC и SIP будут поддерживаться только общие для них обоих услуги, а все дополнительные услуги, предоставляемые в одной сети и не поддерживаемые в другой, не будут пропущены через *IWU*. В связи с вышесказанным необходимо определить дополнительно следующие термины:

- *Incoming IWU* – физическая структурная единица, которая может быть объединена с *ISN BICC*, принимающая вызовы со стороны SIP-сети и обеспечивающая их дальнейшую обработку с использованием протокола BICC;
- *Outgoing IWU* – структурная единица, которая выполняет обратную функцию;
- *Adjacent SIP Node (ASN)* – смежный узел SIP, т.е. прокси-сервер SIP, *SIP-часть IWU* которого взаимодействует с *I-IWU* или *O-IWU*.

Для обмена сигнальной информацией, относящейся к одному вызову, модулю взаимодействия *IWU* необходимо установить прямую зависимость между диалогом SIP и сигнальной связью

BICC/ISUP. Чтобы обеспечить обмен адресной информацией, для одной сигнальной связи BICC/ISUP может быть установлено ее взаимодействие с последовательностью диалогов SIP, продолжающееся до тех пор, пока этап обмена адресной информацией не будет закончен.

Сообщения BICC/ISUP должны или инкапсулироваться, или быть преобразованы в аналогичные запросы SIP. При использовании обеими сетями (и BICC-ориентированными, и SIP-ориентированными) одной транспортной технологии было бы удобно использовать дополнительную возможность BICC – возможность туннелировать информацию управления носителем. Однако текущие возможности BICC CS2 позволяют туннелировать информацию управления носителем средствами механизма *Bearer Control Tunneling* только для одного протокола – IPBCP, – о чем говорилось в параграфе 8.6.

Аналогично понятию *IWU*, относящемуся к управлению обслуживанием вызова, для взаимодействия протоколов управления носителями вводится понятие функции взаимодействия управления носителями *BC-IWF (Bearer Control Interworking Function)*. Функция *BC-IWF* обеспечивает взаимодействие IPBCP с SDP и предоставляется только для определенного вызова. При приеме запросов SDP, передаваемых в сообщениях SIP, *BC-IWF* должна генерировать соответствующий блок данных (*Bearer Control Data Unit*) для вложения в сообщение BICC. Затем производится анализ того, какое из сообщений SIP, содержащих ответы, необходимо передать согласно полученному сообщению запроса. Передача этого сообщения задерживается до получения сообщения BICC, содержащего *Bearer Control Data Unit*. При получении сообщения BICC содержащего *Bearer Control Data Unit*, производится обратная процедура. После получения сообщения *INVITE Incoming-IWU* определяет, что на стороне BICC необходимо выполнить процедуру организации носителя (*Bearer Setup Procedure*). В зависимости от того, содержит ли *INVITE* запрос SDP или нет, канал проключается в прямом или обратном направлении, а *INVITE* преобразуется в IAM с соответствующими параметрами.

8.8.1. Сценарий соединения DSS1 – BICC – SIP

Пользователь, инициирующий вызов, снимает трубку, в результате чего ТЕ подает ему сигнал «Ответ станции» и подготавливается к приему цифр номера вызываемого абонента. Цифры накапливаются в ТЕ, а затем передаются к ISN-A в сообщении *SETUP* вместе с информационными элементами, содержащими требования к характеристикам средств доставки информации, а также с меткой соединения по протоколу DSS1 [5]. Далее узел ISN-A определяет, может ли этот вызов быть маршрутизирован в соответствии с принятой адресной информацией и с требованиями к среде передачи. Если да, то к ТЕ передается сообщение *CALL PROCEEDING*, занима-

ется необходимое значение *CIC* (в заданном направлении), соответственно, определяется *STC*, и запускается процедура контроля отправки *IAM* с вызовом процедуры установления соединения в исходящем направлении (выбирается необходимый блок взаимодействия несущих каналов – *BIWF*).

Рассмотрим вариант проключения канала в прямом направлении (рис. 8.17). В этом случае *IAM* передается со значением параметра индикатора действий: «организация канала в прямом направлении», а также с примитивом *BICC_Data request*, содержащим характеристики опорной сети BNC (определяются посредством выбора *BIWF*). В ответ необходимо получение сообщения *APM*, содержащего требование передать уведомление о проключении несущего канала (о создании носителя), а также, что наиболее важно, — адреса и идентификаторы встречного *BIWF*. Получив *APM*, *CSF* узла *ISN-A* передает к *BCF* запрос организовать несущий канал, *BCF* выполняет необходимые для этого действия и передает запрос встречному блоку при помощи туннелирования протокола *IPBCP* через сигнальную связь *CSF*, после чего переходит в состояние ожидания подтверждения (*Request Message* и *Accepted Message*) протокола *IPBCP*. Канал считается проключенным после получения примитива *Bearer Set-up Connect*. Блок взаимодействия может быть как совмещенным с *ISN-B*, так и отдельной функциональной единицей. Во втором случае требуется такая же процедура передачи сигналов, как если бы этот блок был еще одним узлом BICC. В блоке взаимодействия происходит модификация адресов и параметров, передаваемых в сообщениях BICC, а также преобразование пользовательской информации в тело сообщения SIP (или, при использовании протокола SIP-I, производится инкапсуляция).

К SoftSwitch, реализующему функции SIP-NNI, блоком взаимодействия передается *INVITE*. При этом *IAM* преобразуется в *INVITE* согласно правилам, приведенным в таблице.

Таблица 8.8. Параметры сообщений IAM BICC и поля SIP INVITE

Параметры <i>IAM</i>	Поля <i>INVITE</i>
<i>Called Party Number</i> (номер вызываемого абонента)	<i>Request URL</i>
	<i>To</i>
	<i>P-Asserted-Identity</i>
<i>Calling Party Number</i> (номер вызывающего абонента)	<i>Privacy</i>
	<i>From</i>
	<i>From</i>
<i>Generic Number</i> (общий номер вызывающего абонента)	<i>From</i>
<i>Hop Counter</i> (счетчик переприемов)	<i>Max Forwards</i>
<i>TMR/USI</i> (информация пользователей и требования к среде передачи)	<i>Message Body (SDP)</i>

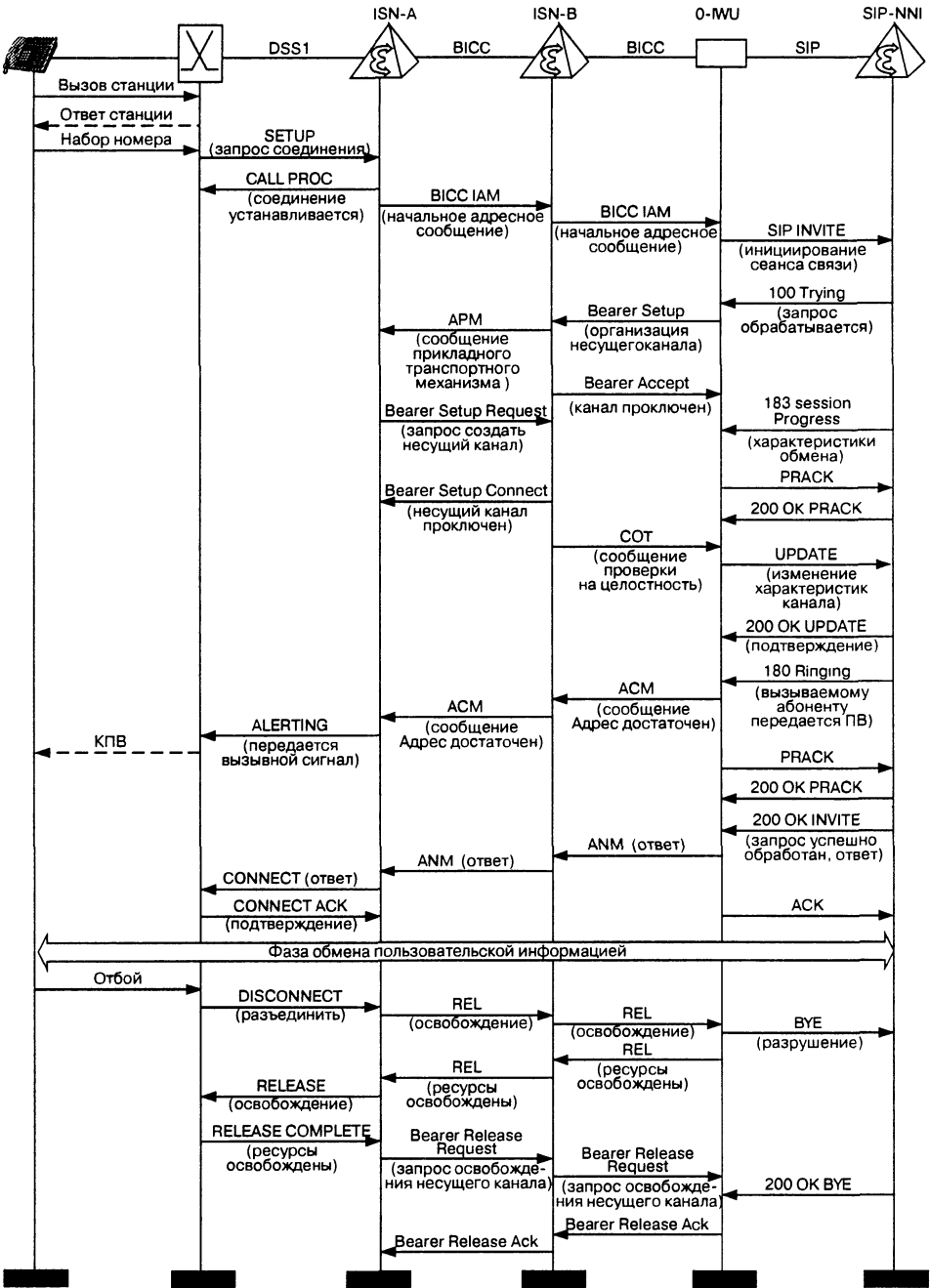


Рис. 8.17. Успешное установление соединения в направлении DSS1-SIP. Проклочение канала в прямом направлении,отбой со стороны вызывающего абонента

Вызываемая сторона принимает запрос *INVITE* и начинает его обработку, о чем уведомляет блок взаимодействия BICC сообщением *100 trying* (производится перезапуск таймеров). Затем от узла SIP-NNI передается ответ *183 Session Progress*, позволяющий блоку взаимодействия BICC получить данные о сеансах на пути к вызываемому пользователю для раннего проключения разговорного тракта. На сообщение *183* передается последовательность подтверждений: *PRACK, 200 OK PRACK*. На этом этапе обеспечивается также резервирование ресурсов. Далее блок взаимодействия может получить от узла ISN-B сообщение *COT*, об успешном выполнении процедуры проверки целостности на предыдущих участках обслуживания вызова (сообщение интерпретируется как сигнал о сквозном проключении несущего канала). В соответствии с этим, к объекту SIP передается запрос *UPDATE*, который содержит окончательные характеристики несущего канала и в ответ на который идет подтверждение *200 OK UPDATE*.

От вызываемого абонента дается индикация того, что к нему поступает вызывной сигнал – *180 Ringing*. На объекте взаимодействия этот сигнал транслируется как *ACM* и передается далее узлам ISN-B и ISN-A по соответствующим сигнальным связям. ISN-A, соответственно, передает к ТЕ сигнал *Alerting*, а вызываемому абоненту посылается сигнал контроля посылки вызова (КПВ). Объекту же SIP передается последовательность подтверждений *PRACK*. После ответа вызываемого абонента передается подтверждение *200 OK INVITE*, которое поступает на блок взаимодействия, а далее транслируется по сигнальным связям как *ANSWER MESSAGE (ANM)*, получив которое ISN-A передает к ТЕ сообщение *CONNECT*. После получения подтверждения *CONNECT ACKNOWLEDGE* начинается фаза обмена пользовательской информацией (и, соответственно, начисление платы). После отбоя вызывающего абонента происходит последовательный запуск процедур освобождения несущих каналов. На участке DSS1 эта процедура инициируется сообщением *DISCONNECT*. Узел ISN-A передает сообщение *RELEASE* к ТЕ, в результате чего происходит освобождение каналов и затребованных для связи ресурсов. Завершение этого этапа на исходящей стороне подтверждается передачей от ТЕ сообщения *RELEASE COMPLETE*. Получение сообщения *DISCONNECT* приводит к тому, что CSF ISN-A дает запрос разрушить внутренний тракт передачи к BCF, а также передает сообщение *RELease* взаимодействующему узлу ISN-B. Параллельно BCF ISN-A передает к BCF ISN-B запрос освободить несущий канал. В свою очередь, BCF ISN-B выполняет необходимые для этого действия и передает подтверждения к BCF ISN-A и к CSF своего узла. После получения CSF ISN-B от своего BCF подтверждения разрушения тракта передачи, к CSF ISN-A передается сообщение *Release Complete*. Аналогичная процедура выполняется

и на участке ISN-B – O-IWU. Здесь, после получения блоком взаимодействия сообщения *RELease*, на узел SIP-NNI передается сообщение протокола SIP – *BYE*, в ответ на которое передается подтверждение *200 OK BYE*.

8.8.2. Сценарий соединения SIP – BICC – DSS1

Этот сценарий (рис. 8.18) во многом повторяет предыдущий. Основное отличие на участке BICC состоит в том, что несущий канал проключается в обратном направлении.

В передаваемом *IAM* на это дается указание с помощью индикатора действий, а также передаются данные, необходимые для обратной адресации при создании носителя (адрес *BIWF*, идентификатор *BFC*). Вместо сообщения *APM* в обратную сторону сразу передается запрос организовать несущий канал от встречного *BIWF*. Разрушение соединения также будет происходить в обратном направлении. Поскольку канал проключается в обратном направлении, сообщение о целостности передается по сигнальной связи вперед.

8.9. Quo vadis?

Вопрос выбора единственного протокола для упрощения взаимодействия оборудования разных производителей и для концентрации усилий на совершенствовании и доработке только одного протокола не раз поднимался на международных форумах. Например, он был вопросом номер один в докладе о NGN компании Telecom Engineering Consultants на форуме Asia Pacific Telecommunity в августе 2003 года.

Рассмотренный в главе 4 протокол SIP (SIP-I, SIP-T) сегодня является безусловным фаворитом с точки зрения выбора единственного протокола взаимодействия для Softswitch. Сейчас некоторые производители и Операторы организуют взаимодействие оборудования Softswitch по протоколу BICC по той причине, что в свое время при построении сети они отдали предпочтение технологии ATM, на которую и был ориентирован протокол BICC CS-1. Заметим, что в этой главе, как и в посвященной SIP главе 4, к аббревиатуре протокола SIP иногда добавляются буквы SIP-T, SIP-I и упоминаются соответствующие расширения протокола. Строго говоря, это не совсем так. Дело в том, что в дополнительных рекомендациях, после выхода которых появились аббревиатуры SIP-T и SIP-I, рассматриваются вопросы взаимодействия протокола SIP с другими системами сигнализации. В них SIP-T определяет правила взаимодействия с телефонными сетями общего пользования, а SIP-I является обобщенным термином для всех рекомендаций, связанных с взаимодействием внешних сетей с сетью SIP.

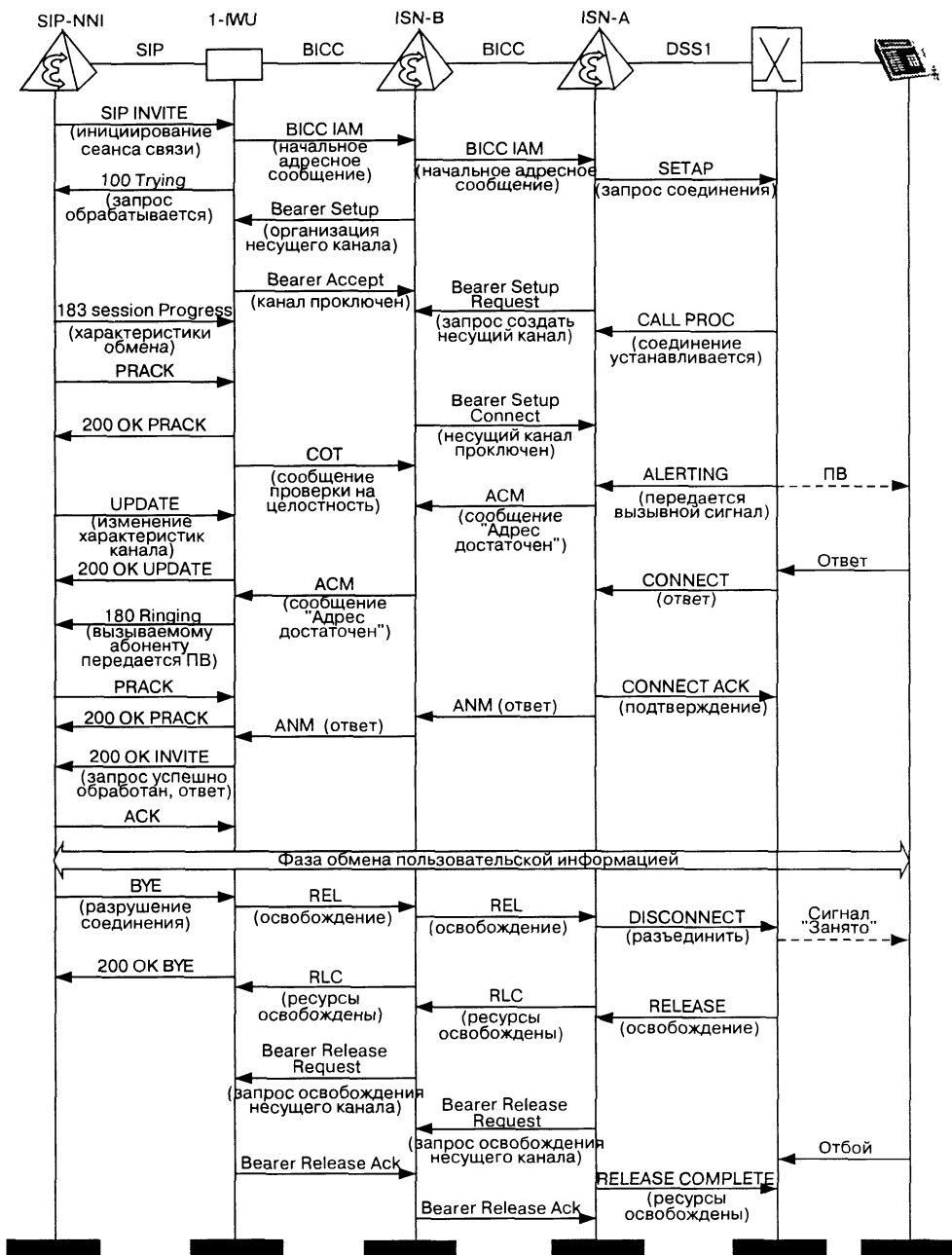


Рис. 8.18. Успешное установление соединения в направлении SIP-BICC. Проклочение канала в обратном направлении, отбой со стороны вызывающего абонента

Что же касается BICC CS-2 и BICC CS-3, то хотя они предусматривают возможность работы протокола BICC в IP-сетях, но даже те производители и Операторы, которые с самого начала строили сети IP, а не ATM, часто не видят смысла переходить с уже используемого в их сетях протокола SIP на BICC CS-2. Поэтому, наблюдая начавшуюся замену коммутируемых сетей TDM сетями SIP/IP и BICC/ATM, можно считать более вероятным постепенный переход в дальнейшем преимущественно на IP-сети, в которых IP будет использоваться без ATM и SDH, а SIP будет замещать BICC.

Но сейчас SIP и BICC обладают практически одинаковыми функциональными возможностями. И если SIP-I лучше подходит Операторам, планирующим создавать SIP-ориентированную сетевую структуру и предоставлять передовые мультимедийные услуги, то BICC удовлетворяет крупных традиционных операторов, эмулирующих услуги ТфОП и желающих лишь получить независимость от транспортной технологии и сохранить только что построенную сеть ОКС7, к которой прочно привязан BICC. Время покажет, какую нишу в перспективе займет BICC. Будут ли это сети традиционных межрегиональных операторов или частные локальные и корпоративные решения? Будут ли и дальше протоколы H.323, SIP, H.248 и BICC развиваться параллельно, или дальнейшие усилия ITU и IETF сконцентрируются только на совершенствовании SIP и H.248?

Время покажет. А сегодня протокол BICC предлагает довольно изящное решение перехода к мультисервисным сетям NGN, описанию которого и была посвящена настоящая глава.

Глава 9

Сети NGN

Единственный способ определить границы возможного – выйти за эти границы
Артур Кларк

9.1. Примеры сетевых конфигураций

Выход за границы возможностей традиционных сетей связи, обусловленный характером сегодняшнего мультимедийного трафика и потребностями в мультисервисном его обслуживании, привел к качественному преобразованию всей сетевой структуры, и появилась концепция сети следующего поколения *NGN (Next Generation Network)*.

Однозначного толкования архитектуры и услуг NGN телекоммуникационное сообщество пока не выработало. По крайней мере, так было на момент написания этой книги, и особых иллюзий относительно изменения ситуации в ближайшем будущем авторы не питают: идет естественный процесс конвергенции сетей связи.

С позиций сетей передачи данных NGN – это сеть Интернет следующего поколения. С позиций сетей мобильной связи этому поколению даже присвоен номер 3G. С позиций традиционной телефонии NGN сегодня воспринимается как сеть пакетной коммутации под управлением *Softswitch*, поддерживающая широкополосный абонентский доступ и мультисервисное обслуживание трафика.

Общими характеристиками NGN, определенными ITU и ETSI являются разделение функций переноса информации и функций управления переносом информации через сеть, а также отделение функций услуг и приложений от собственно связанных функций. Таким образом, речь идет о распределенной архитектуре, в которой связь между компонентами осуществляется исключительно через открытые интерфейсы. Наиболее подробно это рассматривается в стандарте ETSI ES 282 001 v.1.1.1, принятом в августе 2005 г., но мы в этой главе начнем разговор об NGN с обсуждения примеров сетевых конфигураций с *Softswitch*, предложенных консорциумом IPCC.

Первым таким примером является сетевая конфигурация, представленная на рис. 9.1. Элементами изображенной на этом рисунке сети являются Softswitch, сервер приложений AS (*Application Server*), шлюз между ТфОП и IP-сетью TG (*Trunk Gateway*), шлюз доступа AG (*Access Gateway*), шлюз сигнализации SG (*Signaling Gateway*) и транспортный (медиа) сервер MS (*Media Server*).

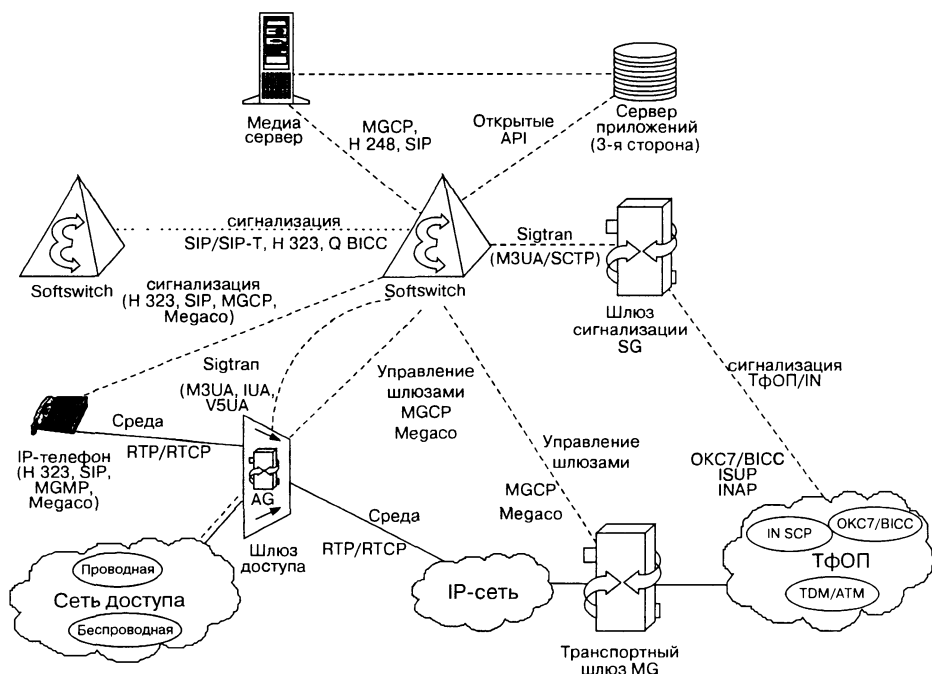


Рис. 9.1. Пример архитектуры NGN

Softswitch в этом примере выполняет функции MGC-F, R-F и A-F, обсуждавшиеся в главе 2, обрабатывает всю сигнализацию, управляет TG, AG и соответствующим выделением медиа-ресурсов, производит аутентификацию вызовов, а также обеспечивает получение учетной информации. Кроме того, каждый Softswitch взаимодействует с другими Softswitch по протоколам SIP/SIP-T, H.323 или BICC.

Сервер приложений AS реализует логику услуг, чему посвящен отдельный параграф этой главы. Вызов, который требует дополнительную услугу, либо может быть передан от Softswitch к AS для дальнейшего управления этой услугой, либо сам Softswitch может получать от AS информацию, необходимую для выполнения логики услуги. Сервер приложений AS может сам управлять MS или передавать управление им Softswitch.

На транспортный шлюз TG поступают потоки пользовательской (речевой) информации со стороны ТфОП, он преобразует эту инфор-

На рис. 9.3 показан пример реализации VoIP-сети, использующей сеть доступа с технологией DSL. Обычные аналоговые телефоны и любые устройства локальной сети Ethernet подключаются к устройству интегрированного доступа IAD в помещении абонента, которое обрабатывает и передает абонентскую сигнальную информацию по IP-сети или через мультиплексор доступа DSLAM к Softswitch. Что касается речевой информации, то IAD оцифровывает ее, пакетирует и переносит в виде пакетов RTP по IP-сети.

Эти три примера иллюстрируют базовое свойство сетей NGN – интеграцию передачи речи, данных и видеoinформации, включая объединение оборудования и функциональных возможностей как на уровне опорной сети (Core Network), так и на уровне сети доступа (Access Network).

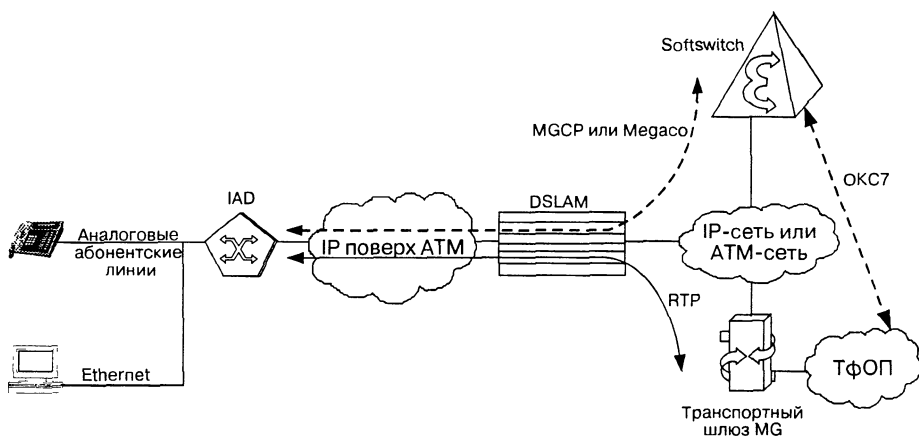


Рис. 9.3. Архитектура NGN с IAD и DSL AM

С этим согласуется и определение сети NGN, данное Международным союзом электросвязи: *NGN – это мультисервисная сеть связи, ядром которой является опорная IP-сеть, поддерживающая полную или частичную интеграцию услуг передачи речи, данных и мультимедиа*. Там же указано, что *NGN – это, прежде всего, сеть с коммутацией пакетов, в которой функции коммутации отделены от функций предоставления услуг; она позволяет предоставлять широкий перечень услуг и добавлять в него новые услуги по мере их разработки*. NGN обеспечивает также широкополосный доступ и поддерживает механизмы качества обслуживания QoS.

Существует также архитектура NGN, разработанная уже упоминавшимся комитетом TISPAN и утвержденным в качестве стандарта ETSI. В ней предусматривается разделение на уровни, включая транспортный уровень и уровень услуг, а также интерфейс взаимодействия с оборудованием пользователя и интерфейс взаимодействия с другими сетями. Подсистемы транспортного уровня – *NASS* (Network Attachment Subsystem) и *RACS* (Resource and Admission Control Subsys-

tem) – отвечают за работу с IP-потоками, процессы идентификации и доступа к ресурсам. Уровень обслуживания объединяет непосредственно услуги или, вернее, подсистему их предоставления, а также элементы управления процессом установления соединения. Расположенная на уровне услуг структура управления соответствует уже подробно обсуждавшейся выше идеологии Softswitch и включает *Core IMS*, подсистему *PES* (PSTN/ISDN Emulation Subsystem) для эмуляции функций ТфОП/ISDN, а также другие подсистемы ETSI для реализации новых приложений. К этой архитектуре мы еще вернемся более подробно в главе 11.

Как видно из приведенных примеров, как, впрочем, и из материалов предыдущих глав, NGN – это не простое развитие или комбинация уже имеющихся телекоммуникационных сетей и сетей IP и не технология модернизации отдельных сетевых узлов или фрагментов сети. Это – качественное изменение всей сетевой структуры, своего рода полное комплексное решение, включающее в себя и эволюцию традиционных телекоммуникационных сетей с наследованием всех их преимуществ, что, в частности, показано в следующем параграфе.

9.2. Взаимодействие Softswitch и ОКС7

Рассмотренная в главе 7 концепция Sigtran нацелена на надежный перенос сигнальной информации ОКС7 через IP-сеть. Для этого Softswitch взаимодействует с рядом шлюзов MG, расположенных вблизи от источников и приемников информации в ТфОП (на границах сети IP). Взаимодействие обычно обеспечивается при наличии, по крайней мере, двух сигнальных шлюзов SG, в которые включены сигнальные звенья ОКС7. Эта архитектура показана на рис. 9.4, причем в число используемых протоколов входят SCTP, M3UA и M2PA или M2UA, которые рассматривались в главе 7.

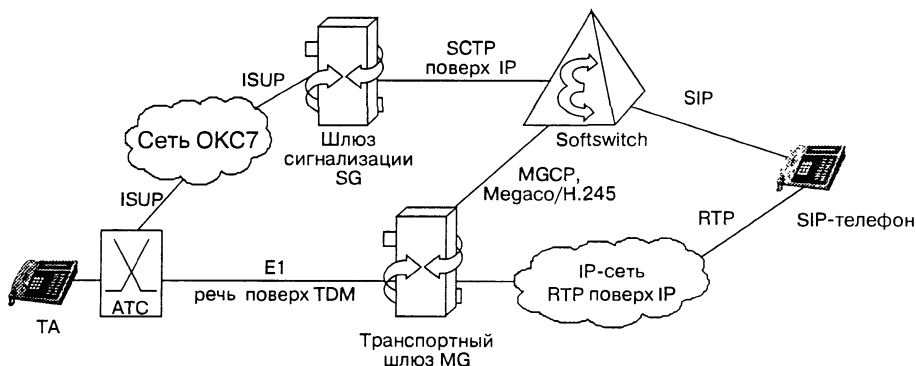


Рис. 9.4. Взаимодействие ОКС7 и архитектуры Softswitch

9.2.1. Инкапсуляция ISUP в SIP

Протокол SCTP и ассоциированные с ним уровни адаптации обеспечивают возможность пересылать информацию протокола приложений ОКС7 из оконечного пункта ТФОП в центр сети VoIP, где расположен Softswitch, получающий таким образом доступ к сигнальной информации для маршрутизации вызовов в сети VoIP. Сами протоколы приложений ОКС7 могут использоваться или не использоваться в сети VoIP; в последнем случае такие протоколы, как ISUP, отображаются в таких эквивалентных протоколах VoIP, как рассмотренный в главе 4 протокол SIP. Отображение SIP-ISUP работает очень хорошо, если одна сторона соединения является узлом VoIP, а другая – узлом ТФОП. Однако когда IP-сеть с Softswitch обеспечивает функции транзита между TDM-сетью коммутации каналов на исходящей стороне и такой же сетью на входящей стороне, могут возникать проблемы. Поскольку протоколы SIP и ISUP разработаны разными способами, редко удается найти прямое соответствие между сообщениями и параметрами одного протокола и сообщениями и параметрами другого. Кроме того, чтобы обеспечить взаимодействие, нужно учитывать различия между конечными автоматами, таймерами и пр. Результат получается хотя и работоспособным, но часто далеким от совершенства. Причина состоит в том, что один протокол может быть несколько лучше в одном отношении, а другой – лучше в другом отношении. Следовательно, взаимодействие часто происходит по схеме логического И, т.е. функциональные возможности, получаемые в результате взаимодействия, ограничены только теми возможностями, которые поддерживают оба протокола. Например, поля заголовков SIP могут переносить информацию, которой просто нет в ISUP. Таков, в частности, заголовок *Retry-after*, поле которого в ISUP вовсе негде отобразить.

ISUP тоже содержит информацию, которую нелегко отобразить в заголовках SIP (если вообще возможно). Часто приходится отображать такую информацию в SIP лишь частично, или вообще отбрасывать. Это не так уж плохо, если вызов поступает от пользователя ТФОП к пользователю SIP, поскольку сервер агента пользователя SIP все равно не смог бы эту информацию интерпретировать. Но когда речь идет о связях TDM-IP-TDM (например, при междугородной/международной связи с использованием VoIP), то в точке входа в IP-сеть ISUP преобразуется в SIP, а в точке выхода из этой сети происходит обратное преобразование SIP в ISUP. В этом случае результат может оказаться таким, что сообщения ISUP, выходящие из транзитной сети, будут отличаться от сообщений, которые в нее поступили. Чтобы решить эту проблему, можно инкапсулировать сообщение ISUP в тело сообщения SIP. Запросы и ответы SIP используются между Softswitch, и там, где надо, они должны содержать тело сообщения SDP, чтобы описать для этих Softswitch инфор-

мацию, которую необходимо передавать между управляемыми им шлюзами MG. Некоторые из сообщений SIP могут содержать в своем теле также и сообщение ISUP в двоичной форме. В этом случае тело сообщения SIP будет переносить и описание сеанса SDP, которое используют Softswitch и шлюзы MG, и инкапсулированное сообщение ISUP, которое транспортируется через сеть IP прозрачно.

Рассмотрим сценарий, который изображен на рис. 9.5.

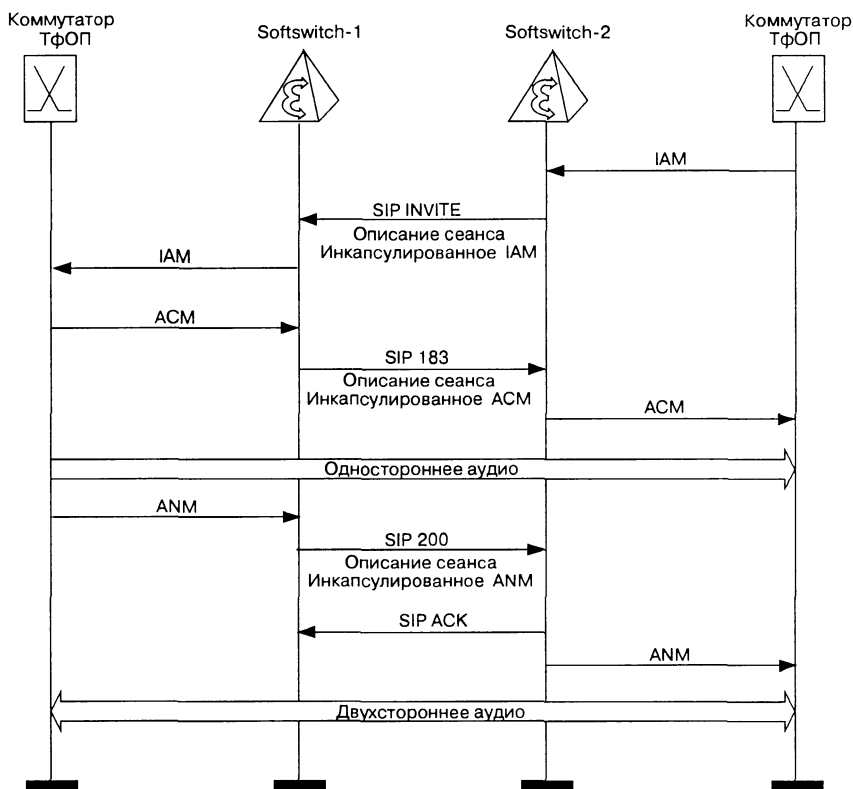


Рис. 9.5. Инкапсуляция сообщений ISUP в сообщения SIP

Входящее сообщение IAM отображается в SIP-сообщении INVITE, которое содержит описание сеанса SDP, а также исходное сообщение ISUP. В пункте выхода из IP-сети информация SDP используется для организации сеанса связи между шлюзами, а информация ISUP извлекается для передачи в ТФОП. Когда соединение в ТФОП установлено, принятое сообщение ACM отображается в SIP-ответе 183 (продолжение сеанса), который содержит временное описание информации SDP и инкапсулированное ISUP-сообщение ACM для передачи в исходящий узел ТФОП. Аналогичный процесс имеет место при ответе на вызов, когда от входящего узла ТФОП поступает сообщение ANM.

Чтобы инкапсулировать сообщение ISUP в тело сообщения SIP, параметр Content-Type в поле заголовка сообщения SIP не должен указывать application/sdp. Вместо этого должен быть следующий формат:

```
Content-type: multipart/mixed; boundary = SDP-ISUP-boundary
```

Content-type указывает, что тело сообщения содержит разные наборы информации в различных форматах. Границу между одним и другим описанием внутри тела сообщения указывает поле границы. Его использование описано в документе RFC 2046 «Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types».

Внутри тела сообщения начало каждой части полезной нагрузки указывается с помощью границы «--boundary» в соответствии со спецификацией в Content-type: header. Поэтому, если бы сообщение SIP должно было содержать поле Content-type, как показано ранее, каждая часть полезной нагрузки в теле сообщения указывалась бы строкой «--SDP-ISUP-boundary». После последней части полезной нагрузки находится другая строка с форматом «--boundary--». В нашем примере последней строкой будет «--SDP-ISUP-boundary--».

SIP-сообщение INVITE с инкапсулированной полезной нагрузкой может выглядеть следующим образом:

```
INVITE SIP: 8129606293@niits.ru SIP/2.0
From: SIP: 8123151515@skri.sut.ru; tag=abcd12345
Call-ID: 123456789@niits.ru
Content-length: xxx
Content-Type: multipart/mixed; boundary = SDP-ISUP-boundary
MIME-Version: 1.0
```

```
--SDP-ISUP-boundary
Content-Type: application/adp
v=0
o=agold 8129606293 IN IP4 4444.333.222.111
S=
c= IN IP4 4444.333.222.110
t=0 0
m=audio 5555 RTP/AVP 0
```

```
-- SDP-ISUP-boundary
Content-Type: application/ISUP; version = ANSI
Content-Encoding: binary
1A 00 01 00 60 00 0A 06 0D 03 80 90 A2 07
03 10 18 27 85 31 48 0A 07 03 11 12 74 66 69
53 EA 01 00 00
-- SDP-ISUP-boundary--
```

9.2.2. Взаимодействие H.323 и ОКС7

Взаимодействие между рассмотренной в главе 5 архитектурой H.323 и ОКС7 может происходить аналогично взаимодействию между Softswitch и ОКС7 и основывается на использовании шлюзов сигнализации SG, в которых заканчивается сигнализация ОКС7. Информация приложений ОКС7 может также переноситься из шлюзов ОКС7 в один

или несколько шлюзов H.323 с использованием Sigtran. Однако, в равной степени, звенья ОКС7 могут подключаться к шлюзу H.323 непосредственно. Такой метод имеет преимущества. В архитектуре H.323 сам шлюз содержит значительную часть логики приложения, необходимой для создания сеанса связи между пользователями, и является также логическим объектом, который выполняет преобразование медиа-информации. Тот факт, что шлюз содержит логику приложения, означает, что он должен передавать и принимать сигнальную информацию управления обслуживанием вызова. Тот факт, что шлюз выполняет преобразование медиа-информации, означает, что он должен находиться на границе IP-сети. Поскольку шлюз расположен на границе сети, вероятно, будет легче и эффективней подключить звенья ОКС7 ТфОП непосредственно к шлюзу.

В действительности взаимодействие ОКС7 и H.323, в некоторых отношениях, легче обеспечить, чем взаимодействие ОКС7 и Softswitch (по крайней мере, для ISUP). Причина заключается в близких взаимоотношениях, которые существуют между ISUP и Q.931. Как-никак, подсистема-пользователь ISUP обслуживает ISDN и является протоколом сети соединительных линий между коммутаторами, использующими протокол доступа ISDN Q.931. Взаимное отображение сообщений Q.931 и ISUP выполняется легко.

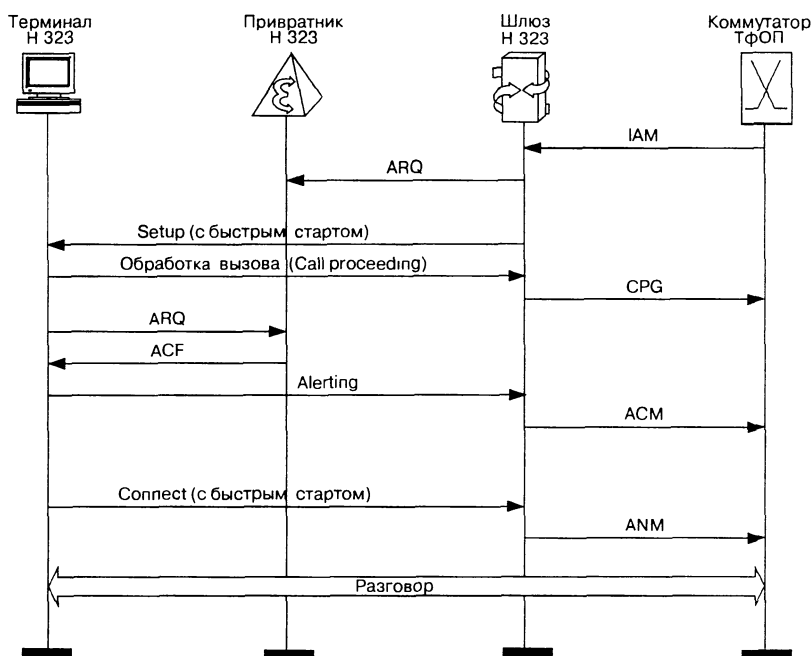


Рис. 9.6. Взаимодействие ISUP и H.323

Например, сообщение Setup Q.931 отображается в IAM ISUP, а ACM ISUP отображается в сообщении Connect Q.931. Поэтому, если бы сеть H.323 должна была принимать вызовы из ТФОП с использованием ISUP, сигнализация была бы подобна показанной на рис. 9.6. Данный пример предполагает использование процедуры H.323 Fast Connect. Если вызываемый терминал H.323 эту процедуру не поддерживает, то сообщение Connect не будет содержать элемент Faststart (быстрый старт). В таком случае приход сообщения Connect в шлюз не приведет к немедленной передаче ANM в сеть ТФОП. Точнее, сначала будут использованы процедуры логического канала H.245 для создания тракта передачи медиаинформации между шлюзом и вызываемым терминалом.

9.3. Эталонная архитектура MSF

Разработкой новой сетевой архитектуры NGN занимаются ITU-T, ETSI, International Packet Communications Consortium (IPCC) и Multiservice Switching Forum (MSF). Во всех четырех версиях эталонной архитектуры NGN присутствует Softswitch, который, как уже упоминалось, может называться узлом управления обслуживанием вызова, телефонным сервером, Call-агентом или контроллером транспортных шлюзов MGC. Эталонная архитектура Softswitch с описанием основных функциональных блоков на основе IPCC (согласно Packet Communication Reference Architecture, v2.0, April, 2003) обсуждалась в главах 1 – 2 и в предыдущем параграфе этой главы, а сейчас рассмотрим архитектуру MSF (согласно Technical Report, MSF TR ARCH 001 FINAL, March, 2003). Архитектура NGN, предлагаемая форумом MSF, представлена на рис. 9.7.

Рассмотрим основные компоненты этой архитектуры.

- *Softswitch* (контроллер медиашлюзов MGC, агент вызовов Call Agent) обеспечивает функции маршрутизации и обслуживания вызовов, логику некоторых дополнительных услуг и взаимодействие с приложениями для услуг, не предоставляемых самим Softswitch, обработку сигнализации и управление терминалами при инициировании, переадресации и терминировании вызовов, а также формирует необходимую информацию для биллинга;
- *SIP-сервер* можно рассматривать как частный случай Softswitch: он обрабатывает SIP-сигнализацию, преобразует ее в H.248 или MGCP для корректной маршрутизации запросов к SIP-приложениям и выполняет функции администрирования и структурирования трафика, а также сбора *CDR*;
- *SIP-клиент* реализует функции, аналогичные функциям SIP-сервера и обсуждавшиеся в главе 4;
- *брокер услуг (Service Broker)* помещается на границе сети Оператора и обеспечивает координацию взаимодействия и управ-

ление серверами речевых приложений, медиасерверами, агентами вызовов и услугами, предоставляемыми третьей стороной, например, Parlay-шлюзами или SCP Интеллектуальной сети;

- сервер приложений AS (Application Server) помещается в сети Оператора и обеспечивает логику дополнительных услуг, не предоставляемых непосредственно Softswitch, например, услуг сервера речевой почты, конференцсвязи или услуг Интеллектуальной сети;

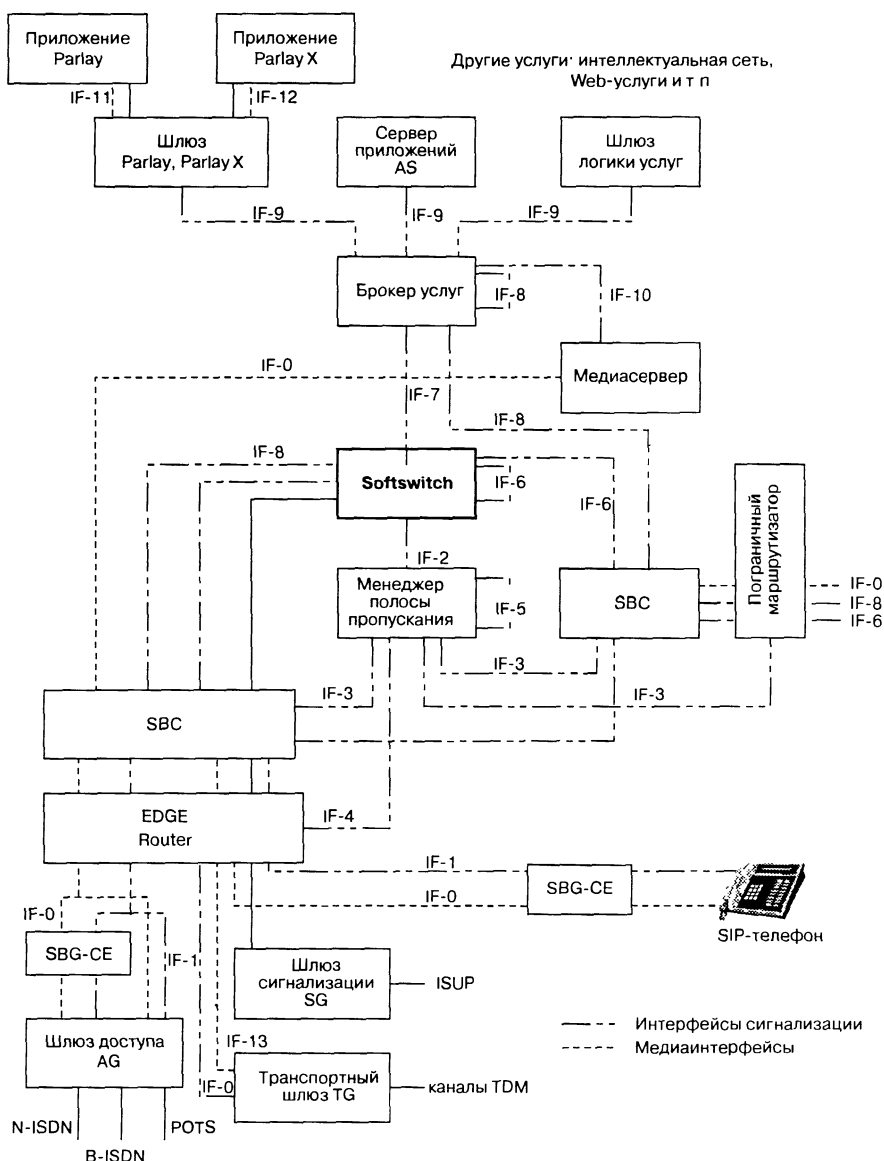


Рис. 9.7. Архитектура NGN согласно MSF. Предоставление речевых услуг в среде пакетной коммутации

- *медиасервер MS (Media Server)* помещается в сети Оператора и работает с информационными сообщениями от и для абонентов, выполняя, например, функции детектирования и генерации тональных сигналов, сервера речевых сообщений, системы оповещения. Для речевых приложений он использует протокол H.248 или MGCP;
- *шлюз сигнализации SG (Signaling Gateway)* преобразует сигнализацию OKC7 сети TDM в среду IP-маршрутизации для обработки ее Softswitch;
- *транспортный шлюз TG (Trunking Gateway)/CAG (Core Access Gateway)* — транспортный шлюз между средой с IP-маршрутизацией и TDM-средой сети с коммутацией каналов. Обычно шлюз использует сигнализацию H.248/Megaco или MGCP;
- *концентратор доступа (Access Concentrator)* — концентратор сети абонентского доступа Оператора, поддерживающий аналоговые порты ТфОП, содержащий окончания абонентских линий «последней мили» или линий с xDSL-портами и интегрированными устройствами доступа IAD, использующий сигнализацию H.248/Megaco или MGCP;
- *менеджер полосы пропускания (Bandwidth Manager)* отвечает за обеспечение необходимого качества обслуживания QoS в сети Оператора, т.е. за выделение соответствующей полосы пропускания и контроль доступа к ней каждого абонентского вызова, а также определяет для каждого вызова политику маршрутизации и переноса медиапотока;
- *пограничный маршрутизатор (Edge Router)* помещается на границе абонентской сети Оператора и маршрутизирует IP-пакеты в его магистральную сеть;
- *интегрированное устройство абонентского доступа IAD (Integrated Access Device)*, помещаемое в точке подключения к сети абонентского доступа и содержащее окончания абонентских линий ТфОП, xDSL, E1, WLL, RON, FTTx, Ethernet и т.п., а также речевые порты и интерфейсы передачи данных для подключения всего набора терминалов абонента.

В соответствии с основными направлениями деятельности MSF наиболее важными на рис.9.7 являются интерфейсы *IF*. Действительно, архитектура с разделенными функциями управления и переноса информации требует наличия вертикальных открытых интерфейсов между вышеперечисленными компонентами мультисервисной сети. Описания интерфейсов IFx сведены в табл. 9.1.

Таблица 9.1. Протоколы взаимодействия между элементами архитектуры NGN по MSF

Интерфейс	Описание	Поддерживаемый протокол
IF-0	Медиаинтерфейс	RTP
IF-1	Взаимодействие SIP-клиента и SIP-сервера (агента пользователя и Softswitch)	SIP, MGCP, H.248
IF-2	Взаимодействие Softswitch с Bandwidth Manager	SIP, NRCP
IF-3	Взаимодействие Bandwidth Manager с Edge Router или с Session Border Controller	H.248, COPS-PR
IF-4	Взаимодействие Bandwidth Manager с Core/Edge Router	Разрабатывается
IF-5	Взаимодействие Bandwidth Manager с Bandwidth Manager	NRCP
IF-6	Взаимодействие Softswitch с Softswitch	SIP, SIP-T
IF-7	Взаимодействие Softswitch с Service Broker	SIP
IF-8	Взаимодействие Service Broker с Service Broker	SIP
IF-9	Взаимодействие Service Broker с Application Server	SIP
IF-10	Взаимодействие Service Broker с Media Server	SIP
IF-11	Parlay Gateway с Parlay приложением	
IF-12	Parlay Gateway с ParlayX приложением	
IF-13	Взаимодействие CAG с Softswitch	H.248 (Megaco), MGCP

9.4. Услуги NGN

Все, о чем говорилось в предыдущих параграфах и главах книги, предназначалось, в первую очередь, для предоставления Оператору возможности быстрого создания новых инфокоммуникационных услуг. На менее конкурентном рынке традиционной коммутации каналов TDM такая задача, разумеется, тоже имела место [7], но там новые телекоммуникационные услуги предлагались, как правило, немногими производителями коммутационного оборудования [6].

Softswitch радикально изменяет эту ситуацию, предоставляя новые возможности благодаря прикладным программным интерфейсам API, основанным на открытых стандартах. Архитектура Softswitch дает возможность Операторам и/или провайдером услуг интегрировать в сети NGN приложения как от производителя Softswitch, так и от разных сторонних производителей, а также самостоятельно разрабатывать свои собственные приложения. В дополнение к функциональной совместимости шлюзов и Softswitch, интерфейсы API стандартизованы для того, чтобы любой независимый сторонний разработчик мог создавать приложения на верхнем уровне архитектуры Softswitch. Услуги сетей нового поколения должны компоноваться чрезвычайно оперативно по принципу *plug and play*, что значительно сократит время и трудозатраты на разработку услуг. Среда создания услуг позволяет разрабатывать новые программные блоки услуг и компоновать услуги из этих

программных блоков, обычно используя специальные инструментальные средства, такие как, например, реализованная в отечественной платформе «Протей» интегрированная среда разработки *IDE (Integrated Development Environment)*. Заложенные в таких инструментальных средствах принципы модульности позволяют провайдеру услуг самостоятельно комбинировать и настраивать компоненты в своей сети, не согласуя все это с производителями оборудования Softswitch. Ушли в прошлое времена монолитных коммутационных узлов TDM-сетей с оборудованием одного единственного поставщика, как это показано в левой части рис. 1.3 главы 1.

Сегодня используются открытые стандартные API – *Parlay*, *JAIN (Java Advanced Intelligent Network)*, *CORBA (Common Object Request Broker Architecture)*, *XML (Extensible Markup Language)*, *CPL (Call Processing Language)*, *CGI (Common Gateway Interface)* и сервисные Java-приложения. Все эти API, расположенные в Softswitch и в серверах приложений, обеспечивают предоставление провайдеру услуг NGN среды, в которой могут быстро развертываться разнообразные услуги. В первой главе на рис. 1.1 уже была показана взаимосвязь интерфейсов API с другими компонентами создания услуг. Рассмотрим их здесь несколько подробнее.

Parlay – платформа для разработки, интеграции и развертывания приложений на базе технологии Java, первоначально ориентированная на сети крупных предприятий. Соединение ее функциональных возможностей с масштабируемостью современных сетей позволяет обеспечить поддержку разнообразных типов передаваемых данных, приложений и клиентских сред и облегчить быструю разработку услуг путем использования распределенных и расширяемых компонентов на базе технологии Java. Разработку стандартов *Parlay* ведет *Parlay Group*, представляющая собой консорциум разработчиков программного обеспечения инфокоммуникационных услуг.

Сетевая топология *JAIN* обязана своим появлением тому, что многие Softswitch размещаются на серверах производства Sun Microsystems, а в качестве API компания Sun и ее партнеры выбрали *JAIN* (развитую интеллектуальную сеть на базе Java). Обеспечивая новый уровень абстракции и имея соответствующие Java-интерфейсы для создания услуг в сетях ТфОП, IP или АТМ, технология *JAIN* позволяет осуществлять интеграцию протоколов IP и IN. К тому же, *JAIN* обеспечивает переносимость услуг, конвергенцию сетей и защищенный доступ как к телефонным сетям, так и к сетям передачи данных. В ней поддерживаются распространенные телефонные протоколы, используемые между различными сетевыми элементами в сетях ТфОП/IN и IP, что иллюстрирует рис. 9.8. На нем показано, как Softswitch отображает интерфейсы управления обслуживанием вызовов/сеансовые интерфейсы в API базовых протоколов SIP, MGCP, MEGACO/H.248, H.323 или стека OKS7 с тем, чтобы обеспечить взаимодействие с телефонной сетью.

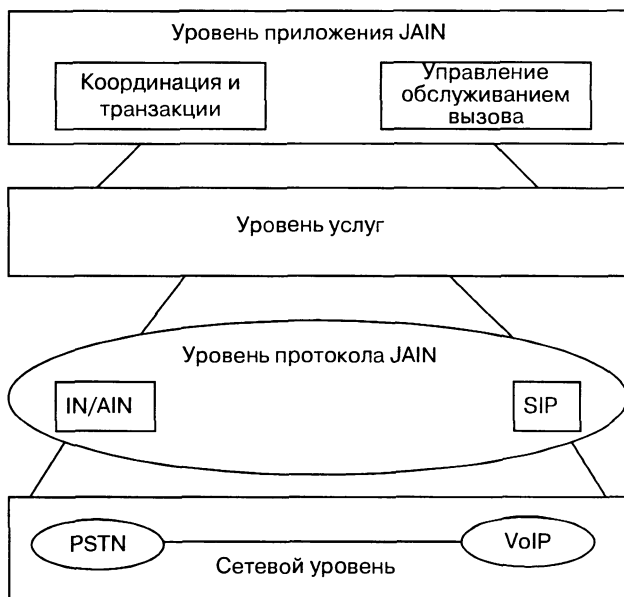


Рис. 9.8. Архитектура JAIN

Архитектура брокера запросов к объектам *CORBA* – открытая, независимая от поставщиков архитектура и инфраструктура, которую используют прикладные вычислительные системы для обеспечения их совместной работы в компьютерных сетях. Используя стандартный протокол *Internet Inter-ORB Protocol (IIOP)*, программа на базе *CORBA* любого поставщика может работать совместно с программой на базе *CORBA* этого же или другого поставщика практически на любом другом компьютере, с другой операционной системой и языком программирования и в другой сети.

Расширяемый язык разметки *XML* – язык HTML нового поколения, который рассматривается как стандартный способ обмена информацией в средах, не использующих общие платформы. Система сетевого управления на базе *XML* использует язык *W3C XML* для управления механизмом передачи данных по сети. Построение API вокруг механизма дистанционного вызова процедуры *RPC (Remote Procedure Call)* на базе *XML* дает простой и расширяемый способ обмена этими данными с устройством.

Описанные выше интерфейсы API размещаются на показанных в правом верхнем углу рис. 1.1 серверах приложений, обеспечивая доступ к инфокоммуникационным услугам NGN. Используя эти API и рассмотренный в главе 4 протокол SIP, можно легко разрабатывать и вводить услуги. Кроме этого, на сервере приложений могут, в принципе, размещаться модели традиционной Интеллектуальной сети [7] и необходимые для нее протоколы TCAP/INAP стека OKC7, как показано на рис. 9.9.

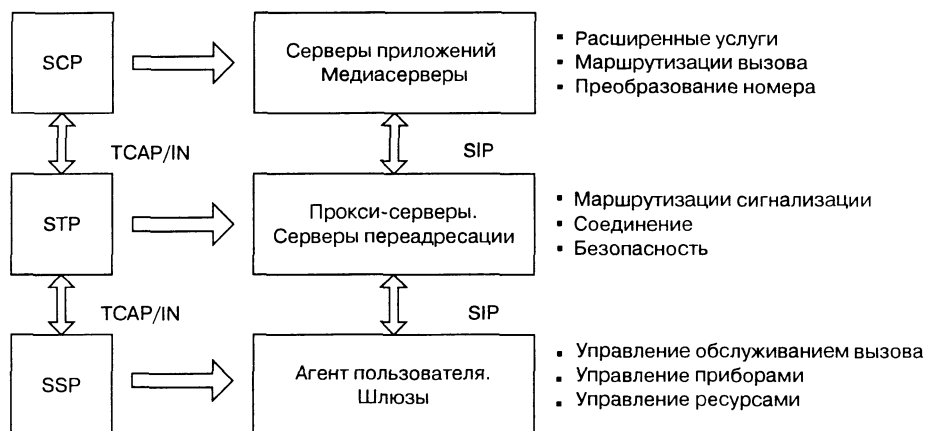


Рис. 9.9. Соответствие архитектуры Интеллектуальной сети и NGN

Медиасервер *MS* обеспечивает специализированные ресурсы для услуг, такие как интерактивную речевую систему *IVR*, средства конференц-связи и факсимильной передачи. Медиасерверы и серверы приложений являются независимыми устройствами и могут разворачиваться на отдельных физических платформах или на одной платформе. Сервер приложений может использовать ресурсы, расположенные на медиасервере *MS*, для обеспечения услуг, которые требуют доступа к мультимедийной информации пользователя. При этом, когда сервер приложений используется в сочетании с медиасервером, логика услуг в сервере приложений имеет доступ ко всем событиям в процессе обслуживания вызова, обычно – посредством сигнализации *SIP*. Сервер приложений взаимодействует по протоколу *SIP* с медиасервером, чтобы получить доступ к потоку информации пользователя с целью обнаружения цифр *DTMF*, воспроизведения и записи речевых сообщений пользователя, создания комбинаций пользовательской информации разных видов (мультимедийной информации), обнаружения и пересылки факсимильных сообщений, передачи записанных объявлений и акустических сигналов, а также для выполнения процедур распознавания речи. Этот доступ к мультимедиа позволяет поддерживать комплексные и сложные услуги, такие как универсальная почта, конференц-связь, обслуживание телефонных дебетных карт, а также приложения *Call-центра* [9]. Некоторые транспортные шлюзы могут также включать в себя функции медиасервера. Если на транспортном шлюзе имеются требуемые ресурсы, сервер приложений может запросить эти транспортные функции через сетевой элемент управления обслуживанием вызовов – *Softswitch*. Как правило, это функции приема и генерирования сигналов *DTMF*, генерирования и распознавания акустических сигналов, а также воспроизведения и записи аудиоинформации. Обработка пользовательской инфор-

мации может производиться либо на транспортном шлюзе, либо на медиасервере. Шлюзы всегда размещаются на границе сети, в то время как медиасерверы могут располагаться на границе сети или в ее ядре.

Взаимодействие между функциональным объектом управления обслуживанием вызова и функциональным объектом сервера приложений иллюстрирует рис. 9.10. Функциональный объект управления обслуживанием вызова определяет, что вызов должен быть переключен на функциональный объект сервера приложений (т.е. передача запроса INVITE) для обработки расширенных услуг. Это переключение может быть инициировано вызывающим абонентом, вызываемым абонентом или каким-либо другим путем. Функциональный объект управления обслуживанием вызова определяет адрес функционального объекта сервера приложений по информации инициирования и пересылает вызов к функциональному объекту сервера приложений вместе с другой информацией об этом вызове. Функциональный объект сервера приложений принимает вызов и вызывает соответствующую расширенную услугу.

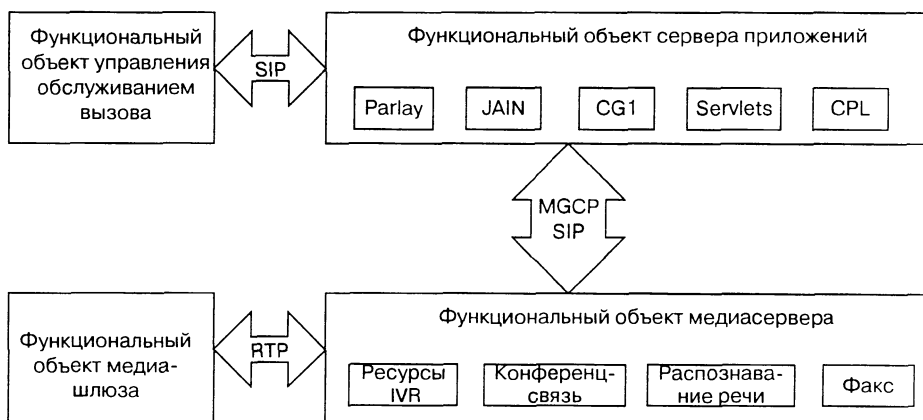


Рис. 9.10. Интерфейсы между сервером приложений и медиасервером

Одна из уникальных услуг, появившихся на рынке приложений Softswitch, которую не поддерживают АТС с коммутацией каналов, – *Web provisioning*, позволяющее операторам Softswitch создавать собственные настройки через Web-сайт, выбирать свои сочетания услуг и включать или выключать индивидуальные услуги по своему усмотрению. Среди других услуг, поддерживаемых Softswitch, предусматриваются: преобразование сообщений речевой почты в сообщения электронной почты, просмотр сообщений речевой почты, «говорящий календарь» (который вслух сообщает о запланированных мероприятиях), речевая передача номера, гибкая маршрутизация вызовов в зависимости от внешних событий, вызовы с помощью иконки

на экране РС, дистанционное управление маршрутизацией вызова (в том числе, его переадресация) через Web-страницу и др.

Речевой Web-интерфейс предлагает услугу доступа к сайтам или электронной почте, т.е. абонент может через свой сотовый телефон получать последние новости, узнавать прогноз погоды и получать электронную почту.

В настоящий момент еще слишком рано прогнозировать, какие приложения, поддерживаемые Softswitch, будут наиболее популярны. Такие приложения, как вызов, следующий за абонентом, речевой доступ к Web-страницам и т.п., сегодня выглядят многообещающими. Но важнее не конкретные приложения, а сама инфраструктура Softswitch с открытыми стандартизованными API, которая обеспечивает создание новых и эффективных инфокоммуникационных приложений.

9.5. COPM

9.5.1. Понятие COPM

Относительная важность тех или иных функциональных возможностей коммутационных узлов и станций меняется во времени. Передача факсов, конференц-связь, dial-up доступ в Интернет и др. из экзотических дополнительных услуг телефонных сетей общего пользования превратились в неотъемлемые функции современных систем коммутации. Не зависящие от связистов обстоятельства, связанные с сегодняшней обстановкой в мире (да и в нашей стране), заставили причислить к таким же обязательным и важным функциям всех узлов коммутации, включая Softswitch, поддержку законного перехвата сообщений или, по-русски, системы оперативно-розыскных мероприятий (COPM).

Под COPM в ТфОП понимается юридически санкционированный доступ правоохранительных организаций к частным телефонным переговорам. Этим уполномоченным организациям, именуемым в международных стандартах аббревиатурой *LEA (Law Enforcement Agency)*, принадлежат так называемые пункты управления ПУ (в российской терминологии) или, согласно терминологии ETSI, средства мониторинга правоохранительными органами *LEMF (Law Enforcement Monitoring Facility)*, обсуждение которых выходит за рамки этой книги. Основное внимание в этом параграфе уделено требованиям к Softswitch, предъявляемым системой COPM и сводящимся к необходимости организовать канал для прослушивания в ПУ контролируемого разговорного тракта, а также канал передачи от ПУ к станции специальных команд управления и от станции к ПУ – сообщений о фазах контролируемых соединений.

Реализация этих требований в Softswitch – отнюдь не тривиальная инженерная задача. Это обусловлено множественностью маршрутов передачи речевых пакетов, относящихся к одному сеансу связи, фактическим отсутствием точек концентрации трафика, где можно экономично реализовать функции COPM, и рядом других трудностей, о которых речь ниже. Но прежде – суть требований COPM.

9.5.2. Законный перехват сообщений

Функция COPM в терминах ETSI называется законным перехватом сообщений *LI (Lawful Interception)*, что, по мнению авторов, достаточно точно отражает суть дела. Имеются некоторые различия в практике применения понятий COPM и LI: COPM в странах СНГ ориентировалась до последнего времени преимущественно на традиционную телефонию, а международные стандарты LI разрабатывались более комплексно, без разделения на способы связи и методы коммутации, с ориентацией исключительно на контент. Кроме того, имеется некоторое различие в организации взаимодействия ПУ и LEA с Оператором связи, связанные с большими полномочиями ПУ по отношению к LEA и отсутствием у Оператора информации о находящихся под контролем абонентов. С учетом этих нюансов, законный перехват сообщений LI используется в этом параграфе как синоним COPM.

Законный перехват сообщений определен ETSI как процесс обеспечения общественной безопасности, в котором оператор сети, провайдер доступа/провайдер услуг (*NWO/AP/SvP – NetWork Operator/Access Provider/Service Provider*) предоставляет официальным уполномоченным лицам доступ к частной информации, например, к телефонным переговорам или сообщениям электронной почты какого-либо лица или организации. Это определение охватывает системы COPM в разных странах, внедряющих оборудование законного перехвата, разрабатывающих соответствующие законодательные акты и инженерные решения, создающих международные рабочие группы по стандартизации спецификаций COPM.

Помимо охвата услуг традиционной и сотовой телефонии, предполагается реализация процедур LI для услуг Интернет, таких как: web-серфинг, e-mail, чат, ICQ, IP-телефония, ftp, telnet и др. Исследуются проблемы систем с зашифрованным трафиком: безопасной e-mail (PGP, S/MIME), безопасного серфинга с использованием HTTPS (SSL, TLS), VPN (IPSec), зашифрованной IP-телефонии (pgr-phone, Nautilus) и т.д., для решения которых рассматриваются два пути – дешифровка информации перед ее передачей к средствам мониторинга, принадлежащим правоохранительным органам, или доступность этим органам ключей шифрования.

9.5.3. Международные стандарты

Общеввропейские стандарты законного перехвата сообщений стремятся гармонизировать национальные документы, опираются на них и, в конечном итоге, призваны их заменить.

Схема организации законного перехвата сообщений согласно общеввропейской концепции показана на рис. 9.11.

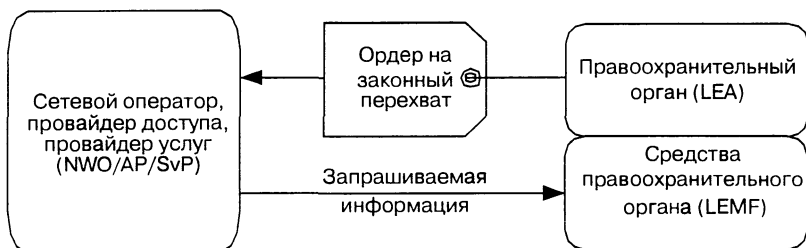


Рис. 9.11. Схема организации законного перехвата сообщений по ETSI

При намерении организовать законный перехват сообщений правоохранительный орган *LEA* подает заявку через уполномоченный орган, например, суд, на получение ордера, который представляется затем в *NWO/AP/SvP* через административный интерфейс H11 (рис. 9.12). Когда ордер на законный перехват получен, средства мониторинга, принадлежащие правоохранительному органу, *LEMF* (*Law Enforcement Monitoring Facility*), через порты интерфейсов H12 и H13 получают перехваченную информацию *CC* (*Content of Communication*), а также связанную с перехватом информацию *IRI* (*Intercept Related Information*) о телекоммуникационных услугах, о соединениях, включая неуспешные вызовы, о местонахождении пользователя и т.п. Ордер может содержать *IRI* и *CC* для конкретного случая перехвата, сведения о периоде своего действия и о предмете перехвата, номер абонента, адрес телекоммуникационные услуги и т.д. Для разных правоохранительных органов и в различных случаях могут применяться те или иные ограничения, устанавливаемые национальными законодательствами и зависящие от абонентских услуг и от сетей. Общеввропейские спецификации содержатся в двух основных стандартах ETSI.

Первый из них, ETSI TS 101 671 «Telecommunications security; Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic», предполагает возможность выбора элементов спецификации интерфейса для того, чтобы соответствовать национальному законодательству, национальным требованиям и правилам правоохранительного органа.

В стандарте ETSI ES 201 158 «Telecommunications security; Lawful Interception (LI); Requirements for network functions» детализируется обобщенная структура реализации законного перехвата сооб-

щения, причем для каждой страны возможна ее трансформация в соответствии с национальным законодательством. В определяемой этими стандартами концепции ETSI упоминаются участники процесса COPM, перечень которых вместе с их ролями приведен в табл. 9.2.

Таблица 9.2. Участники процесса законного перехвата сообщений и их роли

Участник	Роль
Уполномоченный орган (суд)	Выдает LEA законное разрешение – ордер на перехват сообщений
Правоохранительный орган (LEA)	Обращается к NWO/AP/SvP для перехвата информации согласно ордеру и получает результаты перехвата (CC и IRI), касающиеся определенного объекта. Несколько LEA могут одновременно запросить перехват информации одного и того же объекта
Сетевой оператор (NWO)	Эксплуатирует сеть связи и отвечает за обеспечение перехвата информации и ее передачи в LEA через HI. Один и тот же LEA может вести перехват информации в сетях нескольких NWO
Провайдер услуг (SvP)	Предоставляет пользователям услуги в дополнение к услугам самой сети NWO и отвечает за поддержку перехвата в ней информации
Провайдер доступа (AP)	Обеспечивает доступ пользовательского терминала к сети связи
Объект наблюдения	Является пользователем услугами NWO/AP/SvP, имеющим идентификатор перехвата. Под идентификатором перехвата понимается технический параметр, например, списочный номер объекта наблюдения, причем один объект наблюдения может иметь несколько идентификаторов перехвата. Ни объект наблюдения, ни другие стороны, вовлеченные им в связь, не должны быть способны обнаружить факт перехвата
Производители телекоммуникационного оборудования	Обеспечивают реализацию элементов архитектуры законного перехвата в производимом оборудовании, которое используется NWO/AP/SvP. Функциональные возможности оборудования разных производителей должны допускать объединение их в общей телекоммуникационной инфраструктуре

Североамериканская концепция *CALEA (Communications Assistance for Law Enforcement Act)* функционально близка европейской LI. Придирчивое их сравнение позволяет сделать вывод, что при общей схожести моделей CALEA несколько уступает ETSI в области стандартизации COPM для мобильных сетей и GPRS; для стационарных сетей эти модели полностью идентичны.

Инженерные аспекты российского COPM характеризуются следующим. В качестве протоколов для интерфейса HI2 в отечественном COPM на первом этапе выбраны:

- физический уровень – V.24;
- уровень звена данных – LAPB;
- сетевой уровень – packet layer X.25.

Для передачи речевой информации в интерфейсе H13 используются каналы 64 кбит/с тракта E1. Каналы управления и данных в интерфейсе H12 могут быть организованы в 30 и 31 канальных интервалах тракта E1.

9.5.4. Механизмы организации COPM в концепции ETSI

Рассмотрим организацию процесса законного перехвата сообщений в рамках концепции ETSI. Базируясь на приведенном в табл. 9.2 перечне, представим действия участников этого процесса в виде следующего упрощенного алгоритма:

Шаг 1. LEA запрашивает у уполномоченного органа разрешение на ведение законного перехвата.

Шаг 2. Уполномоченный орган выдает LEA ордер на ведение законного перехвата.

Шаг 3. LEA передает законное разрешение NWO/AP/SvP, который, в свою очередь, определяет объекты наблюдения и контрольные идентификаторы согласно полученному ордеру.

Шаг 4. NWO/AP/SvP организует перехват сообщений для/от определенных объектов наблюдения.

Шаг 5. NWO/AP/SvP сообщает LEA о готовности к законному перехвату сообщений каждого объекта наблюдения.

Шаг 6. NWO/AP/SvP получает сведения об IRI и CC контролируемого объекта.

Шаг 7. Данные об IRI и CC контролируемого объекта передаются от NWO/AP/SvP к LEMF/LEA.

Шаг 8. По запросу LEA, или по истечении периода действия разрешения на перехват, NWO/AP/SvP прекращает процедуру перехвата.

Шаг 9. NWO/AP/SvP объявляет LEA о прекращении процедуры перехвата.

Для команд, реализующих перехват, как правило, требуются следующие параметры:

- идентификатор перехвата; идентификатор объекта – параметр, определяемый в ордере, например, указанный номер;
- адрес средств ведения мониторинга правоохранительным органом (ПУ) – для передачи CC;
- адрес средств ведения мониторинга правоохранительным органом – для передачи IRI;
- адресные параметры для средств ведения мониторинга правоохранительным органом (например, для аутентификации и безопасности);
- резервный маршрут;
- идентификаторы NWO/AP/SvP.

Синтаксис команд может различаться в национальных применениях. В отечественных системах СОРМ, например, он определяется выбранным протоколом Х.25. В современной телекоммуникационной сети объект наблюдения может подписаться на услуги, предлагаемые несколькими провайдерами SvP, и имеет возможность выбрать один или более доступов АР (двухпроводная абонентская линия, ADSL-модем и др.) и несколько Операторов сети связи NWO (местная телефонная сеть, Оператор междугородной связи и др.). Такая ситуация требует сотрудничества между Операторами и провайдерами услуг при реализации СОРМ. Если SvP использует среду нескольких АР и NWO, необходима организация их взаимодействия для реализации перехвата.

Для выполнения процедуры перехвата требуется получение от АР и/или от NWO необходимой эксплуатационной информации, касающейся объекта наблюдения и используемых им услуг. В случае совместного предоставления услуг несколькими SvP, любому из них предоставляется сетевая эксплуатационная информация в объеме не большем, чем это нужно для перехвата. Более того, строящаяся сегодня глобальная инфокоммуникационная инфраструктура *GII (Global Infocommunication Infrastructure)* предусматривает, что в организацию перехвата вовлекаются национальные правоохранительные структуры разных государств, в связи с чем возможны сценарии, где в предоставлении услуги участвуют несколько SvP, расположенных в одной или нескольких странах.

9.5.5. Интерфейсы законного перехвата ETSI

Хотя новые сетевые требования к законному перехвату сообщений, возникающие при переходе к NGN, могут привести к пересмотру описываемого ниже интерфейса ETSI, сегодня базовый интерфейс законного перехвата использует три разных порта таким образом, что административная информация, IRI и СС логически разделены между собой. Речь идет о портах HI1, HI2 и HI3 на рис. 9.12, ориентированных на обмен информацией этих трех типов. Порт HI1 выполняет рассматриваемые ниже административные функции и работает обычно в режиме обмена бумажными носителями. Каналы и протоколы для интерфейсов HI2 и HI3 выбираются в зависимости от используемых сетью технологий, например, в российских сетях связи это – временные каналы E1 и протокол Х.25.

Первый из рассматриваемых интерфейсов – административный интерфейс *HI1* предназначен для обмена разнообразной административной информацией между LEA и NWO/AP/SvP (рис. 9.12). Чтобы обеспечить требуемую конфиденциальность информации об абонентах, находящихся под контролем, должно быть обеспечено полное отделение административного интерфейса HI1 от технических интерфейсов HI2 и HI3 в самой сети оператора NWO/AP/SvP.

Обычно интерфейс HI1 имеет двунаправленную структуру, что объясняется необходимостью передачи к NWO/AP/SvP запросов о законном перехвате, например, информации об активизации и о прекращении перехвата или об изменении его параметров, а также необходимостью получения на стороне LEA соответствующих уведомлений. Согласно концепции ETSI исключается любая возможность прямого контроля/управления NWO/AP/SvP оборудованием LEMF/LEA. Сообщениями LEMF и NWO/AP/SvP обмениваются, как правило, путем передачи бумажных документов по факсу или в письмах.

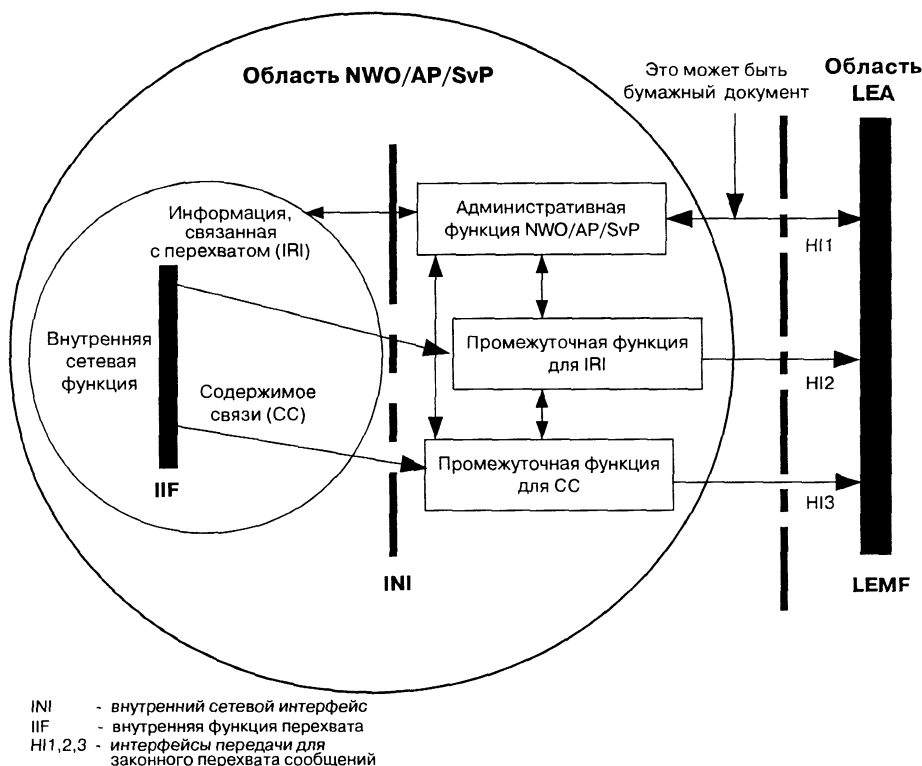


Рис. 9.12. Функциональная архитектура COPM согласно концепции ETSI

Интерфейс HI2 передачи информации, относящейся к вызову, предназначен для транспортировки IRI от NWO/AP/SvP к LEMF/LEA с помощью выбранного для существующей сетевой инфраструктуры протокола передачи данных, например, протокола X.25, или протокола В- или D-канала ISDN по рекомендации ITU-T X.31, TCP/IP и др. Протоколы, использованные для кодирования и передачи данных, основываются на стандартизованных протоколах передачи данных, таких как ROSE или FTP.

На уровне представления (семиуровневая модель OSI) используются правила шифрования *BER (Basic Encoding Rules)*. Индивидуальные IRI-параметры кодируются с использованием *ASN.1*. Формат информационных элементов может быть заимствован из стандартных протоколов (ISUP, DSS1, MAP и IP). Сами IRI-записи передаются индивидуально, хотя возможна и групповая доставка нескольких записей, предназначенных для одного LEA, если это не противоречит ограничениям времени доставки IRI. Именно из-за временных ограничений IRI-записи, как правило, пересылаются немедленно, без накопления. Эти записи содержат обычную информацию Оператора или провайдера, связанную с сетевыми процессами обработки, а также информацию идентификации и управления, соответствующую порту H12.

Для передачи через интерфейс H12 всей необходимой информации определены записи следующих типов:

- IRI-BEGIN – запись, открывающая начало IRI-транзакций,
- IRI-END – запись, закрывающая сеанс передачи IRI,
- IRI-CONTINUE – запись, передаваемая во время сеанса передачи записей IRI.

Сеанс должен начинаться записью IRI-BEGIN и заканчиваться IRI-END. В течение сеанса могут передаваться записи IRI-CONTINUE, содержащие информацию о вызове и СС-информацию. Кроме записей этих трех типов имеется еще и четвертая запись IRI-REPORT, которая предназначена для передачи информации о действиях абонента, не связанных с вызовом, например, при изменении набора дополнительных услуг.

Интерфейс передачи содержимого связи H13 предназначен для транспортировки от NWO/AP/SvP к LEMF/LEA информационного потока СС (содержания телефонного разговора, факса или другого контента). В традиционной коммутируемой телефонной сети содержимое связи должно передаваться к LEMF по коммутируемым каналам на скорости 64 кбит/с.

Существуют два варианта, зависящих от сетевой инфраструктуры: стандартные соединения ISDN, коммутируемые по требованию LEMF для каждого контрольного сообщения, и использование выделенной сети для LI. Заметим, что H12 и H13 – логически различные интерфейсы, хотя и предусматривается возможность корреляции потоков данных H12 и H13 с помощью общего (со ссылкой) поля данных, вложенного в IRI и СС. Возможность эта ориентируется на сети с коммутацией пакетов, но в сетях с коммутацией каналов не используется.

9.5.6. COPM в сетях NGN

Среди услуг NGN выделим следующие, важные в контексте реализации COPM:

- речевое соединение (двустороннее или в режиме конференц-связи) между пользователями сетей коммутации каналов (TDM-сетей) и сетей IP-телефонии;
- услуги Интеллектуальной сети: переадресация, бесплатная связь, телеголосование, связь по карте и пр.;
- доступ пользователей к IP-сети, предполагающий, в частности, обмен сообщениями электронной почты (e-mail), использование систем интерактивного обмена текстовыми сообщениями (chat), обмен HTTP-трафиком, обмен данными FTP и т.д.;
- в перспективе – видеосвязь между пользователями.

На начальных этапах развертывания NGN основной услугой будет оставаться разговорное соединение между пользователями с аналоговыми и цифровыми (ISDN) телефонными аппаратами, подключаемыми к NGN. Но и организация разговорного соединения в NGN имеет принципиальные отличия от установления соединения в традиционных телефонных сетях. Эти отличия, уже упоминавшиеся в начале параграфа, связаны с тем, что медиа-трафик (речь) и сигнальная информация для управления обслуживанием вызова в NGN передаются по разным маршрутам и обрабатываются разными сетевыми устройствами, а не единым узлом коммутации каналов (АТС), как в традиционной ТфОП. Медиа-трафик проходит, как правило, непосредственно между шлюзами доступа (например, МАК) или транспортными шлюзами. Сигнализация же управления обслуживанием вызова проходит через программные коммутаторы Softswitch, но всегда не там, где проходит медиа-трафик.

Отсюда вытекает невозможность получать пользовательскую информацию для COPM от единого устройства управления, определяющего по номерам вызывающего или вызываемого пользователя параметры соединения. Решить эту задачу в частных случаях позволяет новый элемент NGN – пограничный контроллер сеансов *SBC (Session Border Controller)*, которому посвящен заключительный параграф этой главы, и где естественным образом сходятся маршруты медиа-трафика и сигнализации. Но необходимость полного охвата сети связи системой COPM требует решения, общего для всех возможных вариантов архитектуры NGN. Это общее для NGN решение вынуждает реализовать функции COPM одновременно в нескольких сетевых устройствах, в том числе:

- в устройствах управления сетью (Softswitch) с целью постановки на контроль пользователя сети и получения относящейся к его вызову служебной информации;

- в устройствах сети, отвечающих за перенос пользовательской информации (шлюзах досупа, медиа-шлюзах), с целью получения этой информации в интересах правоохранительных органов.

9.5.7. Посредник COPM

Взаимодействие между ПУ COPM и оборудованием Оператора NWO/AP/SvP, т.е. реализацию интерфейсов HI2 и HI3, предлагается производить через специальное устройство – Посредник COPM (*Mediation Device*), – которое, в свою очередь, связано с Softswitch, медиа-шлюзами, абонентским доступом, а также с маршрутизаторами сети IP. Посредник COPM будет исполнять роль конвертера сигнализации, аналогичного известным в отечественных сетях разработкам «Протей» или «Малвин», а также конвертера (шлюза) медиа-поток для доставки перехваченной пользовательской информации к ПУ COPM. Такая архитектура представлена на рис. 9.13.

Здесь ПУ COPM – это пункт управления, применяющийся в существующих сетях с коммутацией каналов и связанный через интерфейсы 1 с Посредником COPM. Интерфейс 1 является стандартным интерфейсом команд и ответов COPM, аналогичным применяющимся в существующих сетях TDM.

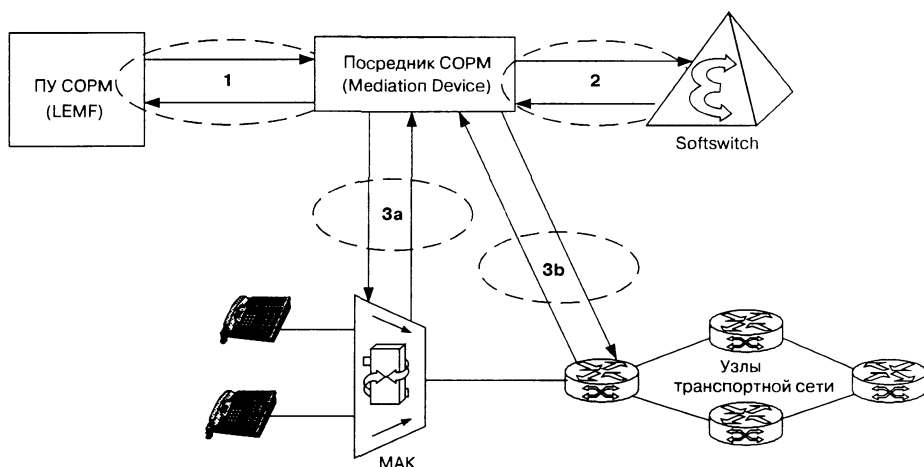


Рис. 9.13. COPM в NGN

Интерфейс 2, используемый для взаимодействия Посредника COPM и Softswitch с целью поставить пользователей на контроль, получать уведомления о действиях пользователей в сети и пр., может быть не стандартным, а предлагаемым разработчиком. Согласование интерфейсов 1 и 3 обеспечивается Посредником, тем самым достигается независимость функций COPM от оборудования разных производителей.

Интерфейс 3 между Посредником и медиа-шлюзами (устройствами доступа или оборудованием транспортного уровня) предназначен для получения пользовательской информации и тоже может настраиваться на оборудование того или иного типа. Указанная схема близка к предложениям по обеспечению функций COPM, разработанным ETSI, что будет показано ниже.

Но прежде рассмотрим процесс проведения оперативно-розыскных мероприятий в NGN. Он будет выглядеть следующим образом. От ПУ COPM к Посреднику поступает стандартная команда поставить на контроль пользователя с некоторым идентификатором (интерфейс 1). Посредник обеспечивает установку в Softswitch триггерной точки для этого пользователя (интерфейс 2), для чего может быть применен нестандартный протокол, например, протокол, реализованный в отечественном Softswitch типа МКД. При активации триггерной точки Softswitch передает информацию об этом событии через интерфейс 2 к Посреднику, а далее эта информация поступает в ПУ COPM. Если необходимо произвести перехват пользовательской информации, то по соответствующей команде от ПУ COPM Посредник через интерфейс 3 настраивает оборудование доступа или оборудование транспортного уровня на копирование пользовательского потока данных и передачу его к Посреднику. Затем эта информация передается в приемлемой форме к ПУ COPM.

Интерфейс 3 между Посредником и медиа-шлюзами (устройствами доступа или оборудованием транспортного уровня) предназначен для получения пользовательской информации и тоже может настраиваться на оборудование имеющегося типа.

Заметим, что такой подход соответствует документам ETSI и комитета IETF в области стандартизации решений COPM для NGN, разумеется, с учетом вышеупомянутых отличий российского COPM от законного перехвата сообщений ETSI. В концепциях, предлагаемых указанными организациями, основой COPM тоже является Посредник или *Mediation Device (MD)* – устройство, принимающее с пункта управления COPM запросы перехвата информации и определяющее посредством взаимодействия с сетевым устройством управления элемент сети, который обеспечивает транзит пользовательской информации. Перехват и передача в ПУ COPM пользовательской информации также ведется этим Посредником.

Это может делаться по нескольким сценариям, также видным на рис. 9.13. В одном из них для копирования информации используется интерфейс 3а между Посредником и устройством доступа (например, мультисервисным абонентским концентратором МАК, рассматриваемым в следующем параграфе), в другом сценарии копирование пользовательской информации производится из подходящего для этой цели маршрутизатора транспортного уровня сети NGN через интерфейс 3б.

Использование для перехвата информации устройств транспортного уровня зависит от возможностей обработки соответствующих команд самими этими устройствами. Однако предпочтительным вариантом является обеспечение взаимодействия Посредника COPM с устройством доступа, например, МАК, что гарантирует отсутствие у персонала Оператора связи и у контролируемого пользователя признаков активизации функций COPM.

Реализация интерфейса 3b между Посредником COPM и узлом транспортной сети (маршрутизатором) или специализированным устройством транзита медиа-поток (например, RTP-прокси) удобна в случае применения IP-телефонов, подключаемых к сети NGN без участия устройства доступа, такого как МАК. При этом для всех подобных терминалов (или для терминалов и идентификаторов пользователей, поставленных на контроль), может быть предусмотрен единый узел сети, в котором и будет производиться перехват информации. Кроме того, при использовании в сети подобных терминалов необходимо предусмотреть механизмы принудительной маршрутизации относящихся к ним сигнальной информации и данных к устройству управления сетью.

Рассмотрим более детально процесс перехвата пользовательской информации. На рис. 9.14 представлена архитектура, соответствующая международным документам IETF и ETSI, а на рис. 9.15 – реализованная в МКД архитектура российской COPM.

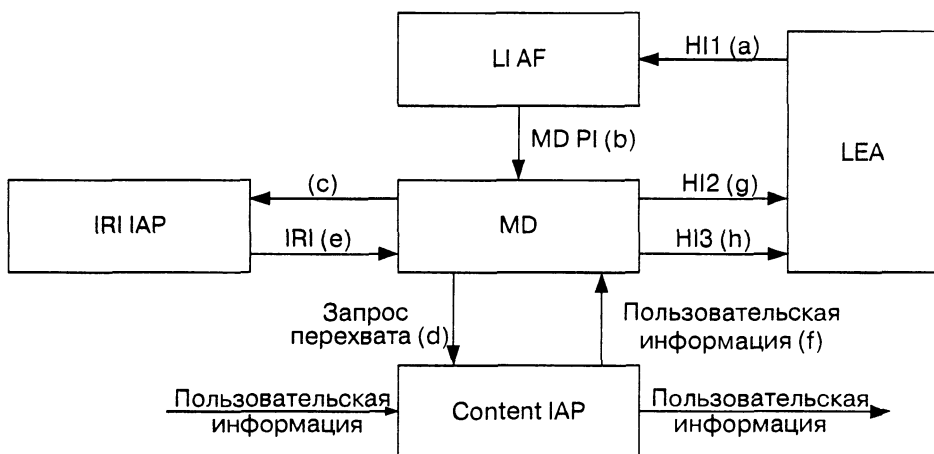


Рис. 9.14. Архитектура законного перехвата по IETF и ETSI

На рис. 9.14 показаны следующие элементы архитектуры законного перехвата сообщений в NGN.

LI AF (Lawful Intercept Admin Function) – функция, обеспечивающая передачу от LEA к Посреднику COPM (в приемлемом для сети виде) запроса поставить на контроль того или иного пользователя.

Преобразование запроса в должный вид и его отправка к Посреднику COPM может производиться с участием уполномоченного человека. Посредник COPM, названный на рис. 9.14 *Mediation Device (MD)*, – устройство, взаимодействующее с другими сетевыми устройствами с целью контроля действий пользователя в сети и перехвата его информации. В частности, MD преобразует перехваченный трафик в формат, требующийся LEA. Если одного и того же пользователя контролирует несколько LEA, MD должно создавать копии перехваченной информации и отправлять их каждому из этих LEA. При этом правоохранительные органы, действующие параллельно, не имеют информации друг о друге.

IAP (Intercept Access Point) – устройство, предоставляющее MD информацию о действиях пользователя в сети, или устройство, в котором производится перехват пользовательской информации. Существуют IAP двух типов:

- *IRI IAP (Intercept Related Information IAP)* определяет устройство доступа, обслуживающее пользователя, или маршрутизатор, обрабатывающий поток пользовательских данных. Функции IRI IAP в NGN может выполнять, например, Softswitch или сервер аутентификации и авторизации.
- *Content IAP* – устройство, через которое проходит пользовательская информация и которое обеспечивает перехват этой информации и передачу ее к MD.

Между элементами рассматриваемой архитектуры COPM имеется следующий набор интерфейсов:

a) *H/I1* – handover interface 1, административный интерфейс, через который LEA передает к LI AF запрос поставить на контроль пользователя (имя, паспортные данные и т.п.);

b) *MD PI (MD provisioning interface)* – интерфейс, через который Посредник MD получает от LI AF такие параметры, как идентификатор абонента, время, в течение которого будет вестись контроль, параметры контроля и т.д.;

c) *IRI IAP Provisioning Interface* – интерфейс, через который IRI IAP получает от MD данные, необходимые для перехвата пользовательской информации;

d) *Content Intercept Provisioning Interface* – интерфейс, через который Content IAP получает команду на перехват пользовательской информации; например, для маршрутизаторов Cisco – это команды протокола SNMP v.3;

e) *IRI to MD* – интерфейс между IRI IAP и MD, через который IRI IAP сообщает MD данные, идентифицирующие нужное Content IRI;

f) *Content to MD* – интерфейс между Content IAP и MD для доставки перехваченной информации к MD;

g) *HI2* – интерфейс между MD и LEA для доставки LEA информации об услугах, предоставляемых пользователю, о его соединениях, включая неуспешные вызовы, и о местонахождении пользователя;

h) *HI3* – интерфейс между MD и LEA для доставки LEA пользовательской информации.

Возвращаясь от рассмотренной версии архитектуры IETF/ETSI к российским требованиям COPM, приведем схему на рис. 9.15, являющуюся, по сути, результатом объединения рис. 9.13 и 9.14. В этой схеме отсутствует интерфейс *HI1*, функции которого частично делегированы *HI2*, при этом функции прочих интерфейсов практически не изменяются. Для большей наглядности на рис. 9.15 в скобках даны также обозначения рис. 9.14.

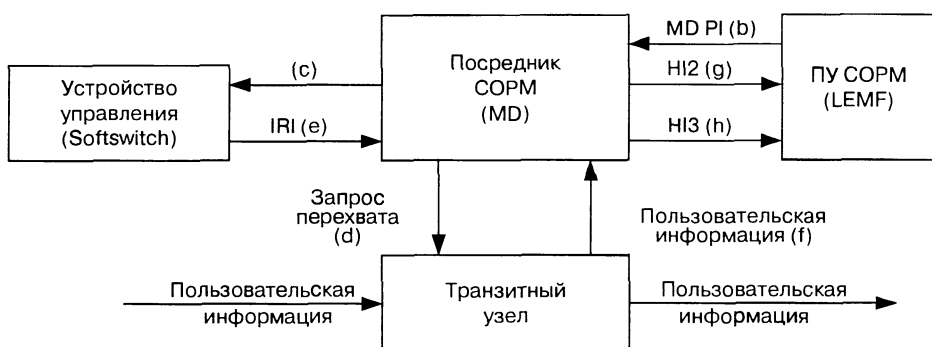


Рис. 9.15. Архитектура COPM для NGN России

Представленная на рис. 9.15 архитектура апробирована в мульти-сервисном коммутаторе доступа Протей-МКД, являющемся первым и пока единственным отечественным Softswitch класса 5, в котором полностью реализованы и сертифицированы функции COPM. Весьма близкая по реализации структура законного перехвата реализована в маршрутизаторах компании Cisco. В терминах рис. 9.14 эти маршрутизаторы являются Content IAP. На основании вышеизложенного можно сформулировать следующие характеристики COPM для сетей следующего поколения с Softswitch:

- при использовании Посредника COPM (MD) достигим порядок взаимодействия ПУ COPM с оборудованием NGN, не отличающийся от установленных правил взаимодействия ПУ COPM с оборудованием традиционных телефонных сетей;
- взаимодействие ПУ COPM с Softswitch при посредничестве специализированного MD обеспечивает независимость функций COPM от оборудования разных производителей, устанавливаемого в сетях NGN;

- операции постановки пользователя на контроль, получения относящейся к вызову информации и т.п. реализуются при взаимодействии Посредника MD и Softswitch;
- операции перехвата пользовательской информации (прослушивания телефонных переговоров) могут производиться в устройствах сети доступа (например, в мультисервисных абонентских концентраторах или медиа-шлюзах), а также возможен перехват пользовательской информации с узлов транспортной сети;
- интерфейс между Посредником и Softswitch сегодня не стандартизирован, что требует адаптации Посредника к разным интерфейсам Softswitch;
- интерфейс между Посредником и устройствами уровня доступа или транспортного уровня тоже не стандартизирован, а наиболее удобной представляется реализация этого интерфейса средствами протокола SNMP.

9.6. Мультисервисный абонентский доступ

О мультисервисных абонентских концентраторах (МАК) говорилось не только в предыдущем параграфе, посвященном СОРМ. На рис. 9.16 приведен вариант построения NGN на базе этих МАК и рассматриваемого в следующей главе Softswitch класса 5 – мультисервисного коммутатора доступа МКД.

В этой схеме МКД взаимодействует с телефонными коммутаторами ТФОП, использующими систему сигнализации ОКС7. Мультисервисные концентраторы МАК могут включаться в эти коммутаторы по трактам ИКМ через универсальный интерфейс V5.2, поддерживающий до 16 трактов Е1. Но более перспективной сетевой архитектурой является включение МАК в программный коммутатор МКД с использованием протокола H.248. При этом для сети TDM мультисервисный коммутатор доступа выполняет функции пункта сигнализации ОКС7.

Интересной особенностью применения МКД является возможность объединять несколько территориально разнесенных устройств доступа в одно с присвоением им одного кода пункта сигнализации.

Таким образом, в случае, рассматриваемом на рис. 9.16, МКД управляет сетью IP-телефонии, построенной на мультисервисных абонентских концентраторах МАК, а также на устройствах доступа сторонних производителей, поддерживающих протокол управления H.248.

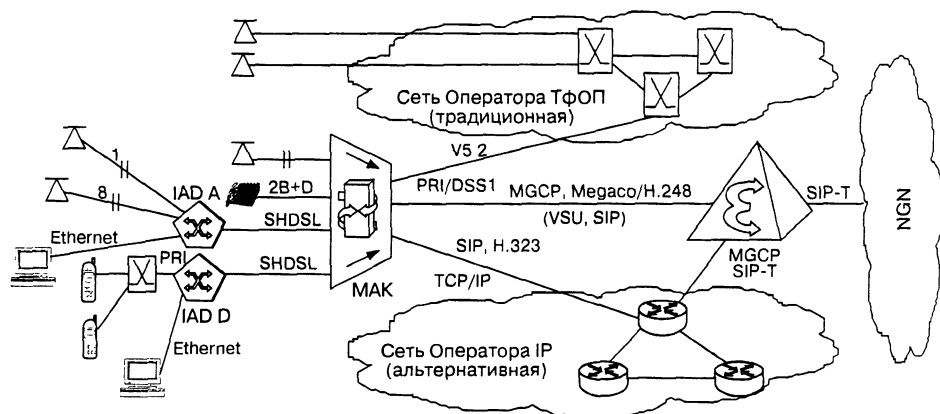


Рис. 9.16. Мультисервисный абонентский доступ

9.7. Пограничный контроллер сеансов

9.7.1. Session Border Controller

Появление пограничных контроллеров сеансов SBC связано с развитием технологий и бизнес-моделей IP-коммуникаций как все более востребованной услуги реального времени в сети Интернет, соседствующей с традиционными услугами Интернет (web-серфинг, ftp, e-mail). Особый интерес к этому новому классу оборудования операторов связи, использующих для предоставления речевых услуг инфраструктуру IP, связан с наблюдающимся сегодня смещением акцентов от взаимодействия операторов VoIP по схеме *TDM-IP-TDM* (при обходе систем междугородной/международной телефонной связи, первые применения IP-телефонии) к прямой передаче трафика *IP-IP*.

Именно для таких соединений, в первую очередь, необходимы SBC – новые устройства NGN сетей. Их основной задачей является соединение отдельных IP-сетей, а главные их преимущества проявляются при передаче через границы сетей речевого, видео или мультимедийного трафика реального времени.

Первоначально провайдеры IP-телефонии взаимодействовали между собой, используя речевые шлюзы по принципу «Back-to-Back». Такая схема работы позволяет обеспечить безопасность соединения и предоставить всю необходимую биллинговую информацию. Правда, за счет дополнительного преобразования кодеков снижается качество речи и повышается стоимость обслуживания трафика. К тому же, такая схема не дает возможности пропускать трафик других мультимедиа-приложений (таких как Instant Messaging и видеопотоки, например). Но пока трафика

IP-телефонии в мире было немного, и он относился, в основном, к соединениям «точка-точка», это не вызывало больших проблем. По мере же роста трафика встала естественная для любых сетей связи проблема межоператорского взаимодействия, на которую и ориентированы появившиеся недавно на рынке оборудования IP-телефонии пограничные контроллеры сеансов.

Традиционная схема работы двух Операторов без SBC выглядит примерно следующим образом: при взаимодействии IP-сетей двух провайдеров на выходе из сети IP-трафик обычно преобразуется в TDM-формат и упаковывается обратно в IP на входе. Этот метод позволяет обеспечить безопасность каждой сети и начислять плату за обмен трафиком, но он довольно дорог и отрицательно сказывается на качестве обслуживания.

Кроме того, большинство корпоративных IP-сетей защищено межсетевыми экранами, и если корпоративным пользователям нужны мультимедийные услуги, то они вынуждены либо позволить всему трафику такого типа беспрепятственно проходить через межсетевой экран, что скажется на безопасности сети, либо модернизировать каждый межсетевой экран, добавив поддержку мультимедийных сеансов, что довольно дорого.

Итак, на пути к пользователю трафик обычно проходит через некоторое количество разных границ, на каждой из которых существует ряд обычных для границ проблем (аналогичных таможенным, паспортным, визовым проблемам на границах между странами). SBC как раз и разрешает все эти весьма актуальные проблемы и обеспечивает обмен мультимедийным трафиком через границы сети, чем и объясняется стремительное появление этого оборудования на рынке, произошедшее раньше, чем появилась теоретическая база для архитектурного построения, функциональных возможностей и соответствующая терминология.

Более того, SBC находятся в состоянии постоянного видоизменения, чтобы приспособиться к ситуации в сетях. Так, ранние решения SBC были ориентированы, в основном, на управление речевыми сеансами, сейчас же добавляется поддержка таких услуг, как передача видео, мультимедийные конференции, дистанционное обучение и т.п.

Таким образом, SBC «отвечает» за решение задач межсетевого взаимодействия, безопасности, надежности и качества обслуживания трафика реального времени. Этот новый элемент сетевой архитектуры, помимо основного названия – пограничный контроллер сеансов SBC (*Session Border Controller*), – имеет также названия *Session Controller*, *Edge Device*, *Boarder Controller*, *Boundary Traversal* или *Edge Session Controller*. Все названия так или иначе отражают его главное назначение – функционировать на границе IP-

сетей и переносить мультимедийный трафик через эту границу без преобразования его в TDM-формат на выходе из сети. Но дело не только в названиях. SBC не обошла и ситуация, типичная для всех новых сетевых элементов NGN, – функции и задачи, возлагаемые на него, очень уж вольно специфицируются разными производителями и могут быть реализованы как в отдельном устройстве, так и располагаться в других сетевых устройствах. Даже понятие «граница сети» здесь довольно условно – это может быть как граница сети Оператора, так и граница между сетью предприятия и Оператором, границы могут быть также определены между разными участками одной и той же сети. Но многое уже определено достаточно строго. Так, ясно, что основные функции SBC сосредоточены на 5 уровне (уровне сеансов) семиуровневой модели OSI. Можно сформулировать основные из этих функций:

- обеспечение взаимодействия сетей: межпротокольного (двустороннее преобразование сигнальных протоколов SIP и H.323), внутрипротокольного (преобразование разных версий стеков протоколов), между Операторами и между провайдерами, включая передачу факсов по протоколу T.38;
- контроль установления телефонных соединений CAC (*Call Admission Control*), управление качеством обслуживания QoS путем ограничения числа одновременно обслуживаемых вызовов;
- безопасность, включая функции RTP-проху для сокрытия внутренней структуры сети;
- функции сигнального контроллера SIP, функции B2BUA (*Back-to-Back User Agent*), функции MGCP проху/NAT, функции привратника H.323;
- обеспечение прохождения трафика через NAT и межсетевые экраны;
- операции с медиа-трафиком, включая преобразование результатов сжатия кодеками G.729, G.729A, G.723.1, G.711A-Law, G.711 μ -Law и т.п.;
- управление качеством обслуживания QoS и поддержка SLA;
- концентрация речевого/сигнального трафика;
- поддержка COPM.

Основные рыночные приложения SBC – это соединение друг с другом сетей разных провайдеров, соединение сети провайдера и корпоративной сети, а также соединение корпоративных сетей в случае построения крупных частных сетей или Extranet. По сути, внедрение SBC выгодно всем игрокам телекоммуникационного рынка. Корпоративный сегмент получит доступ к современным мультимедийным услугам, не меняя существующей системы безопасности (межсетевые экраны, NAT), к тому же сеть может быть

дополнительно защищена средствами SBC. SBC может скрывать топологию сети и защищать ее от атак Denial of Service. SBC позволяют также более гибко управлять в этом сегменте политикой в отношении ширины полосы пропускания, маршрутизации вызовов, QoS и т.д. Для поддержки решения этих и других задач SBC может выполнять различные измерения трафика.

Кроме того, SBC, обеспечивая предоставление услуг через межсетевые экраны и NAT и выполняя преобразование и согласование разных систем сигнализации пакетной сети, существенно расширяет абонентскую базу, помогает поддерживать QoS, обеспечивать соответствующую SLA ширине пропускания и т.п. Подробнее эти и другие функции мы рассмотрим после обзора вариантов архитектурного построения SBC.

9.7.2. Архитектура построения SBC

Логически SBC можно разделить на два функциональных модуля, один из которых занимается всем, что связано с сигнализацией (SBC-SIG), а другой работает с пользовательским трафиком (SBC-MEDIA).

На рынке представлены два варианта построения SBC – интегрированный, при котором оба функциональных модуля расположены в едином аппаратном комплексе, и распределенный, когда каждый из модулей находится в разных сетевых элементах, взаимодействующих по рассмотренному в главе 6 протоколу H.248 или COPS-PR. Рассмотрим оба варианта в контексте соединения сети провайдера с глобальной сетью Интернет, а затем сравним оба подхода. Начнем с интегрированного SBC (рис. 9.17).

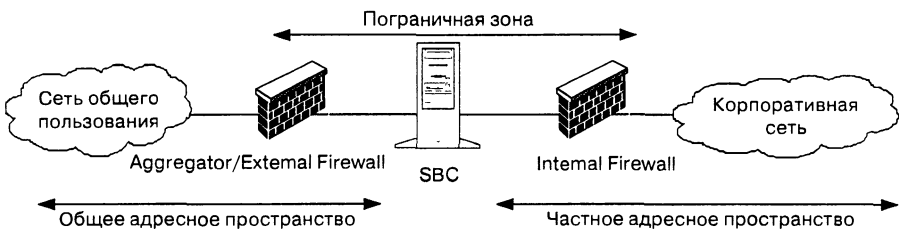


Рис. 9.17. Соединение сети провайдера с Интернет через интегрированный SBC

Внешний и внутренний межсетевые экраны, показанные на рисунке, не позволяют нежелательному трафику проникать в сеть и выходить из сети провайдера. А поскольку SBC обычно содержит функции межсетевого экрана, этот же сценарий может выглядеть следующим образом (рис. 9.18).

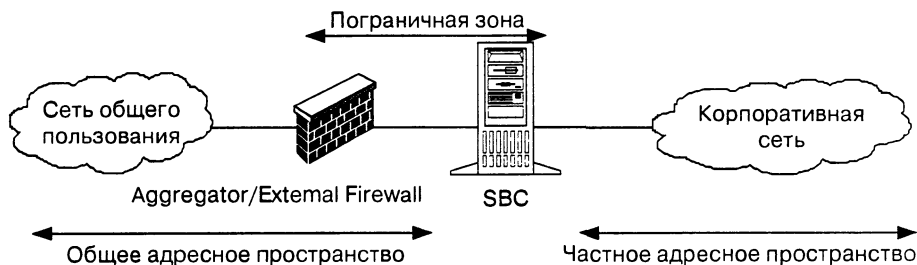


Рис. 9.18. Использование SBC в качестве межсетевого экрана

Если межсетевые экраны – отдельные устройства, то они либо статически запрограммированы администратором пропускать весь трафик, адресованный SBC, либо их динамически конфигурирует сам SBC.

В случае распределенной архитектуры SBC-SIG помещается в сети провайдера, а SBC-MEDIA выносятся на границу сети (рис. 9.19). Весь сигнальный VoIP-трафик из внешней сети направляется к SBC-SIG.

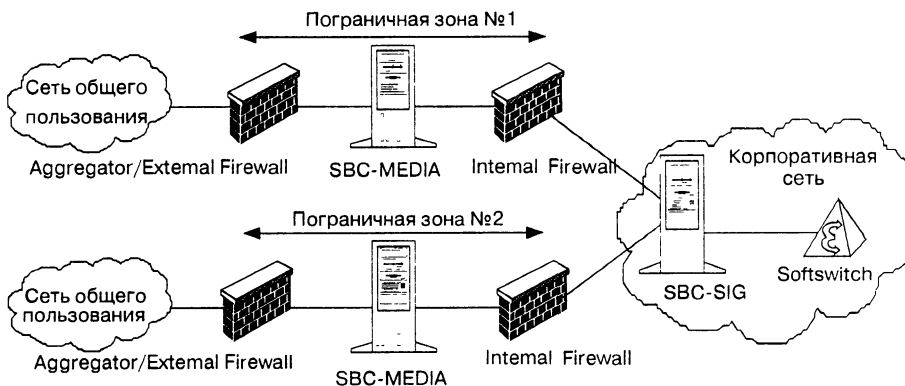


Рис. 9.19. Распределенная архитектура SBC

Большинство производителей сейчас создают интегрированные SBC, которые обычно представляют собой двухпортовые устройства, ориентированные на внешнюю и внутреннюю сети. При этом каждый порт используется как для данных, так и для сигнализации, что создает риск отбрасывания сигнальных пакетов. Следовательно, в будущем, скорее всего, среди интегрированных будут доминировать более сложные SBC, имеющие несколько портов, часть которых будет предназначена для сигнального трафика, а часть – для трафика данных, причем, в идеале, портом каждого типа должен управлять свой процессор. Преимуществом интегрированных SBC является то, что их проще изготавливать, конфигурировать и внедрять. Для

взаимодействия модулей SBC-SIG и SBC-MEDIA в них можно не использовать какой-нибудь сложный протокол связи, а подойдет простейший API, не требующий проведения тестов взаимодействия.

Второй вариант – распределенная архитектура, – тоже неплохо представлен на рынке. Центральное устройство SBC-SIG может обрабатывать сигнализацию, поступающую с нескольких точек доступа и управлять находящимися в них SBC-MEDIA. Соответственно, SBC-MEDIA – более дешевые устройства, чем SBC-SIG, поэтому распределенная архитектура позволяет эффективно строить крупномасштабные решения. Однако такой подход уменьшает сопротивляемость SBC-SIG атакам DoS (*Denial of Service*) и другим всплескам сетевой нагрузки, поскольку SBC-SIG обрабатывает трафик со всех точек доступа.

Для того чтобы удовлетворять базовым требованиям защиты ядра сети от подобных атак, в сети должно находиться несколько SBC-SIG, между которыми делится сигнальная нагрузка, поступающая в сеть, и которые управляют только частью всех SBC-MEDIA. Преимуществом распределенной архитектуры является также возможность независимой разработки и производства взаимодействующих устройств специализированными компаниями. При этом, согласно рассматриваемой в параграфе 9.3 этой главы модели Multiservice Switching Forum, для обеспечения совместимости устройств SBC рекомендуется придерживаться стандарта H.248, однако, производители иногда используют другие протоколы, например, *COPS-PR (Common Open Policy Service Protocol Usage for Policy Provisioning)*. Другим важным преимуществом является то, что SBC-SIG может производить балансировку нагрузки, поступающей на подчиненные SBC-MEDIA.

И, наконец, предваряя обсуждение соотношения SBC и других сетевых элементов, отметим, что функция SBC-SIG может быть помещена непосредственно в Softswitch, управляющий сетью провайдера, что зачастую уже встречается в рассматриваемых в следующей главе существующих Softswitch-решениях.

В начале параграфа уже перечислялись основные функции SBC, теперь постараемся более полно осветить спектр выполняемых ими функций. Разумеется, в каждом практическом случае их набор будет зависеть от конкретного оборудования и места, которое занимает SBC в сети провайдера. Многообразные функции для простоты изложения структурированы по области выполняемых задач.

9.7.3. Функции безопасности

В целях обеспечения безопасности сети практически все SBC могут выступать в качестве NAT (*Network Address Translator*), а также выполнять функцию межсетевого экрана или взаимодействовать с существующими экранами. SBC могут выполнять функцию

сокрытия топологии (в концепции IMS эта функция называется THIG), закрывая для клиентов и других провайдеров информацию о конфигурации сети провайдера и маршрутизации вызовов в ней. Это производится путем преобразования сигнальных сообщений VoIP (например, удалением заголовков SIP Via). Кроме того, SBC может останавливать на входе в сеть сигнальные и информационные сообщения, имеющие дефекты.

Модуль SBC-SIG (в любом из двух рассмотренных выше вариантов построения) может управлять допуском поступающих вызовов в сеть (CAC – *Call Admission Control*) и, таким образом, усиливать безопасность сети, отказывая при необходимости некоторым вызовам в обслуживании. Это позволяет защитить сеть провайдера (и особенно – компоненты Softswitch) от различных атак DoS, массовых всплесков поступающих запросов соединений и общей перегрузки сети.

SBC-SIG ограничивает допустимое количество соединений, устанавливаемых к каждому абоненту, к группе абонентов, ограничивает количество запросов или запрещает («черный список») установление соединений от некоторых пользователей внешней сети. Защитить пользовательский трафик SBC может, шифруя его на входе в сеть или на выходе из сети.

9.7.4. Преодоление NAT и Firewall

Преодоление NAT и Firewall при предоставлении мультимедийных услуг является другой традиционной функцией SBC (рис.9.20). Для выполнения этой функции SBC переписывает транспортные адреса (IP-адреса и порты) сигнальных заголовков и SDP-блоки этих сообщений. Такие преобразования необходимы, поскольку как клиентские сети, так и сети провайдера, защищенные NAT и Firewall, имеют собственное адресное пространство, так что Softswitch не может адресоваться к устройствам внутри сети клиента. SBC заменяет NAT и Firewall со стороны провайдера, в свою очередь NAT и Firewall открывают окна (*pinhole*) сигнализации и данных для SBC, а для всех устройств клиентской сети SBC выступает как прокси-сервер.

Окна для сигнализации обычно имеют статический характер, а окна для данных открываются лишь на время сеанса. SBC создает и запоминает привязку идентификатора пользователя (например, *userphone@niits.ru*) к транспортному адресу сигнального окна (IP-адрес окна, порт окна, TCP-соединение с пользовательским устройством), и для каждого сеанса – его привязку к RTP-порту, открытому на Firewall.

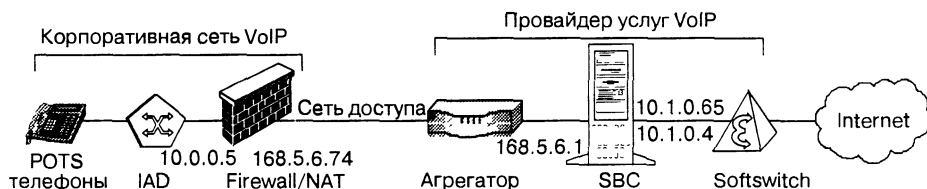


Рис. 9.20. Nat и Firewall

9.7.5. Поддержка QoS и SLA

В большинстве случаев устройства, на которых построена транспортная сеть Оператора (обычно это – IP-маршрутизаторы), не могут различаться в политике QoS, требующей обработки информации верхних уровней модели OSI, такой как идентификаторы пользователя, тип кодека, тип передаваемого трафика и т.д. Эта информация переносится в сообщениях протоколов сигнализации, и SBC, будучи более интеллектуальным устройством, чем маршрутизаторы, может ее анализировать и в соответствии с ней управлять средствами обеспечения QoS (коды DiffServ, MPLS LSP), доступными для понимания маршрутизаторами, в отличие от того, что описано в [3].

К поддержке QoS и SLA можно также отнести управление доступом к сети, уже упоминавшееся в разделе 9.6.3 при обсуждении вопросов обеспечения безопасности. Чтобы избежать перегрузки сети и контролировать соблюдение клиентами соглашений SLA, SBC учитывает уже занятую пользователем полосу пропускания и отказывает в установлении новых соединений, если это приведет к превышению пределов полосы пропускания, оговоренных в SLA.

Механизмы ограничения пользовательского трафика могут быть достаточно гибкими: трафик можно накапливать в буфере и нормализовать. Наиболее известными способами нормализации трафика являются «дырявое ведро» (*Leaked Bucket*) и «ведро с жетонами» (*Token Bucket*). Кроме того, SBC отслеживает количество соединений, установленных для каждого клиента, которое также может быть ограничено в SLA. В дополнение к «черным спискам», упомянутым ранее, номера некоторых абонентов могут быть занесены в «белый список», и для них установление соединения всегда будет разрешено. Такими номерами обычно являются экстренные службы типа 01, 02, 03. SBC даже может отклонять соединения с обычным приоритетом, чтобы обеспечить установление соединений к этим экстренным службам.

9.7.6. Сопряжение сетей

К сопряжению мы решили отнести такие функции SBC, как согласование систем сигнализации, используемых в соседних VoIP-сетях, и согласование формата передачи данных. Являясь, по сути, прокси-сервером для сигнального и пользовательского трафика, SBC может в реальном времени преобразовывать передаваемые пакеты, согласуя их с требованиями обеих сторон. До сих пор наиболее распространенным протоколом в сетях VoIP является рассмотренный в главе 5 протокол H.323. К сожалению, несовместимость оборудования разных производителей, работающего по этому протоколу (вернее, по стеку протоколов), – это сегодня скорее правило, чем исключение. К тому же, согласно представленным в главах 4 и 5 соображениям, доминирование H.323 в ближайшем будущем сменится доминированием протокола SIP, что ставит сегодня задачу обеспечить взаимодействие сетей, использующих разные версии систем сигнализации H.323 и SIP. Будучи постоянно развивающимся протоколом, SIP тоже нуждается в средствах, обеспечивающих взаимодействие его разных реализаций. Таким образом, сопряжение сигнальных протоколов является одной из важнейших задач SBC. Помимо поддержки H.323 и SIP, практически все SBC поддерживают MGCP и/или H.248/Megaco, однако их согласование в SBC обычно не требуется.

Следующей функцией SBC, касающейся согласования сигнализации, является восстановление протоколов. Оно необходимо для взаимодействия с пользовательскими терминалами SIP, не соответствующими стандартам. В этом случае SBC выступает как прокси-сервер, который принимает любые сообщения SIP, а передает только стандартные. В зависимости от конфигурации SBC, поля, содержащие ошибку, могут изменяться или удаляться.

Еще одной важной задачей сопряжения становится преобразование версий протокола IP. Подавляющее большинство IP-сетей сейчас использует версию 4 протокола IP, а широкомасштабное внедрение версии 6 уже довольно долго откладывается, и не последней причиной этого является сложность организации взаимодействия IPv6 с сетями IPv4.

Появление рассматриваемой в главе 11 архитектуры IMS, в которой предусмотрено применение IPv6, может послужить катализатором перехода к новой версии, но для того чтобы эволюция совершалась плавно, незаменимой становится способность SBC к преобразованию IP-заголовков. Даже если SBC имеет распределенную архитектуру, SBC-SIG переписывает SDP данные в сигнальных сообщениях таким образом, что пользовательский трафик обязательно пройдет через тот SBC-MEDIA, который как раз и отвечает за сопряжение по пользовательскому трафику. Описанное выше преобразование версий протокола IP выполняется в отноше-

нии не только трафика сигнализации, но и трафика данных. Обычно в SBC-MEDIA используются отдельные сетевые процессоры для сопряжения по трафику и программируемые аппаратные пакетные фильтры, выполняющие преобразование IP-заголовков. Поскольку речевой трафик в IP-сетях передается по протоколу RTP, каждый SBC-MEDIA поддерживает RTP и RTCP и представляет собой RTP-прокси. Для проходящего речевого трафика SBC может выполнять согласование речевых кодеков. Повсеместно поддерживаются такие кодеки, как G.711 и G.729, но обычно используются и другие кодеки. SBC может не выполнять транскодирование самостоятельно, и в случае, когда оно требуется, должен маршрутизировать трафик к сетевому транскодеру.

Недостатком многих начальных SBC решений было отсутствие возможности передачи по IP факсимильной информации. Дело в том, что при передаче факса по IP не используется протокол RTP. Сегодня SBC поддерживают два способа передачи факса: способ, описанный в рекомендации ITU T.38, и способ Fax Relay, разработанный компанией Cisco. Согласно T.38, данные факса могут передаваться с использованием либо работающего поверх UDP протокола UDP-TL, либо протокола TCP. Сигнальными протоколами, согласно T.38, могут быть H.323, SIP и H.248, причем в последних двух случаях требуется поддержка соответствующих расширений SDP, позволяющих приложениям согласовать параметры, относящиеся к факсимильной передаче. Шифрование трафика также может стать препятствием при взаимодействии сетей. Говоря о безопасности сети, мы уже указывали на способность SBC шифровать пользовательский трафик; притом SBC может поддерживать несколько схем шифрования и обеспечивать двустороннее преобразование. Эта функция оказалась востребованной при внедрении сетей 3G на базе IMS, в которых обязательно использование защиты IPSec. Допустим, оператор проводной VoIP-связи использует протокол *TLS* (*Transport Layer Security*) для обеспечения безопасности сигнальной информации, а пользовательские данные вообще не защищены. В задачу SBC будет входить переход с одной системы защиты на другую.

9.7.7. Сервисные функции для Оператора

На SBC, помимо основных задач, часто возлагаются специфические функции для нужд Оператора. Например, в крупных сетях SBC может использоваться как «концентратор», собирающий вместе трафик некоторой сетевой области. При этом Softswitch и другие SBC будут взаимодействовать только с таким «концентратором», а внутренняя структура этой области будет от них скрыта.

Так как SBC является общей точкой входа/выхода сети, через которую проходит как сигнальный, так и пользовательский трафик, он

позволяет реализовать в сети Оператора поддержку COPM, о чем говорилось в параграфе 9.4. Хотя большую часть этих функций выполняет Softswitch, но SBC могут записывать информацию об обслуживании вызова, необходимую как для COPM, так и для биллинга, а также для планирования сети, сбора статистических данных и других операций с CDR. Кроме того, SBC может отслеживать продолжительность каждого сеанса и обрывать его по таймеру как некорректно проходящий. SBC может также останавливать пользовательский трафик, пытающийся пройти через границу сети после окончания сеанса связи, когда оно обозначено сигнальным сообщением, что позволяет предотвращать кражу услуг.

9.7.8. Сервисные функции для управления

Занимаясь маршрутизацией вызовов, SBC частично претендует на традиционные функции Softswitch. Он представляет собой урезанную версию Softswitch, отвечающую за маршрутизацию вызовов на границе сети, т.е. SBC самостоятельно или при помощи внешнего сервера маршрутизации (*Routing Server*) может выбрать для каждого вызова маршрут, имеющий меньшую стоимость, дающий лучшее качество или удовлетворяющий другим требованиям. При маршрутизации учитывается логика предоставления услуги, требуемые параметры качества и текущее состояние сети. Например, SBC может маршрутизировать исходящие вызовы, требующие связи между сетями разных Операторов междугородной/международной связи, в зависимости от стоимости обслуживания вызова в текущий период времени.

Выполняя эти функции, SBC, во-первых, освобождает от части функций Softswitch и, во-вторых, сводит к минимуму вмешательство обслуживающего персонала в вопросы маршрутизации. Особую ценность интеллектуальная маршрутизация имеет при установке SBC на границе операторских сетей. В этом случае он может выполнять автоматическую ремаршрутизацию устанавливаемой связи (*crankback*). Эта функция подразумевает обработку неудачных попыток установить соединение в сети Оператора верхнего уровня. Вместо того чтобы дать «нижнему» Оператору отказ в установлении соединения, SBC «верхнего» Оператора маршрутизирует вызов в сеть другого, одnogорангового с ним, Оператора, с которым имеется соответствующее соглашение.

Процесс перебора альтернативных вариантов продолжается до тех пор, пока не будет найден Оператор, способный обслужить вызов, или пока не кончится список альтернативных маршрутов. Самому Оператору, использующему SBC, переданный вызов может не приносить прибыли, но он повышает лояльность клиента. Продолжая разговор о различных реализациях архитектуры SBC, приведем сводную таблицу функциональных возможностей SBC.

Таблица 9.3. Функции SBC

Функция	SBC-SIG	SBC-MEDIA
Скрытие топологии	+	-
Предотвращение DoS и контроль доступа	+	-
Шифрование трафика/ преобразование шифров	+	+
NAT	+	-
Firewall	+	+
Преодоление NAT и Firewall	+	+
Контроль полосы пропускания	+	+
DiffServ, MPLS QoS	+	+
Нормализация трафика	-	+
Сопряжение сигнальных протоколов	+	-
Сопряжение IPv4 и IPv6	+	+
Восстановление протоколов	+	-
Согласование кодеков	-	+
Передача сигналов DTMF	-	+
Передача факсимильных сообщений	+	+
Концентрация трафика	-	+
COPM	+	+
Биллинг (CDR)	+	-
Интеллектуальная маршрутизация	+	-

В таблице отражено разделение функций между модулями SBC, причем для выполнения ряда функций иногда требуются совместные действия разных модулей. Как уже упоминалось, в случае распределенной архитектуры функции SBC-SIG может быть размещены в Softswitch или в отдельно стоящем сервере. Функции SBC, необходимые Оператору, зависят, в первую очередь, от того места, которое будет занимать оборудование в его сети. Для интерфейсов UNI, NNI и VPN важны разные задачи. Вышеизложенное иллюстрируется рис. 9.21.

9.7.9. Взаимодействие SBC и других элементов сети

Ключевым моментом, причем не только в контексте этой книги, является взаимоотношение SBC и Softswitch. Задачи Softswitch, в основном, сосредоточены в области управления медиа-шлюзами и маршрутизацией вызовов между ТфОП и IP сетями, а также внутри IP-сети. Хотя SBC может управлять качеством, безопасностью и полосой пропускания для передаваемого трафика, возможности маршрутизации этого трафика у него ограничены.

Для управления обслуживанием вызова всегда необходим Softswitch. В то время как SBC концентрируется на обработке трафика и сигнальных сообщений, Softswitch больше взаимодействует с ба-

зами данных и серверами прикладного уровня. И все же, несмотря на ряд различий, эти устройства схожи: расширение функциональных возможностей SBC может практически сравнять его с простейшими Softswitch 4 класса.

Многие специалисты сегодня считают, что появление нового устройства в сети нецелесообразно, что проще дополнить Softswitch модулем SBC-SIG, а обработку данных поручить межсетевым экранам, пограничным маршрутизаторам, шлюзам и серверам доступа.

Другое распространенное мнение состоит в том, что существование SBC обусловлено лишь причинами недостаточной совместимости разных Softswitch-решений, что носит временный характер. Однако нет ничего более постоянного, чем временное: проблема совместимости оборудования разных производителей будет стоять в течение неопределенно долгого времени развития NGN, в связи с чем авторы, после долгих обсуждений, решили поместить в эту главу об NGN относительно длинный параграф, посвященный SBC.

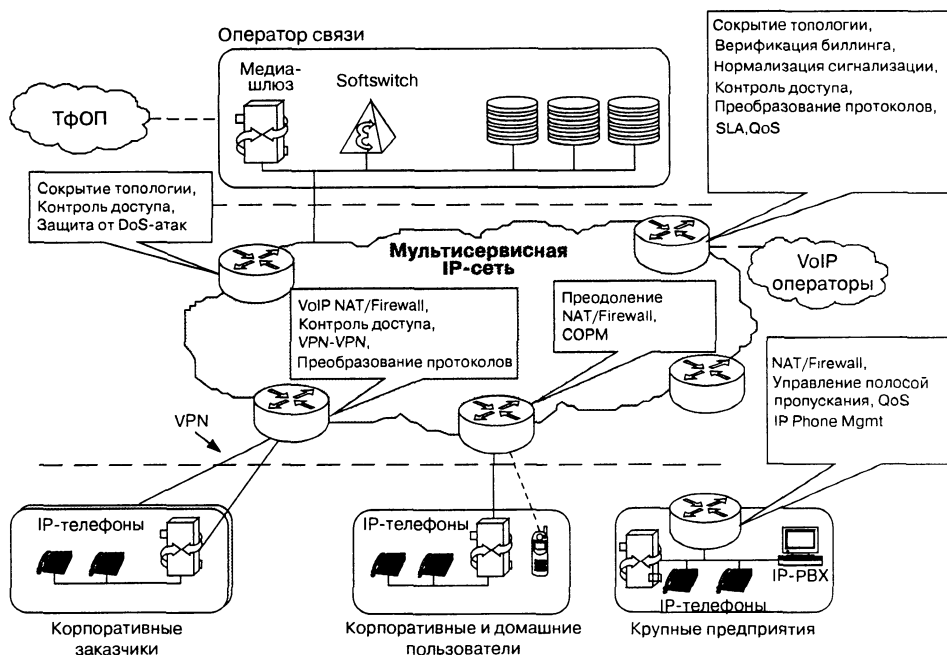


Рис. 9.21. Место SBC в сети Оператора

Кроме взаимоотношения SBC и Softswitch также интересно рассмотреть SBC и устройства NAT и Firewall. Может ли SBC полностью заменить их? В SBC присутствуют подобные функции, но о замене, скорее всего, речь не идет.

Отдельно стоящий Firewall служит не только для обработки речевых соединений, но имеет более развитую систему управления политикой безопасности. Тем более, что мало кто из корпоративных клиентов согласится полностью положиться на оборудование провайдера и постарается защитить сеть со своей стороны. При этом SBC провайдера будет взаимодействовать с Firewall клиента для открытия окон с целью пропуска трафика сеансов мультимедийной связи.

Функция NAT заключается в привязке адресов Интернет к адресам локальной сети. SBC может выполнять похожую функцию, но, опять-таки, он не может полноценно заменить NAT. Проще всего понять разницу между этими типами оборудования можно, представив себе SBC как устройство, выполняющее функцию NAT только для конкретной связи, находящейся в процессе обслуживания.

Недавно появившиеся аналитические обзоры рынка SBC прогнозируют рост популярности оборудования этого типа.

В начале параграфа мы указали на размытость определения SBC, объясняемую ощутимой вариацией его функций в зависимости от класса разработки и места, занимаемого в сети провайдера. Тенденцией в описании разных вариантов сетевой архитектуры стало определение функций вместо физических устройств, и с этой точки зрения можно однозначно утверждать, что SBC как функциональная подсистема будет присутствовать в сетях NGN, но будущее распределение отдельных ее модулей по физическим элементам сети предсказывать пока рано.

Глава 10

Реализация Softswitch

*Любую техническую проблему можно решить,
имея достаточно времени и денег,
но вам всегда будет не хватать либо времени, либо денег.*
NN

10.1. Программно-аппаратные средства Softswitch

Подводя итоги предыдущих 9 глав, авторы решили привести еще одну структурную схему Softswitch. В отличие от двух абстрактных моделей – модели консорциума IPCC, рассмотренной в главе 2, и модели форума MSF, рассмотренной в главе 9, – модель, представленная на рис. 10.1, отражает именно аспекты реализации программно-аппаратных средств Softswitch.

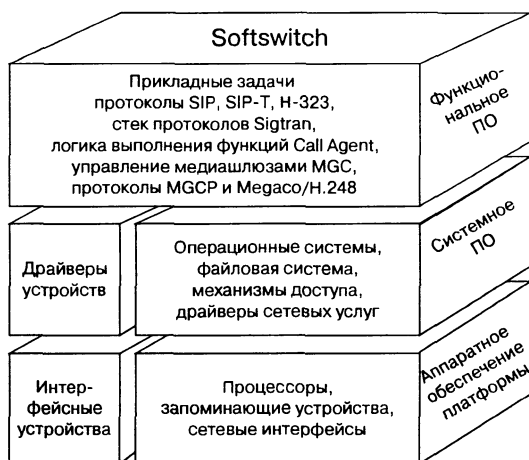


Рис. 10.1. Модель реализации Softswitch

Основное внимание в этой главе уделяется верхнему функциональному уровню, показанному на рисунке, а именно – функциональным возможностям и услугам, поддерживаемым протоколом NGN. Впрочем, по мере возможности, авторы затронут также вопросы производительности, надежности и масштабируемости, которые в большей степени определяются нижними двумя уровнями модели рис. 10.1.

Таблица 10.1. Варианты реализации Softswitch

Компания	Название	Сертификат	Формула сертификата
Alcatel	5020 Softswitch	ОС/1-СПД-762	Оборудование гибкого коммутатора Alcatel версии ПО Network release 3 в составе. Alcatel 5020 – гибкий коммутатор, Alcatel 5023 – шлюз сигнализации, Alcatel 8690 – сервер приложений, Alcatel 8605 – сервер приложений, Alcatel 8688 – медиа-сервер, Alcatel 5795 – центр менеджмента сети производства фирмы Alcatel BELL N.V. (Бельгия), технические условия ТУ665 1-471-04604025-2003, код ОКДП 3222150
Альтертекс	AlterPSS	Нет	
CedarPoint Comm.	Safari C ³	Нет	
Cirpack	HVS	Нет	
Cisco Systems	BTS 10200 Softswitch	Нет	
Clarent	CDSNA	Нет	
Convergent Networks	PMC (бывший ICSX CMS), ICS2000*	Нет	
CopperCom	CSX 1100*, CSX 2100*	Нет	
Экран	Протей-МКД	ОС/1-СПД-787	Программно-аппаратный комплекс с функциями гибкого коммутатора Softswitch МКД (версия ПО 1.3) производства ЗАО “Экран” (Россия), технические условия ТУ 4604021.050 402-2.0, код ОКДП 3222150
Ericsson	ENGINE Integral (TeS)	нет	
Hughes Software	HSS Softswitch	нет	
IpGen	Genovation-MSP	нет	
IntereXchange Carrier	IXC Softswitch	ОС/1-СПД-777	Аппаратно-программный комплекс «IXC System» версии 4.1 производства ООО «Ай-Экс-Си Групп» (Россия), технические условия ТУ 5600-101-47397453-2003, код ОКДП 3222155

Продолжение таблицы 10.1

Компания	Название	Сертификат	Формула сертификата
Huawei Technologies	U-SYS SoftX3000	ОС/1-СПД-800 от 29.06.2004 до 29.06.2007	Комплекс оборудования U-SYS, реализующий функции гибкого коммутатора (Softswitch), в составе: U-SYS SoftX3000 (версия ПО V300), U-SYS MRS6000 (версия ПО CMS6000-АО-8441), U-SYS SG7000 (версия ПО V100), U-SYS AMG5000 (версия ПО V100), U-SYS TMG8010 (версия ПО V100), U-SYS UMG8900 (версия ПО V100), U-SYS IAD132E(T) (версия ПО V100) производства компании Huawei Technologies Co., Ltd (Китай), технические условия Huawei_U-SYS/rus.2004, код ОКДП 3222151
Italtel	iMSS Softswitch	ОС/1-СПД-682	Программно-аппаратный комплекс с функциями гибкого коммутатора семейства iMSS (версии ПО 21.20, 21.21, 21.22, 21.23) производства компании Italtel S.p.A. (Италия), технические условия ТУ-3222150-045-52614645-20 03, код ОКДП 3222150
Lucent Technologies	Lucent SoftSwitch,	ОС/1-СПД-420 ОС/1-СДС-37	Комплекс аппаратных средств и программного обеспечения IP-телефонии SoftSwitch IP (версия ПО Rel. 2.4, 3.1, 3.2) в составе гейткипера SoftSwitch и шлюзов семейства MAX (MAX TNT, APX 1000, APX 8000) производства фирмы Lucent Technologies, технические условия 4604021.034 101-2.0 ТУ, код ОКДП 3222150 АТМ коммутатор Softswitch АТМ (версия ПО: Rel. 2-3) производства фирмы Lucent Technologies (Нидерланды), технические условия 4604021.036 101-2.0 ТУ, код ОКДП 3222410
MetaSwitch	VP3500*	нет	
NEC	CX6800-CA, SS	нет	
NetCentrex	CCS Softswitch	нет	
Nortel Networks	Succession CS2000, CS2000 Compact	нет	
Nuera	ORCA SSC	нет	
OKI	CenterStage NS	нет	
RealEast	RSF 1000	нет	
Marconi	XCD5000	нет	

Окончание таблицы 10.1

Компания	Название	Сертификат	Формула сертификата
Mera	MVTS	ОС/1-СПД-606	Аппаратно-программный комплекс операторского класса MERA VOIP TRANSIT SOFT-SWITCH (MVTS) версии 2.1. в составе: базовый компьютер конфигурации 1 с характеристиками: SlimDesktop Flex ATX, Intel Celeron 1000, RAM 512 Мб, HDD 20 Гб, ОС Linux RedHat 7.3 (FreeBSD 4.4), ПО MVTS версии 2.1; базовый компьютер конфигурации 2 с характеристиками: PLE133, Intel Celeron 1000, RAM 512 Мб, HDD 20 Гб, ОС Linux RedHat 7.3 (FreeBSD 4.4), ПО MVTS версии 2.1; базовый компьютер конфигурации 3 с характеристиками: Intel E7500, Intel XeonDP, RAM 1024 Мб, HDD 100 Гб, ОС Linux RedHat 7.3 (FreeBSD 4.4), ПО MVTS версии 2.1; производства фирмы MERA
Samsung	SSX5000	нет	
sentitO Networks	ONX	нет	
Siemens	SURPASS hiQ 8000	нет	
Sonus Networks	Insignus SSW	нет	
Syndeo	Syion 426 CMS	нет	
Tekelec/Santera/ Taqua	GenuOne Tekelec 3000 MGC/8000 MG (6. SanteraOne OFX/BOX), Tekelec 7000 (6. Taqua OCX)*	нет	
Telcordia	Call Agent	нет	
Veraz Networks	NexVerse ControlSwitch	нет	
Verso/Clarent	C4CM, C5CM	нет	
VocalTec	VSA 3000	нет	
Walkersun	WCS	нет	
ZTE Corporation	ZXSS10 SS1	нет	
UTStarcom	mSwitch	нет	

По аналогии с предыдущей книгой этой же серии [6], посвященной традиционным системам коммутации каналов, в следующих двух параграфах будут рассмотрены отечественные и импортные платформы Softswitch, общий перечень которых приведен в табл. 10.1. Материал этих параграфов построен на базе скрупулезного анализа вариантов реализации трехгранной пирамиды, взятых из самых разных и, как правило, открытых источников. И все же, для правильного его восприятия, кроме эпиграфа к главе, нужно учитывать коэффициенты, взятые авторами из соображений,

следующих законам Мерфи, апробированные сразу в трех опытных зонах Softswitch у Операторов Единой сети электросвязи РФ и имеющие непосредственное отношение к таблице 10.1 и двум следующим параграфам:

- приводимые фирмой-производителем параметры системы нужно умножать на коэффициент 0.5;
- приводимые продавцом параметры системы нужно умножать на коэффициент 0.25;
- планируемые сроки ввода новых функций нужно умножать на коэффициент 2.0.

С учетом чего и начнем.

10.2. Импортные платформы Softswitch

Поскольку пионером Softswitch была компания **Lucent Technologies**, логично обзор оборудования начать именно с **LSS (Lucent SoftSwitch)**, представленного на рис. 10.2. Эта компания не только изобрела сам термин Softswitch и создала первый образец оборудования, но и получила первые сертификаты Мининформсвязи России под номерами ОС/1-СПД-420 и ОС/1-СПС-37.

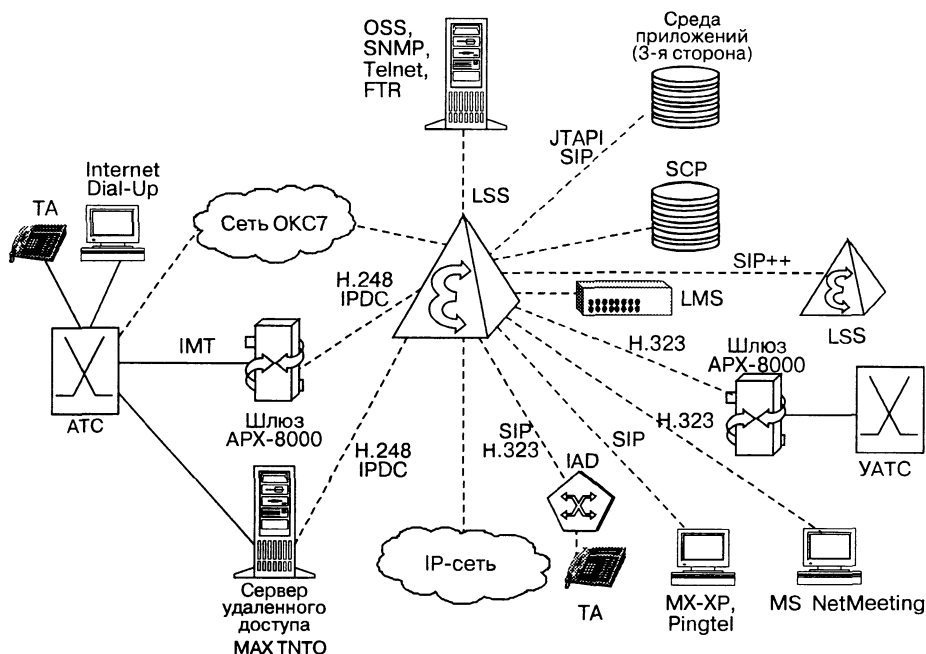


Рис. 10.2. Softswitch LSS компании Lucent

Показанная на рис. 10.1 аппаратная платформа LSS отвечает за ее взаимодействие с внешними устройствами и называется сервером устройств (*Device Server*). Его задачи – поддержка взаимодействия с медиашлюзами; работа с протоколами сигнализации (MTP, ISUP, SIP, MGCP/H.248, BICC и др.). Конструктивно он может быть выполнен в виде отдельно стоящего оборудования или плат для установки в общее шасси. Все функции установления, контроля и разрушения соединений выполняются в отдельном устройстве – сервере обслуживания вызовов (*Call Server*). В нем принимаются решения о маршрутизации вызовов, выполняются алгоритмы обработки соединений, в том числе и на основе информации, получаемой от Интеллектуальной сети. SoftSwitch может работать как с внешними интеллектуальными платформами, выступая в качестве SSP и отправляя запросы в формате TCAP к внешним SCP, так и со встроенными в Softswitch платформами на базе серверов SPINS (*Softswitch Platform for Intelligent Network*) или FullCircle API.

LSS поддерживает протоколы Megaco/H.248 – для взаимодействия с транспортными шлюзами, серверами удаленного доступа и шлюзами ISDN PRI; IPDC 0.15 – для тех же целей; H.323 v1, v2 – для взаимодействия с H.323 шлюзами и конечными пользователями; SIP – для взаимодействия с другими Softswitch, с устройствами SIP, серверами приложений и оконечным оборудованием; протоколы сигнализации OKC7 в версиях ANSI (T1.113, GR-317, GR-394), Q.761, Q.762, Q.763, Q.764, ISUP-ETSI, SCCP/TCAP, (планируется Sigtran), ISDN PRI Q.931, Euro ISDN; поддерживается также программный интерфейс JTAPI.

LSS может взаимодействовать со шлюзами Lucent APX-8000, APX-1000, MAX TNT и с IP-шлюзами других производителей, поддерживающими протокол H.248. Платформа LSS строится на специализированных серверах или на серверах *SUN Netras*. Все устройства LSS для надежности дублированы и могут конфигурироваться в 2-х режимах: защищенном (дублированном) или не защищенном, но с удвоенным количеством обслуживающих приборов. Серверы SPINS представляют собой UNIX-платформу на базе *SUN Solaris*.

Компания **Alcatel** выпустила **5020 Softswitch**, представленный на рис. 10.3. Предлагается три сетевых решения на базе Alcatel 5020 Softswitch: IP-телефония (приложение IPT), обход уровня междугородной/международной связи (приложение LDB) и вывод IP-трафика из сети (приложение IPO). Во все эти приложения входят сервер приложений *Alcatel 5021 Application Feature Server*, обеспечивающий дополнительные функциональные возможности Softswitch, магистральные шлюзы для LDB и соответствующее терминальное оборудование IP для IPT. В Alcatel 5020 Softswitch конфигурируются следующие функциональные модули: модуль подсистемы эксплуатационного управления, модуль управления виртуальными частными сетями; модуль контроля местоположения

пользователя, модуль управления авторизацией, аутентификацией и учета пользования услугами; модуль управления услугами, модуль взаимодействия с другими Softswitch, интерфейсы ОКС7, IPDC, H.323, Megaco/H.248, MGCP, SIP. В приложении IPT поддерживаются протоколы Sigtran.

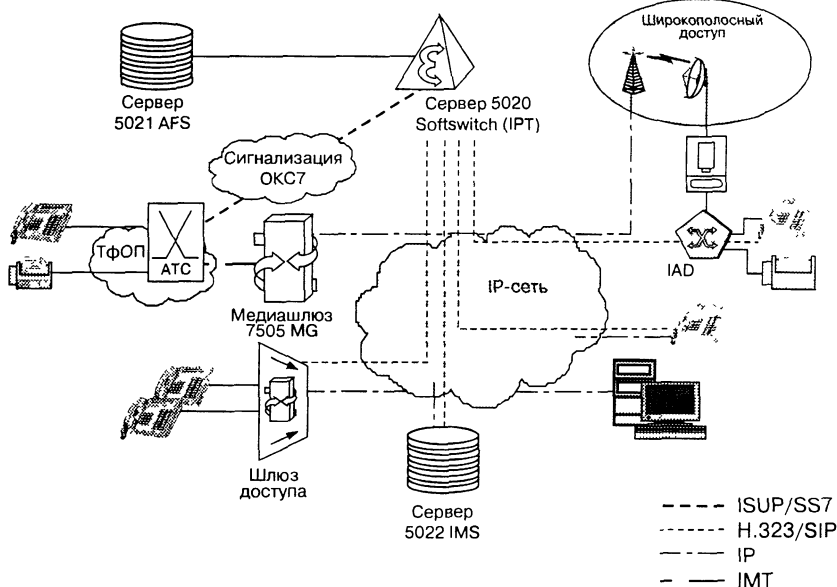


Рис. 10.3. Softswitch A5020 компании Alcatel

Особый интерес представляет медиасервер *Alcatel 5022 IP Media Server*, построенный согласно рассматриваемой в следующей главе концепции IMS и реализующий такие услуги, как рассылка объявлений по IP-сетям, интерактивный речевой диалог по IP, распознавание речи и пр.

Softswitch компании **Ericsson** входит в линейку продуктов **ENGINE**, представляющую собой целую сетевую архитектуру (рис. 10.4). В этой архитектуре телефонным сервером (*TeS*) как раз и является Softswitch, который выполняет функции управления соединениями и обработки сигнальной информации. Для взаимодействия с ТФОП/ISDN используются такие системы сигнализации, как ISUP, DSS1, QSIG и V5.2. Работа ведется через мультисервисные шлюзы TDM, ATM/FR, IP/MPLS. Телефонные серверы взаимодействуют с мультисервисными шлюзами по стандартному протоколу H.248, что позволяет использовать в сети, основанной на телефонных серверах Ericsson, оборудование сторонних поставщиков. Между собой телефонные серверы взаимодействуют по протоколу BICC. В целом же система, управляемая телефонным сервером, может обеспечить поддержку протоколов SIP, H.323, Sigtran. Взаимодействие с Интеллектуальной сетью происходит по протоколу INAP.

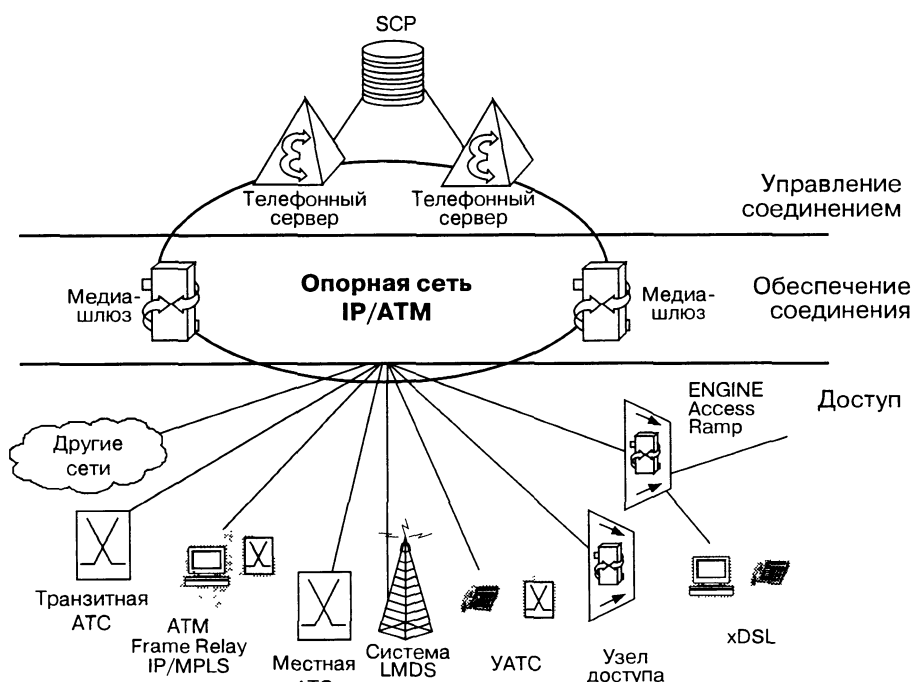


Рис. 10.4. Телефонный сервер ENGINE компании Ericsson

Сама компания рассматривает Softswitch, как сетевую архитектуру, которая состоит из групп компонентов, относящихся каждая к одному из трех иерархических уровней, а именно: к уровню доступа – узлы доступа (ENGINE Access Ramp), к уровню обеспечения соединения – опорные коммутаторы и медиашлюзы на границе сети, и к уровню управления – узел управления услугами IN и телефонные серверы TeS. Последние и являются тем ключевым оборудованием, которое именуется также Softswitch, исполняя роль интеллектуальной части сети, отвечающей за контроль над установлением соединений и за обработку сигнальной информации.

Телефонный сервер может обслуживать до 400 вызовов/сек. При этом возможны соединения следующих типов: PVC – постоянное виртуальное соединение, SPVC – полупостоянное виртуальное соединение, SVC – коммутируемое виртуальное соединение, ATM соединение «точка-точка», LSP – Label Switched Paths (тракты MPLS).

Nortel выпустила на рынок Softswitch сразу две версии своего продукта, назвав их **Succession Communication Server 2000** и **Succession Communication Server 2000 Compact**. Succession Communication Server 2000 (рис. 10.5) поддерживает все программно-реализуемые приложения Succession Centrex/Centrex IP, Succession Primary Voice и Succession VoIP VPN.

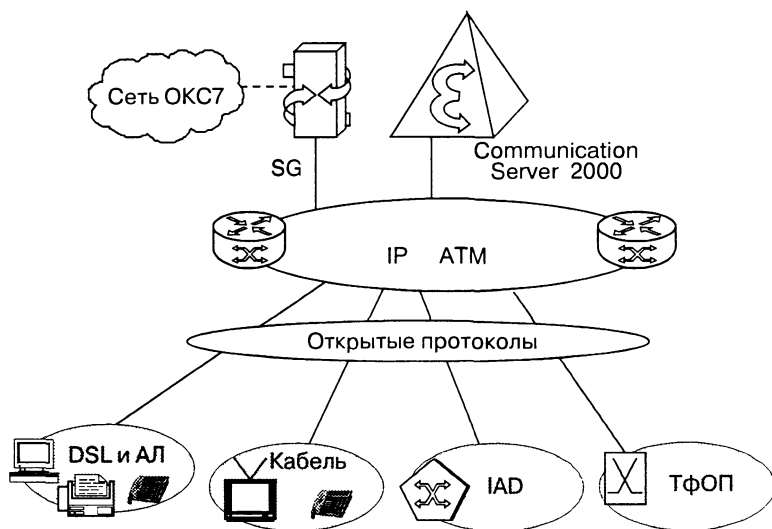


Рис. 10.5. Softswitch Succession компании Nortel

Для предоставления услуг Succession на базе SIP, необходимо использовать дополнительно *Nortel Networks Succession Interactive Server*, который расширяет возможности в области мультимедиа и повышает производительность системы Softswitch. На его базе реализуются сервисные приложения Succession Personal Communication Manager и Succession Multimedia and Collaboration.

В Succession Communication Server 2000 разные функции, связанные с процессом обслуживания вызовов и с управлением системой, распределены по нескольким независимым процессорам. Это позволяет наращивать общую емкость системы, просто добавляя съемные платы. Таким образом, максимальная производительность системы может достигать 2 миллионов вызовов в ЧНН. Емкость системы может составлять до 250000 линий по всем шлюзам и до 165000 магистральных каналов DS0.

Компания **Italtel** разработала оборудование для NGN под названием **iMSS** (*Italtel Multi-Service Solutions*) (рис. 10.6). Это – линейка Softswitch, которая в зависимости от функциональных возможностей конфигурации относится к одной из серий: iMSS 4050/5050 – только Softswitch (5050 сейчас находится в разработке), iMSS 4040/5040 – функции TDM и Softswitch (5040 тоже пока разрабатывается), iMSS 4030/5030 – для работы в TDM-сетях с возможностью дальнейшей модернизации сети.

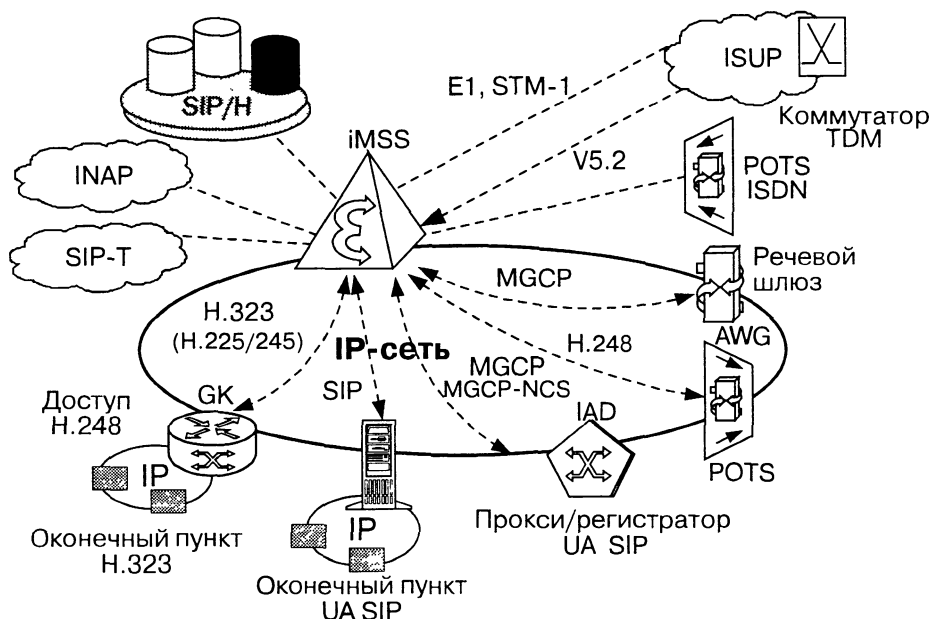


Рис. 10.6. Softswitch iMSS компании Italtel

В состав iMSS входит оптический периферийный модуль *OPM* (*Optical Peripheral Module*), содержащий TDM-интерфейсы (STM-1), коммутационное оборудование, сигнальные терминалы, записи автоинформаторов, многочастотные приемники и т.п. Поддерживается сигнализация OKC7 ISUP, INAP CS1/ASE-R1, PRI DSS1, V5.2, MGCP. Производительность модуля составляет более 135000 вызовов в ЧНН (всего в системе может быть до 100 модулей). Кроме OPM в платформу входят *OMS* (*Operation and Management Supervisor*) – модуль эксплуатационного управления, сервер обработки протоколов *PHS* (*Protocol Handler Server*) с поддержкой H.323 и SIP, модуль основных услуг *BSH* (*Basic Service Handler*), *VTCH* (*Virtual Termination Call Handler*) – модуль, выполняющий функции виртуального линейного окончания и поддерживающий протоколы MGCP, SCTP, а также модуль коммутации и взаимодействия *ISM* (*Interconnection and Switching Module*), представляющий собой коммутационный блок с функциями синхронизации и подсчета времени. iMSS может масштабироваться от 2000 до 300000 DS0. Емкость и производительность одного шкафа при этом будут составлять до 80000 DS0 и до 2000000 вызовов в ЧНН соответственно. Система поддерживает до 1024 звеньев OKC7.

Softswitch компании **Siemens** входит в линейку **SURPASS**. Он представляет собой центральный сервер обработки речевых вызовов и сигнализации, управляющий шлюзами на границах сети передачи данных (рис. 10.7).

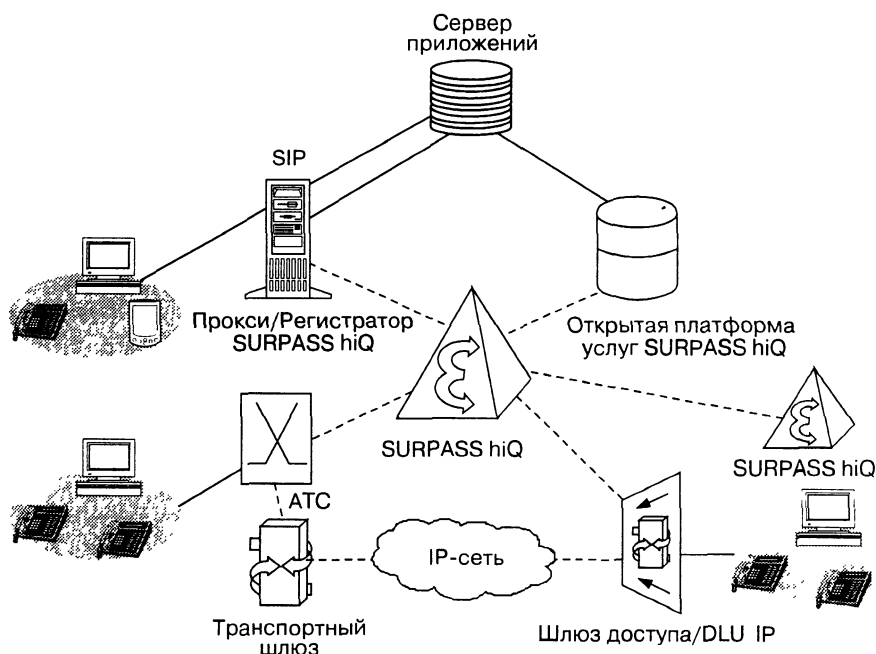


Рис. 10.7. Softswitch SURPASS hiQ компании Siemens

Этот Softswitch содержит несколько компонентов: *hiQ Softswitch* – интеллектуальный центр сервера – поддерживает реализацию приложений VoIP, управляет оборудованием доступа и медиа-шлюзами, а также выполняет функции шлюза сигнализации; *HiQ Open Service Platform* – на основе набора программных модулей предоставляет, вместе с *hiQ Softswitch*, открытые программные интерфейсы; *hiQ Gatekeeper* и сервер аутентификации *RADIUS* – обеспечивают регистрацию пользователей и маршрутизацию в сетях H.323; *HiQ Proxy and Redirect Server* – позволяет включать в сеть SURPASS оборудование SIP; *HiQ Directory Server* – поддерживает *Gatekeeper* и SIP Proxy посредством централизованной пользовательской базы данных на основе облегченного протокола службы каталогов LDAP.

Реализована поддержка национальных вариантов систем сигнализации ISUP, INAP, H.323, SIP, MGCP, MEGACO/H.248. Интегрированный в *hiQ* шлюз сигнализации ОКС7 может обеспечивать туннельную пересылку через IP-сети сообщений ОКС7 с помощью протокола SCTP (Sigtran). В *hiQ* реализованы различные (в том числе и PARLAY) прикладные программные интерфейсы API для взаимодействия с программными продуктами сторонних производителей.

Softswitch американской компании **UTStarcom** носит название **mSwitch** (рис. 10.8). Он имеет более распределенную структуру,

чем рассмотренные выше Softswitch, и является сетевой архитектурой, состоящей из комплекса серверов и шлюзов, в который входят: сервер обработки вызовов (Call Server), сервер приложений (Application Server), Policy Server, сервер поиска местонахождения пользователя (SLR Server), сервер авторизации, аутентификации и ведения счетов (AAA Server), медиа-сервер (Media Server), SCP-сервер.

В mSwitch реализованы физические интерфейсы E1/T1, OC3/STM-1, 10/100Base-T, Gigabit Ethernet, ATM-155, POS. Поддерживаются разные виды сигнализации ТфОП, такие как OKC7 TUP/ISUP, INAP/TCAP/SCCP, V5.2, Q.931, DSS1. Для взаимодействия с остальным оборудованием IP-сети и с другими Softswitch поддерживаются протоколы SIP, SIP-T, H.323, MGCP, Megaco/H.248, SNSP, SIGTRAN, CAMEL, PARLAY/JAIN/JTAPI, BICC. Платформа mSwitch может обслуживать от 10 тыс. до 10 млн. абонентов, обрабатывая до 20 млн. вызовов в ЧНН (100 тыс./шлюз) и нагрузку более 500 тыс. Эрлангов.

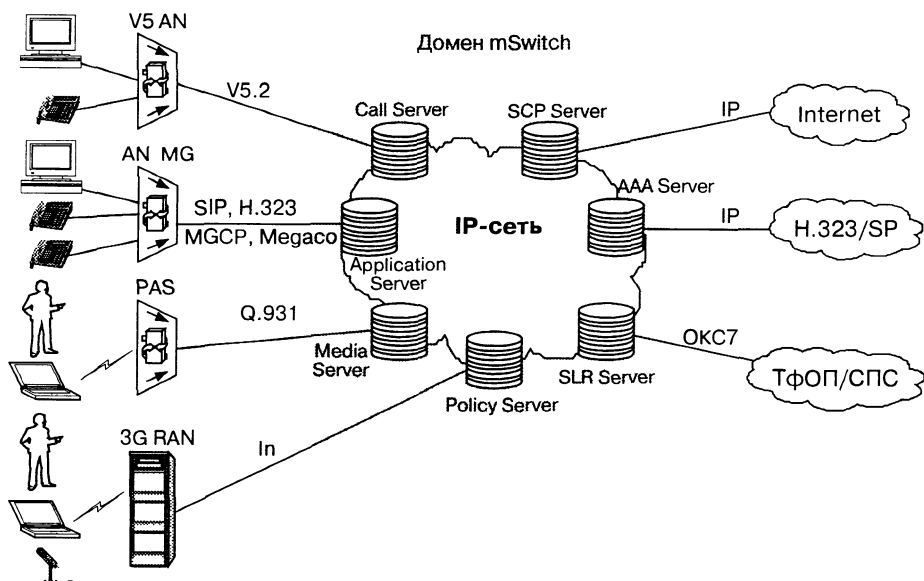


Рис. 10.8. Softswitch mSwitch компании UTStarcom

Компания **Cisco** подошла к разработке **BTS 10200 Softswitch** со стороны IP- и ATM-сетей (рис. 10.9). Аббревиатура BTS в названии означает широкополосные телефонные услуги, что отражает основное применение этого оборудования.

Cisco BTS 10200 Softswitch обеспечивает взаимодействие IP- и ATM-сетей с ТфОП, используя входящие в стек OKC7 протоколы (MTP, SCCP, TCAP, ISUP, INAP), а также SIP, H.323, MGCP, Analog DID,

CAS, CORBA, SNMP. На открытой UNIX-платформе система объединяет программные модули, отвечающие за процесс обслуживания вызова и за предоставление услуг. Все элементы оборудования имеют резервированную структуру, обеспечивающую надежность 99,999 %, что, впрочем, характерно для каждой из представленных в этой главе систем Softswitch. Блок BTS 10200 может встраиваться в общий конструктив или поставляться в собственном шкафу.

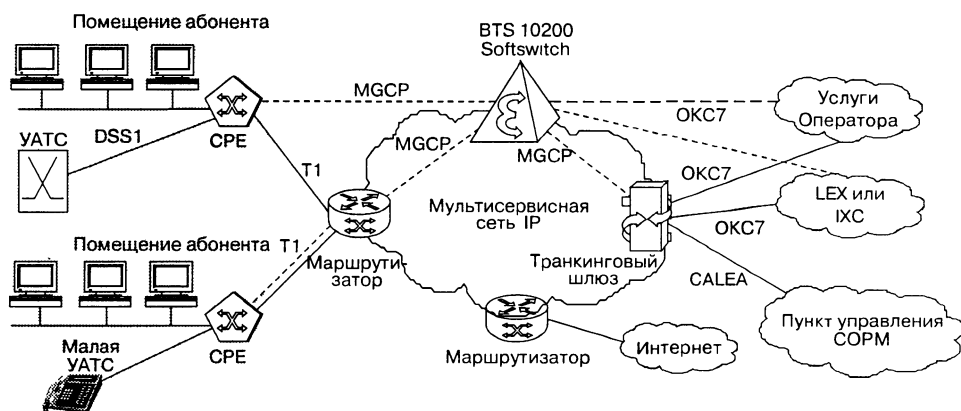


Рис. 10.9. BTS 10200 Softswitch компании CISCO

Каждый BTS 10200 Softswitch включает в себя: контроллер шлюзов *Call Agent*, выполняющий функции управления обслуживанием вызовов и контроль над медиа-шлюзами; систему эксплуатационного управления элементами *EMS*, которая служит посредником между системой эксплуатационного управления сетью и одним или более контроллерами шлюзов, производя администрирование, составление отчетов и реализацию функций биллинга; функциональный сервер, предоставляющий открытые протоколы и гибкую структуру для внедрения новых функций и позволяющий провайдерам услуг использовать в сети оборудование сторонних производителей, а также услуги POTS, Centrex, Tandem и IN для вызовов, обрабатываемых контроллерами шлюзов. Для выполнения функций, связанных с биллингом и обеспечением QoS, в Cisco BTS 10200 Softswitch для каждого вызова создается подробная запись, содержащая такие метрики QoS, как джиттер и задержка пакета. Данные о трафике регистрируются через постоянные интервалы времени в течение суток и хранятся два дня, генерируются подробные отчеты.

Известная своим изобретением промышленного шлюза IP-телефонии компания VocalTec представляет **VocalTec Softswitch Architecture Series 3000 (VSA 3000)**. Это комплекс взаимосвязанного оборудования, образующего определенную сетевую архитектуру.

VSA 3000 – это мультисервисная, многопротокольная платформа, которая поддерживает предоставление независимо от расстояния инфокоммуникационных услуг, не привязанных к местоположению абонента. VSA 3000, будучи системой с распределенной архитектурой, позволяет строить надежную и хорошо масштабируемую сеть VoIP с конвергенцией протоколов и услуг.

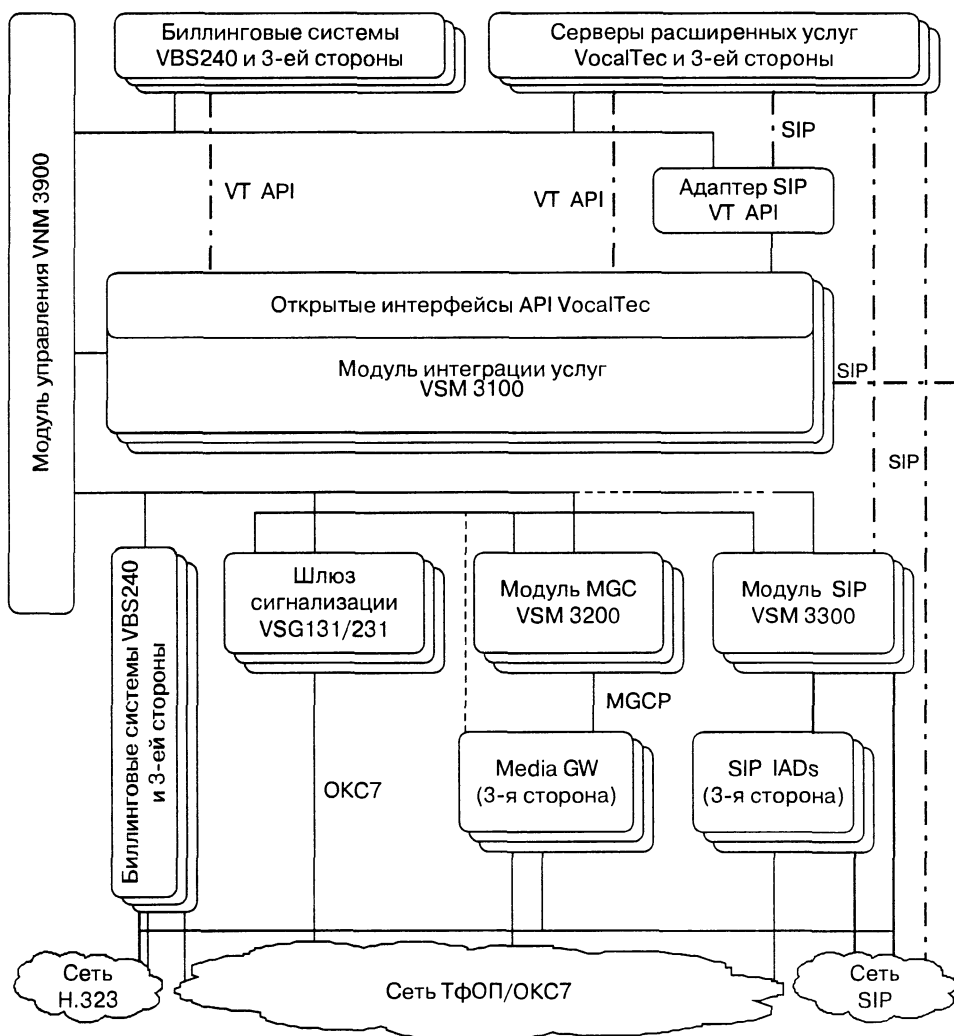


Рис. 10.10. Softswitch VSA 3000 компании VocalTec

Оборудование компании **NetCentrex** называется **CCS** (*Call Control Server*) **Softswitch** и состоит из главного системного модуля, коммутационного модуля, модуля преобразования сигнализации, модуля абонентского доступа, модуля регистрации и базы данных, модуля ведения счетов.

Главный системный модуль – *System Master Unit, SMU*, – распределяет поступившие вызовы по коммутационным модулям.

Коммутационный модуль – *Switching Unit, SU*, – обеспечивает обслуживание вызовов и управляет коммутацией. SU отвечает за маршрутизацию вызовов с выбором маршрута наименьшей стоимости, распределение нагрузки по нескольким шлюзам VoIP, маршрутизацию по месту назначения, управление услугами CLIR/CLIP по запросу. Опционально SU поддерживает маршрутизацию по месту назначения и источнику, виртуальную частную сеть, а также индивидуальное управление обслуживанием вызова, включающее в себя установку языка обработки вызова и профили обслуживания абонентов. В основу SU заложен принцип Интеллектуальной сети. Коммутационный модуль работает с протоколами H.323 и SIP непосредственно, а вместе с модулем абонентского доступа – поддерживает также протокол MGCP.

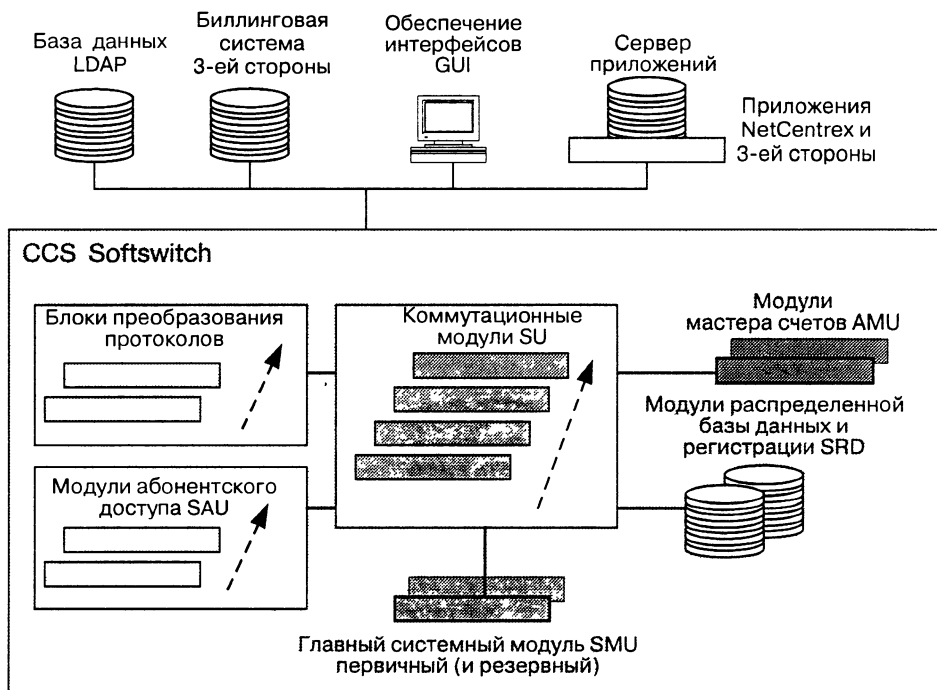


Рис. 10.11. Softswitch CCS компании NetCentrex

Модуль абонентского доступа – *Subscriber Access Unit, SAU* – обеспечивает предоставление услуг пользователям устройств MGCP. SAU может быть централизован или распределен в местах присутствия провайдера услуг. Модуль регистрации и базы данных – *Shared Registration Database Unit, SRD*, – ведет централизованную регистрацию устройств H.323/SIP в зоне действия CCS. Модуль мастера

счетов – *Accounting Master Unit, AMU*, – обеспечивает обмен в реальном времени информацией базы CCS с внешней биллинговой базой данных или сторонней системой биллинга. Большинство услуг предоставляется системой на базе CCS Softswitch при помощи еще одного сетевого компонента *NetCentrex – SVI Media Server*. Он обеспечивает поддержку протоколов сетей ISDN и X.25, а также OKC7 (ISUP/TCAP, INAP), CAS, R2, CAMEL.

Китайская компания **Huawei** разработала свое решение для NGN под названием *U-SYS* (рис. 10.12). Softswitch – **U-SYS SoftX3000** является центральным компонентом системы, способным взаимодействовать с другими SoftX3000 и с Softswitch сторонних поставщиков по протоколам SIP, SIP-T, BICC и H.323. Взаимодействие со шлюзами происходит по протоколам H.248/Megaco и MGCP, а с серверами приложений – на базе PARLAY. Между SoftX3000 и шлюзами сигнализации SIGTRAN, как и между SoftX3000 и мультимедийными терминалами, используется SIP. Из протоколов ТФОП SoftX3000 поддерживает ISUP/TUP, R2 и PRA ISDN. Благодаря поддержке INAP, возможно предоставление услуг Интеллектуальной сети.

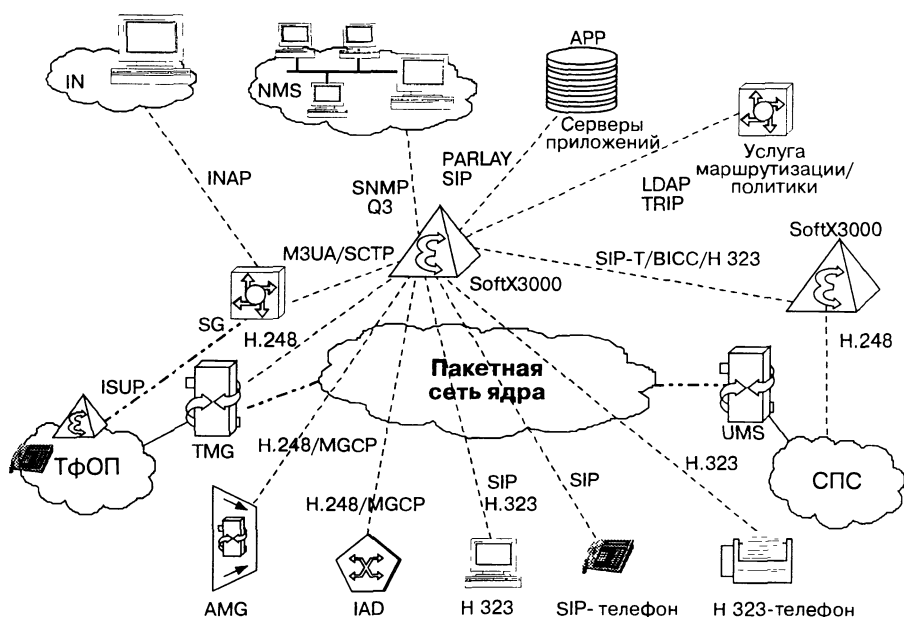


Рис. 10.12. Softswitch U-SYS SoftX3000 компании Huawei

Американская компания **ipGen** представляет на рынке Softswitch свою разработку под названием **Genovation-MSP** (*Multi Service Platform*), представленную на рис. 10.13. Она имеет многоуровневую модульную архитектуру и ориентирована на использование в проводных, беспроводных и транзитных сетях.

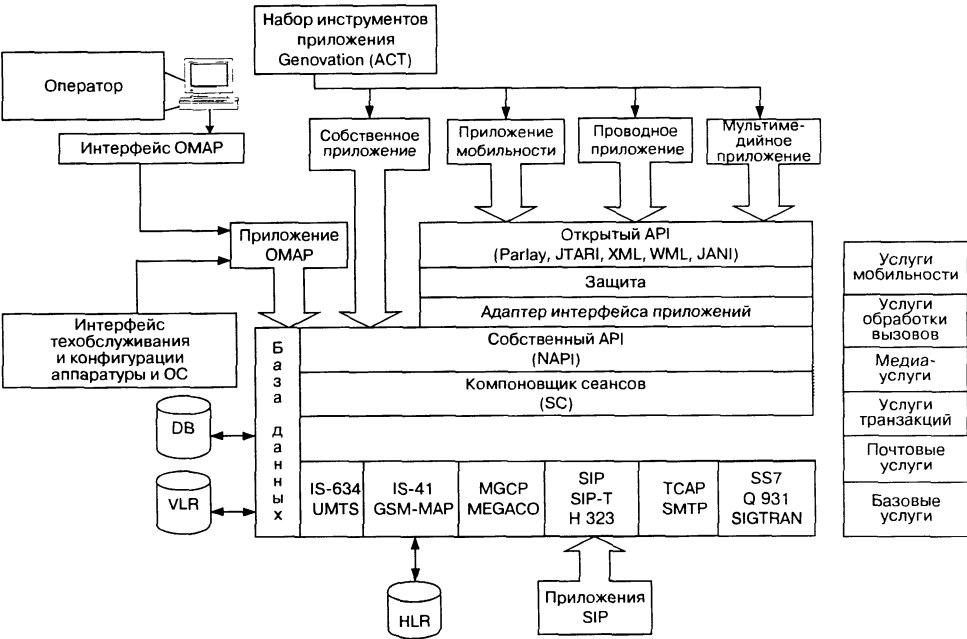


Рис. 10.13. Softswitch Genovation-MSP компании ipGen

Ключевыми компонентами мультисервисной платформы MSP являются API–программные интерфейсы приложений, с которыми на верхнем уровне архитектуры взаимодействует Genovation-MSP, причем поддерживаются как промышленные стандарты, так и внутрифирменные. Для последних MSP преобразует JTAPI, PARLAY, JAIN и S.100 во внутрифирменные API (NAPI).

Представителем корейской компании **Samsung** на рынке Softswitch является модель **Softswitch SSX5000**, основными компонентами которой являются *System Manager (SM)*, *Call Application Node (CAN)*, *Communication Server Node (CSN)* и *Network Address Translation/Firewall Node (NAT/FN)*. Архитектура SSX5000 (рис. 10.14) позволяет гибко масштабировать систему от небольших объемов до крупных систем.

По декларации компании, производительность системы может достигать 5 млн. вызовов в ЧНН и до 125 тыс. одновременно обслуживаемых вызовов. В сети общего пользования система поддерживает до 1 млн. аналоговых или IP-абонентов, или до 1 млн. аналоговых абонентов и 20 тыс. DS0, когда она используется для замены существующих АТС с коммутацией каналов, включая и интерфейсы с сетями коммутации пакетов.

Аналогичные пределы для бизнес-приложений: до 500 тыс. аналоговых, 500 тыс. IP-абонентов и 20 тыс. магистральных каналов DS0. Поддерживаются протоколы MGCP, Megaco/H.248, H.323, SIP, Sigtran (SCTP, M3UA, IUA), OKC7 (MTP 1-3, SCCP).

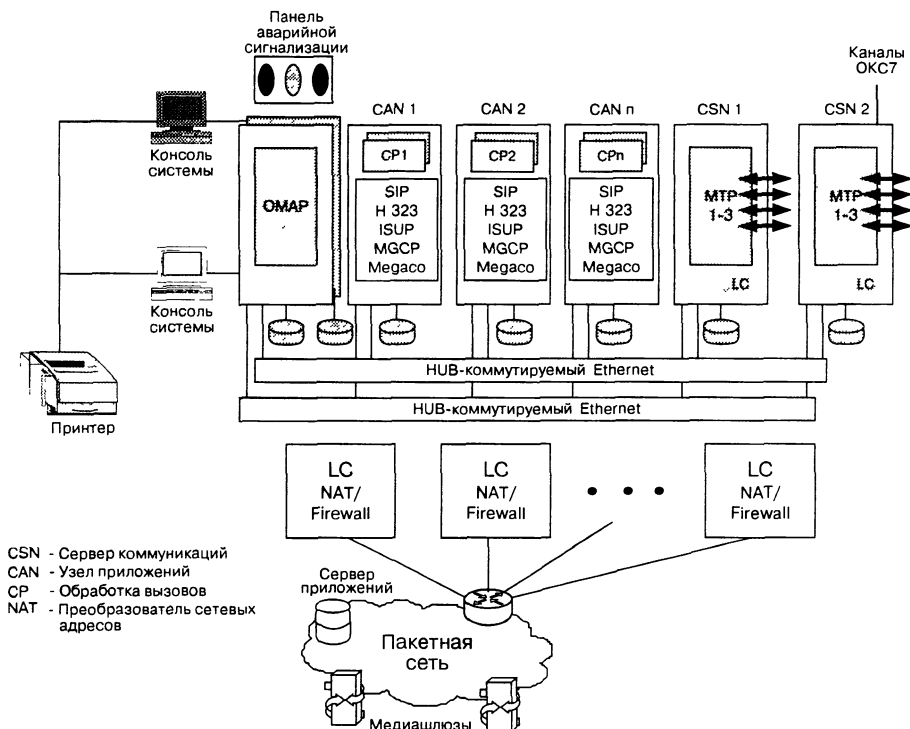


Рис. 10.14. Softswitch SSX5000 компании Samsung

Softswitch компании **Sonus** под названием **Insignus Softswitch** (рис. 10.15) имеет аппаратно-распределенную архитектуру, причем все его модули взаимодействуют через IP-сеть.

Основанный на принципе открытых интерфейсов, Insignus Softswitch позволяет строить сеть с использованием оборудования сторонних производителей. Состав Softswitch: PSX Policy Server – главный модуль Insignus Softswitch, играющий интегрирующую роль для всех решений Sonus; SGX OKC7 Gateway и GSX-GC Gateway Controller – обеспечивают функции сигнализации и управления процессом обслуживания вызова для медиа-шлюза; TSX Gateway Controller – поддерживает функции сигнализации и контроля обслуживания вызовов для транспортных шлюзов, используя стандартные протоколы, такие как MGCP, ASX Access Server – для контроля абонентской линии и поддержки различных функций обслуживания вызовов.

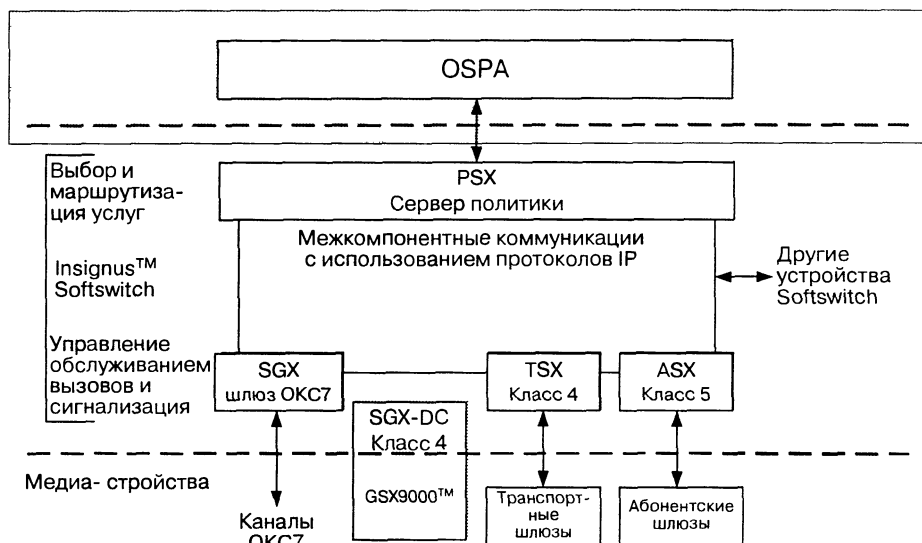


Рис. 10.15. Insignus Softswitch компании Sonus

Поддержка открытых протоколов позволяет PSX выступать в роли привратника H.323, взаимодействовать с серверами приложений по SIP, и по SIP-T взаимодействовать с Softswitch сторонних производителей, а также поддерживать разные планы нумерации и алгоритмы маршрутизации.

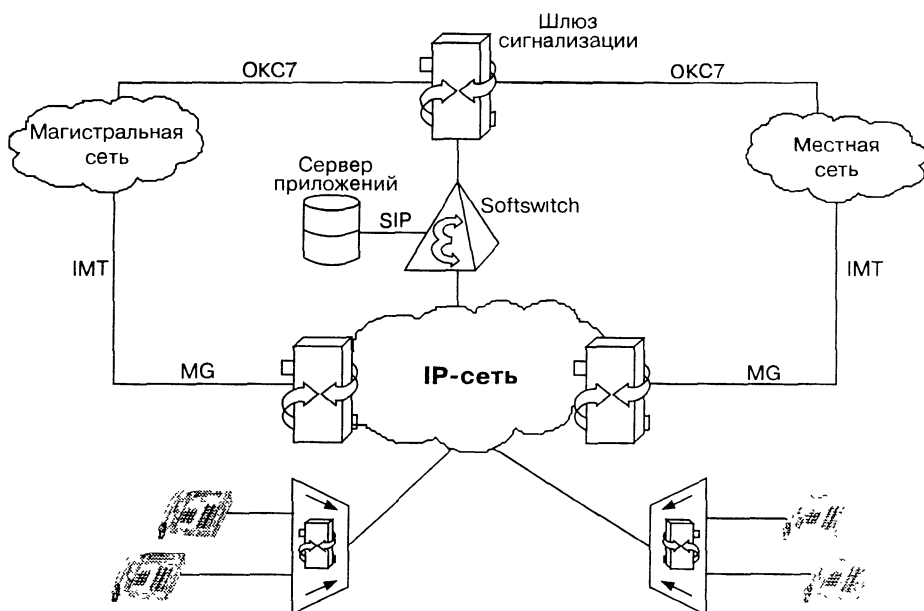


Рис. 10.16. Softswitch GenuOne компании Tekelec

Американская компания **Tekelec** назвала свой Softswitch **GenuOne**, и определяет его как платформу пакетной телефонии, поддерживающую управление процессом обслуживания вызова, приложения, функции сигнализации и управления в сетях TDM, IP и ATM. Все эти функции могут быть интегрированы в одном сетевом устройстве или иметь распределенную архитектуру. На базе Tekelec Softswitch обеспечивается предоставление как традиционных телекоммуникационных услуг, так и услуг Интеллектуальной сети.

Компания **Veraz Networks** возникла в результате слияния компаний NexVerse и ECI. Ее Softswitch носит название **NexVerse ControlSwitch**, т.к. создавался до слияния, и имеет распределенную архитектуру. Система имеет открытые, основанные на H.323, SIP, JAIN и XML интерфейсы с Web-ориентированными инструментальными средствами разработки, и изначально предполагала работу с сетевым оборудованием сторонних производителей. Благодаря модульности построения, оборудование хорошо масштабируется, его производительность достигает в 1 млн. вызовов в ЧНН. ControlSwitch работает на платформе SUN Netra под ОС Solaris 2.6 или Solaris 2.8, но может работать и на других SUN платформах.

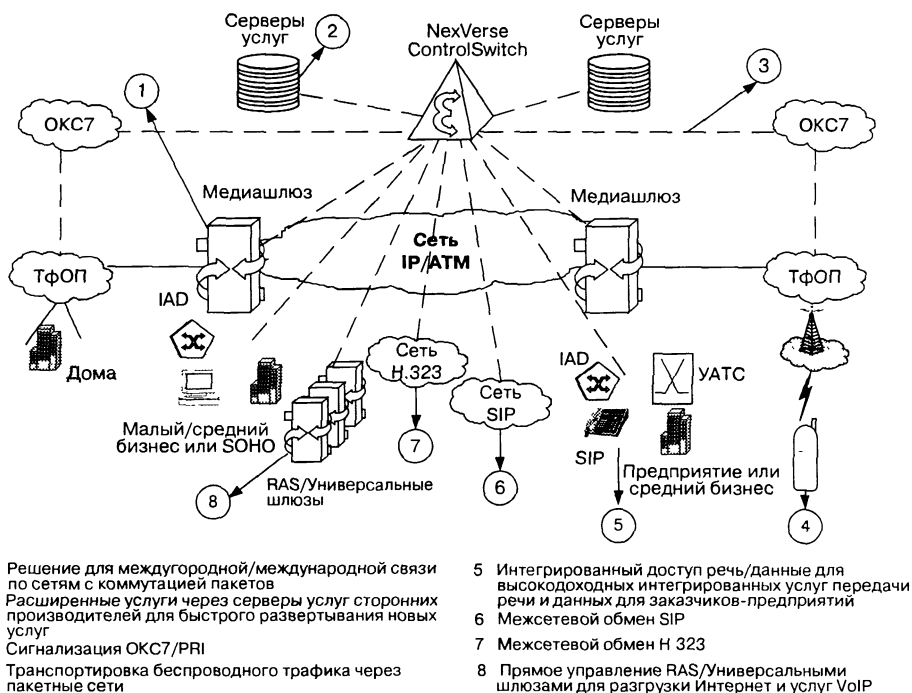


Рис. 10.17. Softswitch NexVerse ControlSwitch компании Veraz Networks

Clarent Distributed Softswitch Network Architecture (распределенную сетевую *Softswitch*-архитектуру *Clarent*) заявляет на рынке оборудования для будущих NGN компания Clarent. В этой архитектуре *Softswitch* каждый функциональный блок выделен в специализированный сервер с целью обеспечить объемную и функциональную масштабируемость системы.

В *Softswitch* Clarent входят Clarent Command Center, Clarent Class 4-5 Call Manager, Clarent Signaling Solutions, Clarent Announcement Server и система эксплуатационного управления. На основе этих компонентов Clarent построен ряд готовых решений для ТФОП (Clarent PSTN Access Softswitch Solution), для сетей Frame Relay, ATM и IP.

Clarent Call обеспечивает управление обслуживанием вызовов, исходящих от или входящих в PSTN (CAS, OKC7, PRI), поддерживает безобрывность соединений при переключениях и техническом обслуживании, взаимодействует по протоколу MGCP с Clarent Command Center для запроса и выполнения интеллектуальной маршрутизации вызовов и с медиашлюзами Clarent или сторонних производителей.

Для класса 5 поддерживаются протоколы TCP/IP, UDP, ARP, TFTP, ICMP, а также протоколы MGCP и SIP (в том числе SIP-T). Clarent Signaling Solutions обеспечивает взаимодействие между ТФОП и IP-сетями. Система эксплуатационного управления сетевыми элементами Clarent (CEMS) управляет всеми элементами архитектуры *Softswitch* с одного центрального сервера, поддерживая интерфейсы SNMP, XML, JDBC.

Clarent Class 4 Call Manager (C4CM) используется в решении PSTN Access Softswitch, являющемся альтернативой обычному коммутатору 4 класса. Clarent Class 5 Call Manager (C5CM), функционально близок к C4CM, но обеспечивает большую производительность и поддержку большего количества протоколов и услуг. Возможно гибкое наращивание производительности C4CM до 2.5 млн. ВНКА на одну кассету.

Американская компания **Marconi** представлена на рынке *Softswitch* разработкой **SoftSwitch XCD5000**. XCD5000 имеет аппаратно-распределенную архитектуру, которая включает в себя, кроме функций Call Agent, все управляющие функции, такие как аутентификация пользователей, маршрутизация вызовов, генерация CDR, преобразование IP адресов, функции поддержки дополнительных услуг для телефонии и ряд других сетевых компонентов, обеспечивающих функциональные возможности, которые необходимы современному *Softswitch*-решению. *SoftSwitch XCD5000* является модульным устройством, позволяющим плавно наращивать емкость и производительность системы, работает на стандартной

UNIX-платформе и сочетает в себе компактность и низкое энергопотребление с производительностью до 1 млн. ВНСА.

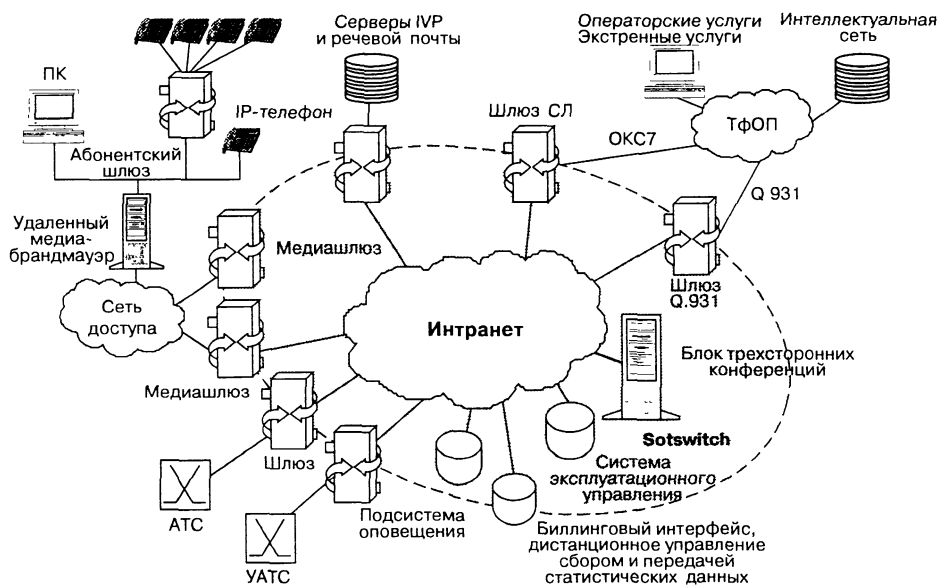


Рис. 10.18. Softswitch XCD5000 компании Marconi

В реализации Marconi используются принципы декомпозиции шлюзов: медиашлюзы служат для соединения Softswitch с традиционными TDM-сетями, преобразуя речь и данные в пакеты и наоборот, а сигнальные шлюзы служат для переноса сигнальных сообщений ОКС7 и Q.931 от ТФОП к Softswitch и наоборот.

Элементами системы являются также: Media Firewalls, – служат для обеспечения безопасности, позволяя проходить через сеть только авторизованному трафику, ведут мониторинг пакетного трафика в реальном времени и отбрасывают пакеты, нарушающие разрешенную данному пользователю полосу пропускания; Announcement Subsystem – хранит записанные речевые объявления и акустические сигналы и передает их конечным пользователям в виде пакетов по команде Softswitch; ISDN and DPNSS (Digital Private Network Signalling System) Gateways – обеспечивают взаимодействие Softswitch с существующими PBX (Q.931 и DPNSS); Three Party Bridge – обеспечивает функции трехсторонней конференции; Management – ведет эксплуатационное управление сетью и элементами Softswitch, имеет распределенную архитектуру и модульное ПО, что обеспечивает масштабируемость и гибкость, поддерживает интерфейсы с внешними управляющими и биллинговыми системами. На базе Marconi Softswitch можно создавать разнообразные решения. Например, Class 5 Solution обеспечивает функции узкополосного местного узла коммутации, поддерживает

обслуживание вызовов и предоставление услуг, таких как Centrex, доступ к Интеллектуальной сети, переадресация вызовов, трехсторонняя конференция, а Class 4 Solution обеспечивает функции транзитного узла, поддерживая обслуживание вызовов и соединения с традиционной ТФОП (последнее – только для взаимодействия с Интеллектуальной сетью).

Softswitch компании **Telcordia** называется просто Call Agent или Service Manager, а в состав Softswitch-решения входят: Accounting Gateway – участвует в ведении биллинга, получая от шлюзов, привратников и серверов биллинговую информацию и сведения об использовании ресурсов; AG – преобразует полученные данные в CDR; Announcement Server – получает от Call Agent указания передавать IP-шлюзам речевые объявления и тональные сигналы (рис. 10.19).

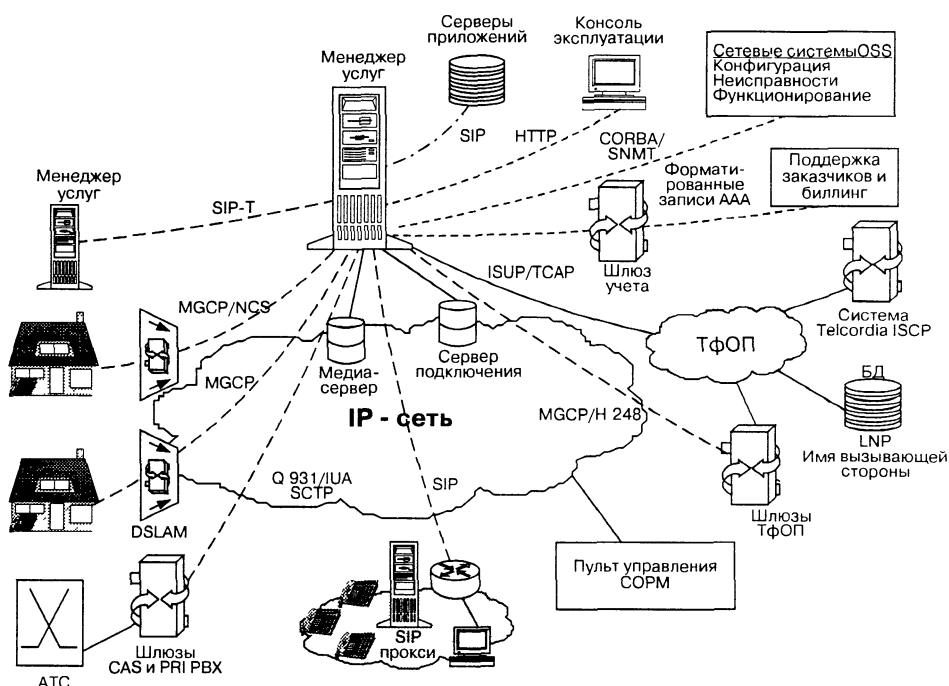


Рис. 10.19. Softswitch компании Telcordia

Для взаимодействия с другими сетевыми устройствами Softswitch поддерживает обычный набор протоколов: SIP – для работы с сетями IP-телефонии на базе SIP и для взаимодействия с серверами приложений, SIP-T – для взаимодействия с другими Softswitch, MGCP и H.248(Megaco) – для работы с медиашлюзами и мультисервисными концентраторами доступа, CORBA и SNMP – для взаимодействия с OSS (Operation Support System) или TMN, OKC7 (ISUP, TCAP), Q.931

(DSS) – для работы с ТфОП и связи с УАТС, а также протоколы многочастотной сигнализации и сигнализации ВСК.

Softswitch компании Telecordia тоже можно адаптировать к выполнению функций коммутаторов 5 и 4 классов. Параметры Softswitch Class 5: ВНКА – 720000, максимальное количество абонентских линий – 500000, максимальное количество межстанционных линий – 150000, количество одновременно обслуживаемых вызовов – до 150000.

Параметры Softswitch Class 4: ВНКА – 1500000, до 100000 линий прямого доступа (DAL – Direct Access Line), до 300000 межстанционных линий, до 150000 одновременно обслуживаемых вызовов.

Компания **HSS (Hughes Software Systems)**, основанная в 1991 году в Индии одним из подразделений Hughes Electronics Corporation (США), занимается разработками в области ИТ. На мировом рынке HSS предлагает свой **Softswitch HSS**, способный заменить коммутаторы классов 4 и 5 и представленный на рис. 10.20.

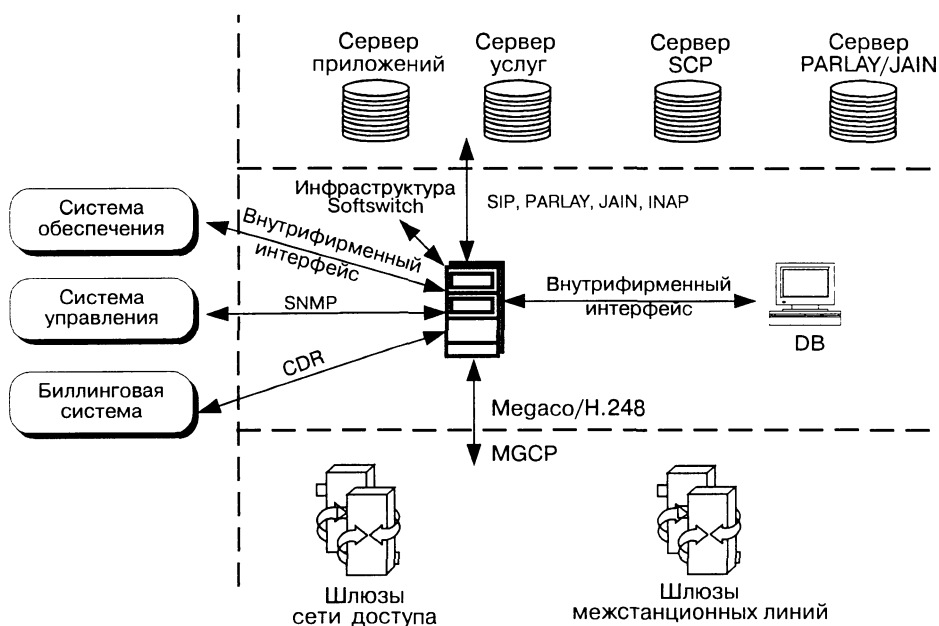


Рис. 10.20. Softswitch HSS компании Hughes Software Systems

Softswitch HSS имеет распределенную архитектуру, предоставляющую возможность внедрения как стандартных, так и новых функций и услуг. Разработчики HSS обращают внимание на то, что управление обслуживанием вызова в их Softswitch не зависит от управления услугами, что упрощает внедрение востребованных рынком услуг. Построение Softswitch HSS согласуется с архитектурой, предложенной TIPHON. Система поддерживает протоколы

сигнализации OKC7, системы сигнализации R1 и R2, Q.931 DSS1. Возможно внедрение V5.2. Управление медиашлюзами производится по протоколам Megaco/H.248 и MGCP. Система поддерживает предоставление услуг IN CS2, а архитектура системы не зависит от сигнализации, но, кроме вышеперечисленных систем сигнализации, реализована поддержка SIP, H.323 и сигнализации POTS.

Компания **Iskratel** ранее предлагала Softswitch-решения на базе линейки продуктов Siemens SURPASS, ..дополняя ее собственными мультисервисными абонентскими концентраторами и шлюзами. Сейчас в Iskratel разработано семейство оборудования **SI2000 NG**. При разработке и создании SI2000 NG усилия концентрировались на прозрачной интеграции с существующим оборудованием ТФОП и с существующими системами эксплуатационной поддержки (OSS).

В состав SI2000 NG входят: медиашлюз SI2000 MGW; шлюз VoIP SI2000 VGW; сервер обработки вызовов SI2000 CS, который взаимодействует с серверами приложений (по протоколам MGCP, MeGaCo, CSTA, LDAP и SIP), с медиашлюзами (протоколы MGCP, MEGACO/H.248), с другими серверами обработки вызовов (протоколы SIP-T, H.323, BICC) и со шлюзами сигнализации (протоколы SigTran, SCTP, M3UA и IUA); медиа-сервер SI2000 MS, который обеспечивает на базе VoiceXML речевые услуги для конечных пользователей сетей TDM или IP и может работать как автономное устройство или как устройство, управляемое Softswitch; видеосервер SI2000 Pilot Box, производящий оцифровку исходного аналогового видеосигнала и передачу цифрового видео по IP-сети; мультисервисный узел доступа SI2000 MSAN, производящий преобразование информации между сетями с коммутацией каналов и пакетов, а также обеспечивающий взаимодействие сигнализации между линиями ТФОП или ISDN (BRI, PRI) и сетевым интерфейсом H.323 или MGCP-Sigtran. Производительность SI2000 CS составляет до 2 млн. вызовов в ЧНН.

Компания **sentitO Networks** имеет линейку продуктов для организации транспортной сети и предоставления услуг VoIP под названием **Open Network Xchange (ONX)**. Этот ряд состоит из трех компонентов: *IVG, Intelligent Voice Gateway*, – медиа-шлюз VoIP, в котором, к тому же, реализованы логика и механизмы управления соединением; *Proxy7 Signaling Gateway* совмещает в себе функции SIP-проxy с шлюзом OKC7 и выполняет задачи переадресации, регистрации и аутентификации; *PreVision Network Manager* ведет в сети работу с ошибками и со счетами пользователей, управляет конфигурацией, производительностью и безопасностью. Будучи разработан в соответствии с концепцией TMN, PreVision Network Manager позволяет управлять отдельными компонентами ONX и обеспечивает возможность плавной интеграции с существующей системой OSS.

Компания **Telica** приобретена Lucent Technologies в августе 2004 года. Ее приобретение было призвано укрепить портфель решений Lucent Accelerate для сетей VoIP. До этого Telica предлагала Softswitch-решение **Plexus Unified Service (PLUS) Softswitch**. Оно было основано на платформе Plexus 9000 Platform и состояло из PLUS Signaling Gateway, PLUS Media Gateway Controller, Plexus 9000 Media Gateway, PLUS Compact Controller, PLUS Compact Softswitch и Telica's PlexView® EMS. Первые три компонента (SG, MGC, MG) представляют собой уже знакомое Softswitch-решение. PLUS Compact Controller, совмещающий в себе функции шлюза сигнализации и контроллера медиашлюзов, может использоваться в простых случаях для облегчения установки и настройки. PLUS Compact Softswitch – полное Softswitch-решение в едином конструктиве, обеспечивающее поддержку до 80000 портов.

Китайская компания **ZTE** имеет собственное Softswitch-решение, базирующееся на модели Softswitch **ZXSS10 SS1** (рис. 10.21).

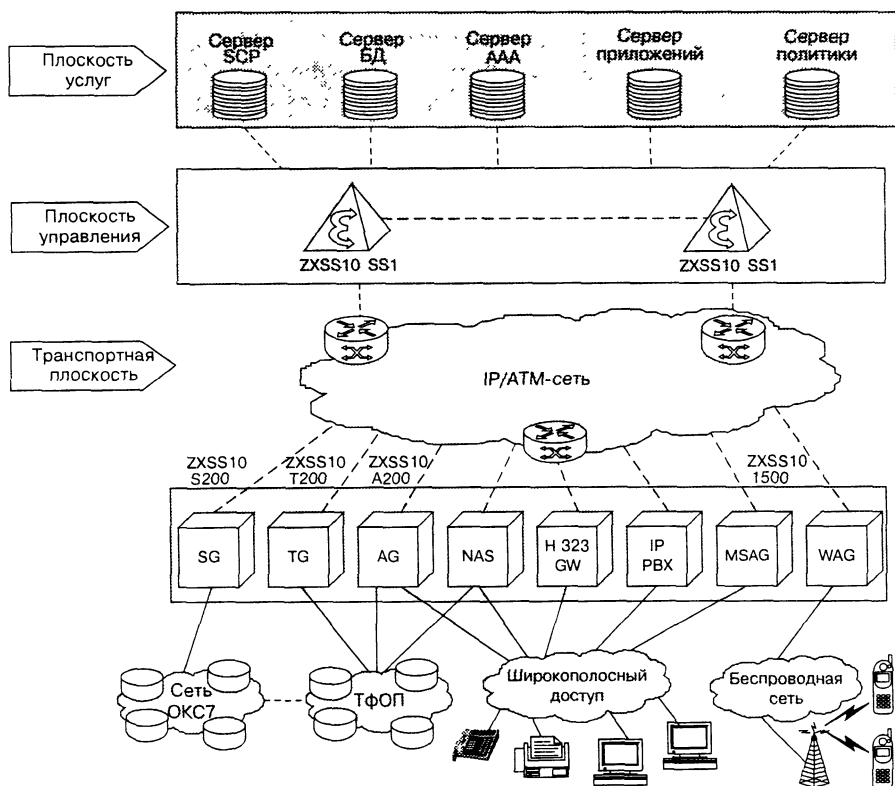


Рис. 10.21. Softswitch ZXSS10 SS1 компании ZTE

В состав NGN-оборудования компании входят также шлюз сигнализации (ZXSS10 S100), транспортный шлюз (ZXSS10 T200, M100), шлюз доступа (ZXSS10 A200), IAD (ZXSS10 1500, 1600),

сервер приложений (ZXSS10 APP), медиасервер (ZXSS10 MeS) и др. Система ZTE Softswitch обеспечивает реализацию интегрированных сетевых услуг, объединяющих в себе функции передачи речи, данных и видео. Она поддерживает традиционные протоколы коммутации и обеспечивает взаимодействие между сетями различных типов посредством преобразования протоколов. В общем случае, имеются следующие прикладные типы конфигурации системы ZTE Softswitch: предоставление услуг местной связи в IP MAN; предоставление услуг междугородной связи в базовой сети передачи данных; возможность взаимодействия сетей и услуг с существующими ТфОП; предоставление решений для 3G. Система позволяет предоставлять базовые услуги связи, услуги Интеллектуальной сети, услуги с добавленной стоимостью и мультимедийные услуги. В центре всех NGN-решений компании ZTE находится ZXSS10 SS1. Он поддерживает до 200000 каналов, до 2 млн. абонентов, максимальная нагрузка – 2 млн. вызовов в ЧНН.

Французская компания **Cirpack** в конце 2004 года, согласно обзору, подготовленному Dittberner Associates inc., была признана вторым по величине (после Italtel) поставщиком VoIP решений в EMEA (Европа, Средний Восток, Африка).

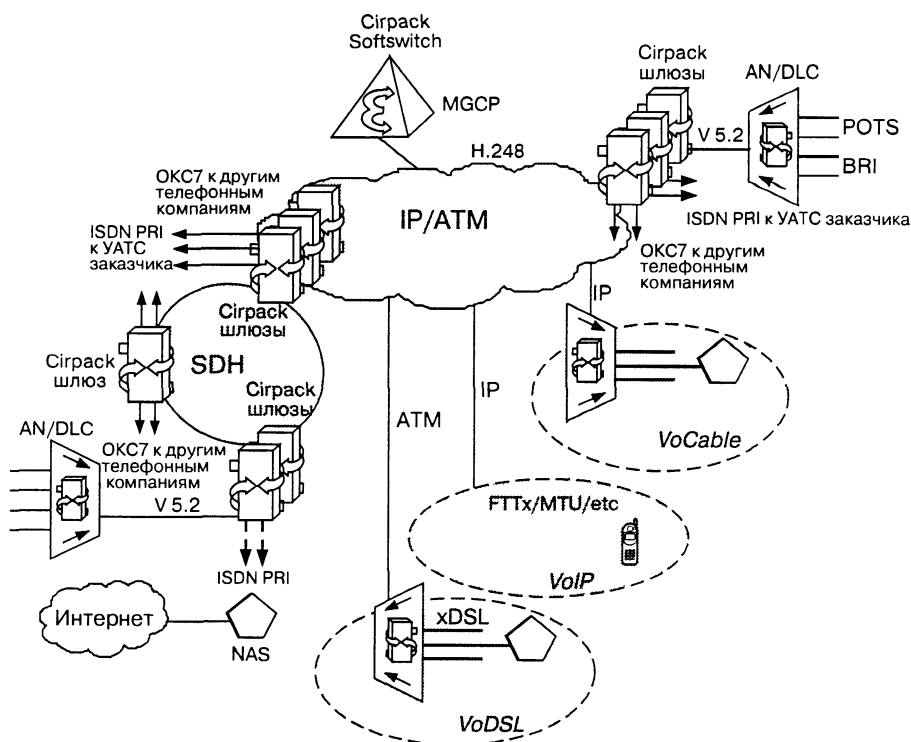


Рис. 10.22. Softswitch Cirpack HVS компании Cirpack

Cirpack предлагает ряд решений для коммутаторов класса 4 и класса 5, различающихся производительностью. Так, Softswitch компании под названием Cirpack High Velocity Softswitch, или Cirpack HVS, может либо быть самостоятельным решением, либо входить в виде одного из модулей в крупный мультисервисный NGN-коммутатор. Все решения базируются на универсальной телефонной платформе и на серверах IBM. Платформа может становиться Softswitch 5/4 класса, медиа-шлюзом и сигнальным шлюзом, интегрированным Softswitch решением. Система может обрабатывать до 5 млн. вызовов в ЧНН, может устанавливать 1390 соединений в секунду и поддерживать до 90000 соединений одновременно, а также позволяет обслуживать до 264000 абонентов.

Компания **CedarPoint Communications** – занимается разработкой оборудования для кабельного телевидения. Их телекоммуникационная система класса Softswitch, в первую очередь, ориентирована на предоставление мультимедийных услуг Операторами кабельного телевидения.

Softswitch Cedar имеет название **Safari C³** и является единственным коммерческим предложением операторского класса в своем сегменте рынка. Safari C³ – решение класса 5 с емкостью системы, наращиваемой от 5 до миллиона абонентов.

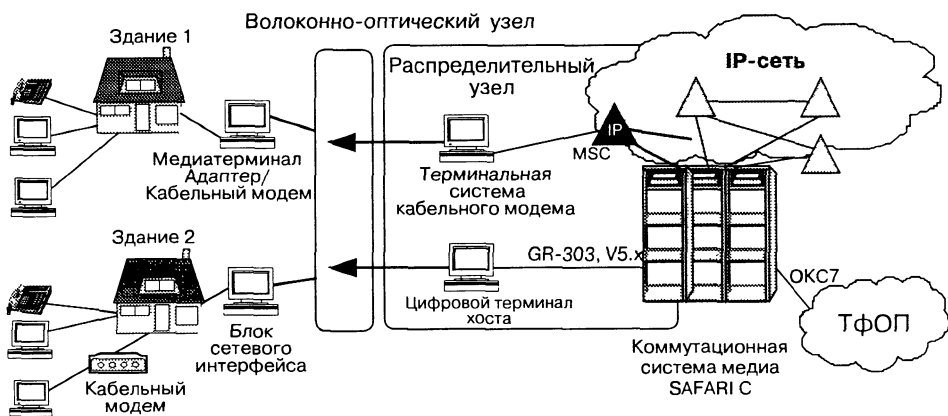


Рис. 10.23. Softswitch SAFARI C³ компании CEDAR

Американская компания **Nuera Communications** имеет линейку VoIP продукции под названием **ORCA (Open Reliable Communications Architecture)**, в состав которой входят IP-шлюзы, система управления и оборудование Softswitch (рис. 10.24). Softswitch компании Nuera имеет название ORCA SSC и базируется на серверной платформе Hewlett Packard 9000, поддерживающей HP Open Core. SSC поддерживает полностью дублированные «зеркальные» базы данных с непрерывным обновлением.

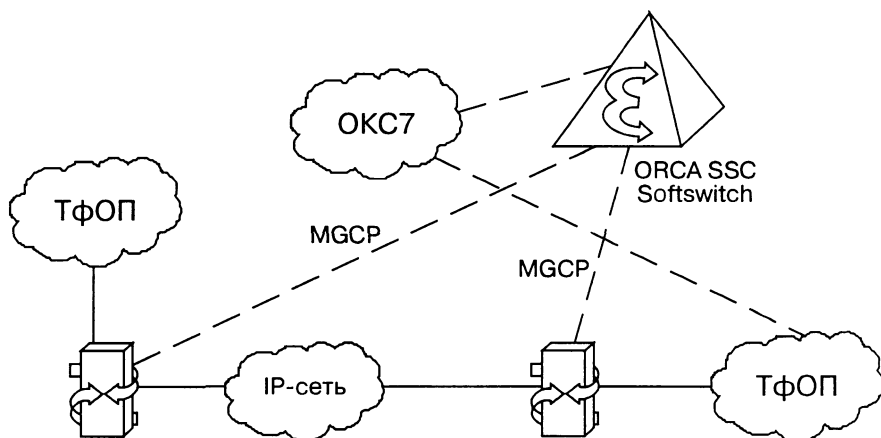


Рис. 10.24. Softswitch ORCA компании Nuera Communications

ORCA SSC использует до 64 звеньев системы OKS7, реализованной согласно рекомендациям ITU и ANSI. (возможны интерфейсы V.35, T1 и E1). Поддерживается также сигнализация ISDN (Euro, N12) и CAS-сигнализация: R2, DTMF, China R1. Из протоколов IP-сетей реализованы MGCP и NCS (протокол для реализации VoIP в сетях кабельного телевидения), а также SIP. На текущий момент система может обслуживать до 4000 соединений одновременно и обрабатывать до 100 тысяч вызовов в ЧНН, но в следующей версии оборудования планируется одновременное обслуживание до 12000 соединений и более 330 тысяч вызовов в ЧНН. SSC поддерживает более 100 шлюзов.

Walkersun – тайваньская компания, основанная в 1999 году. С 2001 года занимается разработками VoIP-решений разного уровня для корпоративного и операторского рынка. Компания имеет линейку VoIP продуктов, в которую входят биллинговые и CDR серверы, серверы приложений и Softswitch 4/5 класса, имеющий название **Walkersun Communication Server (WCS) Softswitch**. WCS выпускается в нескольких модификациях, различающихся производительностью: WCS 6000, WCS 3000, WCS 2000. На базе своего оборудования Walkersun предлагает ряд готовых VoIP-решений, ориентированных на разные сегменты рынка, включая использование карт предоплаты и междугородную/международную связь. Производительность системы – до 1 млн. вызовов в ЧНН и возможность одновременной поддержки более 20000 соединений.

10.3. Отечественные платформы Softswitch

По своему объему этот параграф значительно уступает предыдущему. По крайней мере, это следует из Инфобанка СОТСБИ (Сертифицированное Оборудование Телефонных Сетей – Базы Информации), который содержит несколько сертификатов на отечественные Softswitch среди которых уже упоминавшийся и включающий функции СОРМ сертификат отечественной Softswitch-платформы Протей с весьма скромным названием – мультисервисный коммутатор доступа (МКД). Этим названием определяется и область применения МКД – гибкий коммутатор для местных сетей связи или, согласно распространенной международной классификации, Softswitch класса 5. Этот Softswitch имеет сертификат Мининформсвязи ОС/1-СПД-787 и является оборудованием операторского класса с показателем надежности 99,999%, который обеспечивается внутрифирменной системой эксплуатационного управления на базе SNMP.

На рис. 10.25 представлены основные интерфейсы МКД.

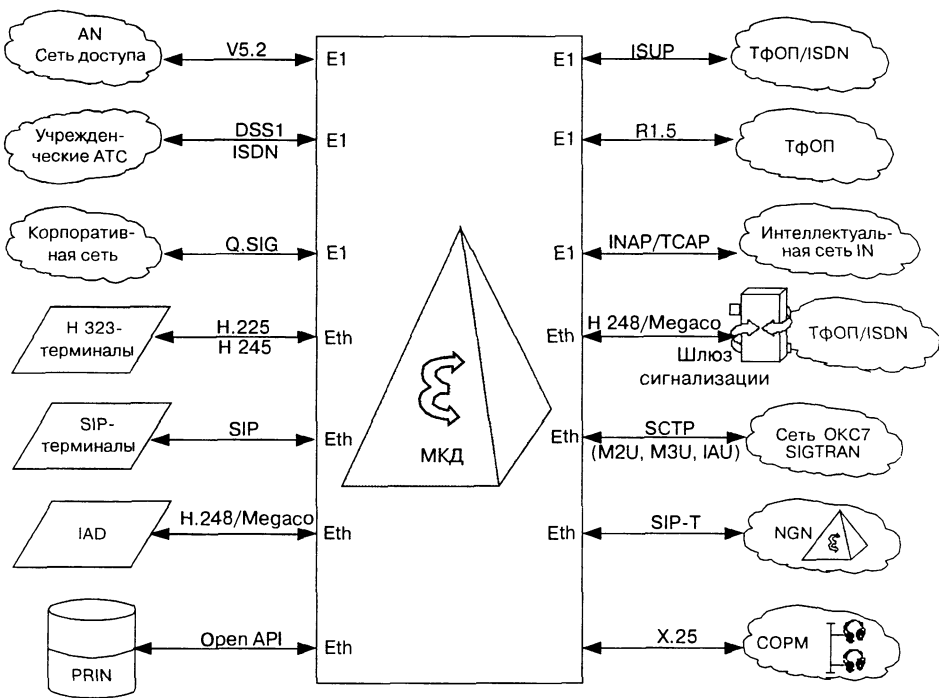


Рис. 10.25. Softswitch МКД компании ПРОТЕЙ

Этот Softswitch, включающий в свой состав сигнальные шлюзы, строится на специализированном сервере под операционной системой Linux и поддерживает стек протоколов ОКС7, включая МТР1-3,

ISUP, SCCP, TCAP, протокол INAP для непосредственного взаимодействия с узлом управления услугами SCP, апробированный недавно в г. Чайковский во взаимодействии с пермским SCP, который разработала компания Alcatel, а также протокол DSS1 первичного доступа PRI ISDN по Q.931 и редко встречающиеся в Softswitch протоколы интерфейса V5.2. Вторая группа протоколов МКД включает в себя SIP по RFC 2543, MGCP/Megaco/H.248, а также наиболее распространенный сегодня в ЕСЭ России H.323 для взаимодействия шлюзами и конечными пользователями сети H.323.

С другими Softswitch, рассматриваемыми в этой главе, МКД взаимодействует двумя способами: по протоколу SIP-T (глава 4) или по BICC (глава 8). Предусматривается также поддержка рассмотренных в главе 7 протоколов OKC7 и V5.x поверх по IP по спецификациям Sigtran (протоколы SCTP, M3UA, M2PA, IUA, SUA/SCTP, V5UA), а также IP/MPLS [3]. МКД выполняет аутентификацию и авторизацию и имеет встроенную поддержку протокола RADIUS. Он организует также разные режимы маршрутизации, включая, разумеется, и маршрутизацию по полному номеру E.164, выбор одного из нескольких маршрутов по критерию стоимости и/или надежности (в случае отказа основного маршрута), специальную маршрутизацию для контакт-центров и спецслужб [9], маршрутизацию Интеллектуальной сети [7] и др. Важным отличием этого Softswitch является полная (и, на момент написания книги, – единственная сертифицированная) реализация функций CPM, о чем уже подробно говорилось в предыдущей главе.

В полном соответствии со своим названием, МКД рассчитан на применение в максимальной близости к сети доступа и ориентирован на последующий переход к NGN. Именно от сети доступа (точнее, от оборудования мультисервисного абонентского доступа МАК, упоминавшегося в главе 9) и отталкивалась эта первая отечественная разработка Softswitch. Именно в таком режиме проводились сертификационные испытания, а при разработке основной упор делался на гибкое масштабирование МКД в диапазоне от 25 тыс. до 2.5 млн. вызовов в ЧНН.

Другой продукт в этой области – **RealEast Softswitch RSF1000** – имеет распределенную структуру и может быть размещен на нескольких серверах (рис. 10.26).

Внутренние связи компонентов RealEast Softswitch RSF1000 реализуются с использованием технологии CORBA поверх SSL. Модульная структура позволяет клиенту строить систему с теми модулями, которые ему необходимы. Модуль *SIP Proxy RSP100* обеспечивает функции аутентификации, регистрации, маршрутизации, биллинга для шлюзов и оконечных устройств SIP. Модуль *H.323 Gatekeeper RGK100* обеспечивает те же функции что и SIP Proxy RSP100, но для устройств H.323.

Модуль *RTP Proxy RRX100* допускает как программное, так и аппаратное (с использованием оборудования компьютерной телефонии) обеспечение прохода через него RTP-трафика. Для подсоединения RSF1000 к разного вида сетям пакетной коммутации и коммутации каналов необходимы соответствующие шлюзы SIP, H.323, ISUP и ISDN, разработка которых проводится в настоящее время. Компанией заявлены следующие интерфейсы с ТфОП: программно переключаемые тракты E1/T1, протоколы MFC-R2, R1,5 и 11 вариантов OKC7 и ISDN PRI.

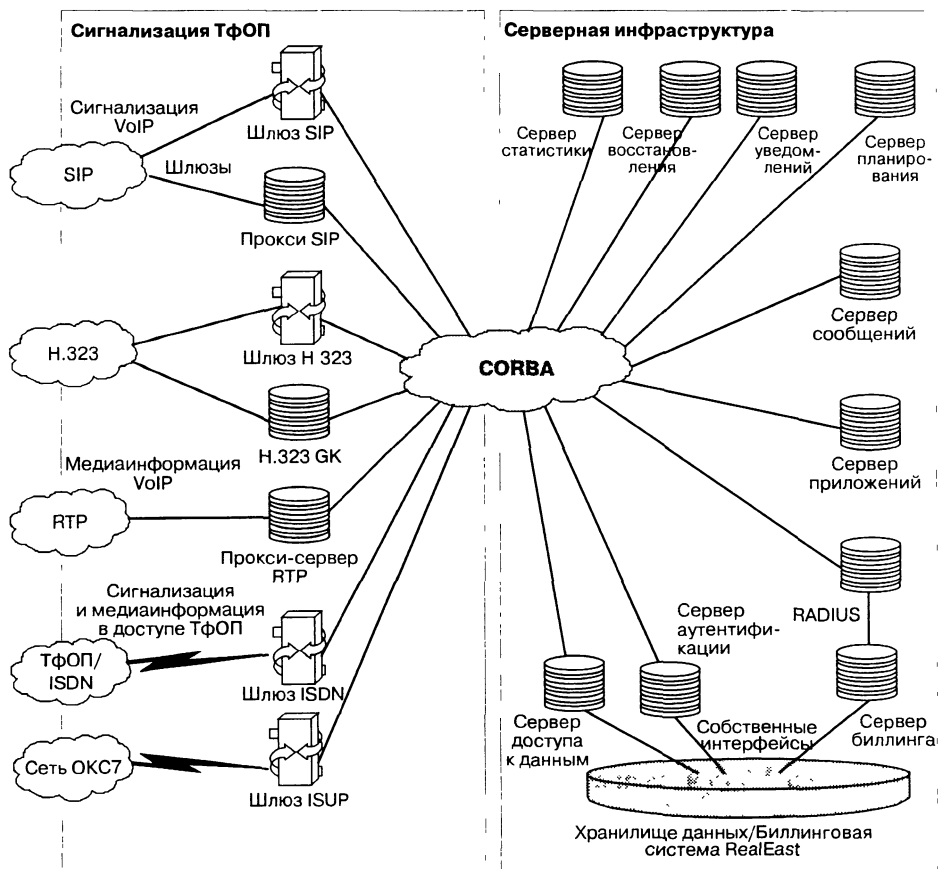


Рис. 10.26. RealEast Softswitch RSF1000 компании Real East

CDR сервер предназначен для записи и хранения *CDR* в системе. Сервер получает от других модулей информацию о начале и конце сеанса и запрашивает Billing Server по протоколу RADIUS, что позволяет использовать с RealEast Softswitch любую RADIUS-совместимую систему биллинга. Биллинговый сервер обеспечивает биллинг и блокировку в режиме реального времени, при превышении определенной суммы долга вызывает RBS1000 для предоставления

информации о текущем сеансе, чтобы проверить баланс клиента и передать эту информацию на Softswitch.

Компания **Mera** также получила сертификат Мининформсвязи ОС/1-СПД-606 своей версии Softswitch, называющейся **MERA VoIP Transit Softswitch (MVTS)** и имеющей функциональные возможности коммутатора класса 4. MVTS – это аппаратно-программный комплекс операторского класса, обеспечивающий управление телефонной сигнализацией и речевыми потоками в сетях связи (рис. 10.27).

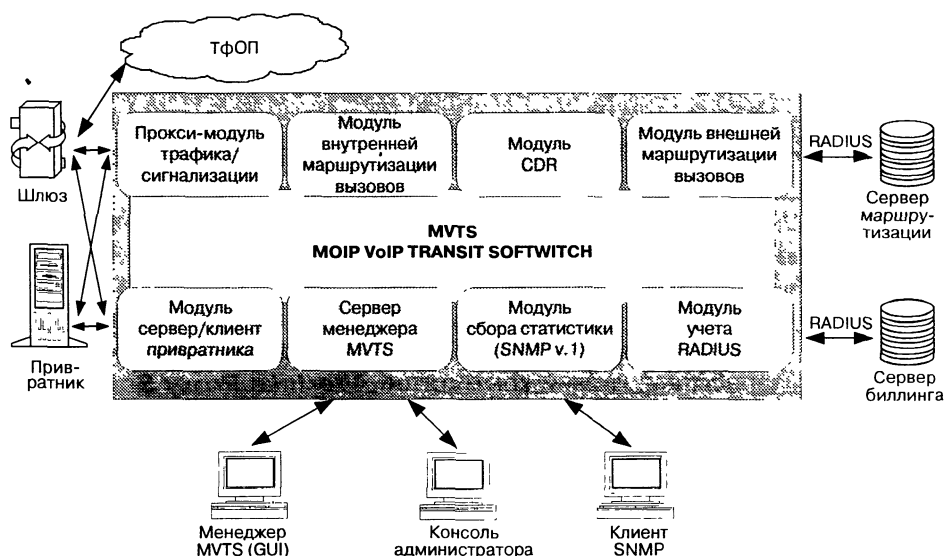


Рис. 10.27. Mera VoIP Transit Softswitch компании Mera

MVTS выполнен в нескольких вариантах, различающихся производительностью – от MVTS 30 до MVTS 1500, т.е. от 30 до 1500 одновременно обслуживаемых вызовов. Стандартный комплект поставки включает в себя функции: H.323-привратника, обработки сигнального (H.323) и мультимедийного (RTP) трафика, внутренней маршрутизации, внешней динамической маршрутизации (по RADIUS-протоколу), сбора статистических данных, системы начисления и учета платы в CDR-формате и через RADIUS. Дополнительно поставляются графический интерфейс MVTS Manager и SIP/H.323-конвертер. Одной из функциональных особенностей MVTS является конверсия H.323-диалектов, т.е. сопряжение оборудования разных производителей, в том числе Cisco, VocalTec, Clarent и др.

Другой Softswitch, разработанный компанией MERA Networks, но еще не имеющий сертификата, – **MERA VoIP Centrex Softswitch (MVCS)** – обеспечивает функции коммутатора классов 4/5 классов и совмещает функциональные возможности классической YATC с возможностями NGN.

Украинская телекоммуникационная компания **IntereXchange Carrier** разработала **IXC Softswitch**, получивший сертификат Мининформсвязи № ОС/1-СПД-777 до июля 2007 года в качестве Softswitch класса 4. Функциональные возможности этого оборудования включают в себя:

- поддержку H.323-диалектов (сопряжение оборудования разных производителей);
- поддержку SIP;
- обработку сигнального трафика (H.225, H.245);
- статическую маршрутизацию на основании: стоимости минуты разговора, времени поступления вызова, номера вызываемого абонента, идентификатора группы, которой принадлежит вызывающий абонент, доступности шлюза места назначения, приоритета каждого направления в прайс-листе оператора, приоритета шлюза места назначения;
- авторизацию вызовов на основании данных системы бухгалтерии о состоянии счета клиента, доступности полосы пропускания, доступности шлюза, соответствия медиа-кодексов и др.

Организованная на базе структурного подразделения IP-телефонии компании «Агат-РТ» в 2003 году компания ООО «Альтер-текс» разработала гибкий коммутатор **Alterteks Proxy SoftSwitch (AlterPSS)**, который позволяет направлять сигналы и речевой трафик с одного шлюза IP-телефонии на другой, или пропускать данные через себя. К функциям AlterPSS относятся: совмещение в одной сети оборудования с протоколами H.323, SIP v.2; сглаживание различий в реализации сигнализации H.323 в оборудовании разных производителей; выполнение функций прокси-сервера при работе шлюзов в разных сетях (например, когда требуется позвонить из локальной сети через Интернет общего пользования); прием и пересылка речевых пакетов для передачи их по каналу с лучшими характеристиками; авторизация шлюзов по IP-адресам; авторизация пользователей по паролю (согласно H.235 или MD5 Digest Authorization); пересылка согласно плану маршрутизации, который может быть задан индивидуально для каждого пользователя или шлюза; обход неисправных маршрутов; предоставление клиенту информации о счете и другой справочной информации.

10.4. Тестирование Softswitch

Многообразие рассмотренных в этой главе реализаций Softswitch, как и сложность всего представленного в книге материала, выдвигает проблему тестирования Softswitch и оценки времени полного тестирования Softswitch. В реальном Softswitch вполне могут использоваться все рассмотренные в книге протоколы, определенным образом взаимодействующие друг с другом,

а для обеспечения качества обслуживания трафика могут использоваться разные дополнительные средства типа многопротокольной коммутации по меткам MPLS [3], что исключает возможность получить простые ответы на поставленные выше вопросы. В настоящий момент не существуют универсальных, пригодных для всех случаев автоматических наборов тестов для проверки взаимодействия разных протокольных реализаций, поскольку во многих случаях причиной отказов и нарушения нормальной работы Softswitch является не функционирование какого-то одного протокола, а именно взаимодействие разнотипных протоколов. Другими словами, поддерживаемые протоколы сигнализации могут по отдельности работать хорошо, а при их объединении и преобразовании в Softswitch могут возникать ошибки. Проблему усугубляет географическая разобщенность сетевых элементов, которая может стать решающим фактором, препятствующим оперативному устранению ошибок. Линейные испытания (*beta test*) – это метод, очень популярный в разных опытных зонах Softswitch в составе ЕСЭ России, но он не дает гарантий исчерпывающего тестирования, т.к. при этом не проверяются все деревья принятия решений в программе и тестируются не все ветви и переходы.

Необходимость внешних протокол-тестеров Softswitch, варианты которых представлены на рис. 10.28, очевидна.

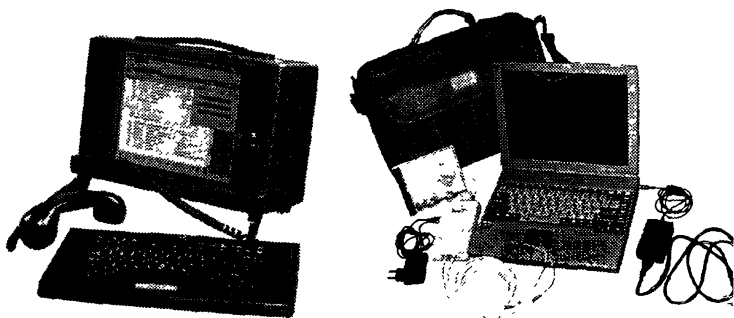


Рис. 10.28. Протокол-тестеры SNT-7531 и SNTlite

Именно с их помощью инженеры-разработчики проводят испытания отдельных модулей Softswitch, за которыми следуют постепенная интеграция системы и испытание ее в целом. Когда эта фаза успешно пройдена, выполняется пошаговое комплексное испытание в составе фрагмента сети NGN. Комплексные испытания должны выполняться по шагам, т.е. система строится и тестируется путем постепенного добавления в нее модулей. После этого проводится исчерпывающая опытная эксплуатация системы, позволяющая выявить скрытые до сих пор вещи, такие, например, как взаимозависимость функций и услуг.

10.5. Варианты реализации COPM

Сегодня на телекоммуникационном рынке имеется целый ряд решений COPM для Softswitch в рамках концепций ETSI и CALEA для сетей стационарной и мобильной связи, которые сведены в табл. 10.2.

Таблица 10.2. Производители программно-аппаратных средств COPM

Компания	Функции COPM			
	Доступ	Преобра- зование	Сбор данных	Анализ
Accuris				
Aceuris				
ADC (SS8)	X	X	X	—
Agsacom	X	X	X	—
Arpege	—	—	X	—
Bartec	—	—	X	—
Cetacean	—	—	X	—
Cisco	X	—	—	—
Codem	—	X	—	—
EDI	—	X	—	—
Ericsson	X	—	—	—
ETI	X	X	X	X
I2	—	—	—	X
JSI	X	X	X	—
Juniper	X	—	—	—
Lucent	X	—	—	—
Малвин	—	X	X	X
Marconi	—	—	X	—
Motorola	X	—	—	—
Narus	X	—	—	—
Nice	X	X	X	—
Nokia	X	—	—	—
Nortel	X	—	—	—
Orion	—	—	—	X
Pen-Link	—	—	X	X
Pine	X	X	X	—
Протей	X	X	X	—
Raytheon	—	—	X	—
Roke Manor	—	—	X	X
Septier	—	X	—	—
Siemens	X	X	X	X
Soghi	X	X	X	—
Spectronic	—	—	—	X
Syborg	—	—	—	X
SyTech	—	—	—	X
TopLayer	X	—	—	—
Utimaco	X	X	—	—
Verint	X	X	X	—

Предложенная в таблице классификация оборудования СОРМ предусматривает четыре области его применения: доступ к коммутационным узлам и станциям, преобразование информации СОРМ в интерфейсах НІ2 и НІ3, сбор данных СОРМ и выполняемый в ПУ (LEMF) анализ информации СОРМ.

Разделение систем по этим классам несколько условно и базируется, преимущественно, на информации самих компаний, поэтому для правильного восприятия данных таблицы 3 читателю рекомендуется принимать во внимание уже упоминавшиеся в этой главе коэффициенты из законов Мерфи.

В табл. 10.2 полезно отметить некоторые импортные системы, в частности разработку компании *ADC*, известную раньше как *SS8*, которая используется в сетях спутниковой связи и базируется на весьма оригинальном аппаратном обеспечении, систему израильской компании *Verint*, известную раньше как *Comverse Infosys* и эксплуатирующуюся, например, в сетях Израиля и Голландии, систему *Accuris* с концентрацией трафика, системы *Pine*, *Nice*, *Aqsacom*, *Digivox*, поддерживающие разные упоминавшиеся выше стандарты законного перехвата сообщений, включая европейский ETSI ES 201 671, американский CALEA и др.

Все эти системы разработаны как для стационарных, так и для мобильных сетей связи, контролируют все соединения с участием объекта наблюдения и передают результаты этого контроля одному или нескольким LEMF/LEA. Любопытна опубликованная оценка стоимости реализации СОРМ для вышеупомянутых импортных систем, колеблющаяся в диапазоне 100 000 до 700 000 Евро.

Отечественных систем СОРМ, функционирующих в составе Единой сети электросвязи России, всего две – это выделенные жирным шрифтом в таблице 10.2 продукты компаний Малвин и Протей. В этих системах в качестве основного для НІ3 поддерживается протокол X.25 для организации перехвата речи и данных в заранее маркированных соединениях.

Для системы Протей, в частности, характерны распределенная архитектура взаимодействия с удаленными модулями, управляемыми по защищенным IP-сетям, и возможность передачи данных об объектах наблюдения одновременно к нескольким пунктам управления LEMF/LEA, включая и уникальные переносные пункты управления. Обе системы имеют единое решение как для мобильных, так и для стационарных сетей.

10.6. Реализации пограничных контроллеров SBC

Точно так, как в начале эпохи Softswitch многие производители оборудования VoIP в погоне за модой называли гибкими коммутаторами Softswitch свои прокси-серверы с весьма ограниченными функциональными возможностями, хитом нового сезона мод стали рассмотренные в главе 9 пограничные контроллеры *SBC (Session Border Controller)*.

Уже упоминавшаяся в параграфе 10.2 компания IntereXchange Carrier пополнила свое предложение на рынке новым продуктом — IXC Session Border Controller. -

Это оборудование производит подключение региональных точек присутствия, выступая в роли концентратора трафика, т.е. собирая вместе трафик отдельных регионов и обеспечивая взаимодействие с центральным IXC Softswitch. К тому же, региональные IXC SBC выполняют функции маршрутизации и сбора статистики, а конфигурационные данные поступают с центрального узла.

В крупных сетях часть вызовов, которая может быть завершена на региональном узле, обрабатывается непосредственно в SBC. Это значительно снижает загрузку магистральных каналов речевыми потоками. Пограничные контроллеры SBC в этих случаях передают в центральный узел только информацию о поступивших вызовах и их характеристиках, сами выполняют основную обработку данных, но обеспечивают также удаленное начисление платы за услуги.

Последнее позволяет филиалам предприятия самостоятельно изменять ценовую политику, а центральный сервер принимает решение о маршрутизации вызова на основании цены, которую платит абонент регионального узла.

Глава 11

Подсистема мультимедийной связи IMS

*Прогнозы тем лишь интересны,
что вместо них текут сюрпризы,
ведь даже Богу неизвестны
Его грядущие капризы*

Игорь Губерман

11.1. Softswitch в сетях подвижной связи

Именно с позиций, отраженных в эпиграфе, рассматривается в этой главе дальнейшее развитие идеологии Softswitch, определяемое в значительной степени бурным прогрессом в сетях и технологиях подвижной связи. Успех архитектуры Softswitch в сетях стационарной связи побудил Операторов распространить на мобильные сети тот же подход, т.е. физически разделить функции управления обслуживанием вызова и функции установления и поддержания медиа-сеанса с узлом коммутации MSC. Необходимое для этого оборудование было успешно разработано и внедрено многими ведущими производителями, как уже имеющими Softswitch-решения для стационарных сетей, так и теми, кто занимался оборудованием только мобильной связи.

Как и Softswitch-решения, они имели довольно произвольную архитектуру. Многообразие вариантов наглядно показано на многочисленных рисунках предыдущей главы, но в условиях роуминга услуг, принятого в мобильной связи, оно сильно затрудняло взаимодействие Операторов, ограничивало возможности обслуживания пользователя за пределами домашней сети и имело целый

ряд других недостатков. Именно поэтому, параллельно с попытками внедрения Softswitch в мобильные сети, в международной организации *3GPP (Third Generation Partnership Project)* была развернута серьезная работа, направленная на создание концепции и на стандартизацию мобильных сетей третьего поколения 3G. В недрах этой организации родился проект перехода от GSM-сетей 2G к сетям 3G, основой которых станет *IMS (IP Multimedia Subsystem)* – сетевая архитектура, эффективно использующая принципы Softswitch и возможности протокола SIP. Она призвана утвердить Softswitch в мобильных сетях, устранив при этом основные проблемы, присущие первым мобильным Softswitch.

11.2. Стандартизация IMS

11.2.1. Роль 3GPP/3GPP2

Объединение 3GPP было создано 4 декабря 1998 г. с целью проведения практических работ по стандартизации систем подвижной связи 3G. В него вошли основные азиатские и европейские органы стандартизации. Основные учредители – ETSI, японская ассоциация радиопромышленности и бизнеса ARIB (Association of Radio Industries and Businesses), T1P1, ТТА и комитет телекоммуникационных технологий Японии (Telecommunication Technology Committee).

Во второе объединение 3GPP2 входят Ассоциация промышленности связи США, представленная подкомитетами TIA TR-45.3 и TIA TR-45.3, а также ряд азиатских региональных организаций: ARIB, CWTS (China Wireless Telecommunication Standard Group), ТТА и TTC. Члены 3GPP2 являются сторонниками эволюционного развития двух технологий сотовой связи 2G – IS-136 и cdmaOne, – которые в настоящее время широко распространены как в США, так и в других странах мира.

Общим в работе обеих организаций является использование в создаваемой архитектуре протоколов Интернет, традиционно разрабатываемых и специфицируемых комитетом IETF. Наиболее интересен для нас проект, явившийся результатом совместной работы 3GPP и 3GPP2. Версии IMS, предложенные этими организациями, несколько различаются, но в целом практически идентичны.

11.2.2. От GSM к 3G

Первая спецификация 3GPP появилась уже через год после его основания и носила название 3GPP Release 99. Основным изменением, касающимся сетей GSM, стал новый стандарт участка радиодоступа – WCDMA. Были также введены классы качества обслуживания QoS и, что особенно важно, намечен революционный переход от стандартизации услуг к стандартизации возможностей

предоставления услуг (*Service Capabilities*). Для создания услуг была выбрана архитектура *OSA (Open Service Architecture)* [14, 28].

После этого в 3GPP начали разрабатывать концепцию мобильной сети, полностью базирующейся на протоколе IP и названную *All-IP*, но, в силу трудоемкости задачи, ее решение была разбито на Release 4 и Release 5. Release 4 был закончен без введения концепции IMS, а его основными нововведениями стали эволюция домена коммутации каналов в направлении разделения транспорта и управления, т.е. создания распределенного MSC в виде пары – *MSC Server* и *MGW*, – а также перевод на IP-транспорт протоколов опорной сети.

В Release 5 была впервые представлена IMS. Предполагалось, что она должна стать независимой от технологии доступа и полностью базирующейся на IP сетевой архитектурой, способной взаимодействовать с существующими сетями передачи речи и данных, как стационарными, так и мобильными. Архитектура IMS позволяет создавать одноранговые мультимедийные IP-сеансы с требующимся качеством и между пользовательскими терминалами разных типов, а также обладает всеми средствами, необходимыми для организации услуг, включая регистрацию, роуминг, безопасность и т.п. В Release 5 работа над IMS не была закончена: а были лишь проработаны основные моменты и намечены пути развития в направлении к Release 6.

И все же, в Release 5 была создана полностью базирующаяся на IP архитектура IMS, определены ее сетевые элементы и интерфейсы между ними, а также функции начисления платы. Были разработаны общие принципы маршрутизации вызовов и процедуры управления сеансом, определены процедуры обеспечения безопасности, включающие в себя аутентификацию пользователей, проверку целостности сигнальных сообщений и защиту сети от внешних атак, процедуры взаимодействия IMS и базирующихся на GPRS услуг. Были также определены контрольные точки управления услугами и использование серверов приложений. Для идентификации в IMS-сети был разработан *ISIM (IP Multimedia Services Identity Module)*.

Release 6 был призван ликвидировать возможные недоработки Release 5 и добавить несколько новых функций. Было обеспечено взаимодействие с сетью коммутации каналов, с другими IP-сетями и с разными технологиями доступа (в частности, *WLAN*), добавлены некоторые объекты и контрольные точки, функции групповой маршрутизации, установления сеансов связи с экстренными службами, а также множественная регистрация.

К возможностям обеспечения безопасности были добавлены конфиденциальность сообщений SIP, использование ключей и абонентских сертификатов. Были определены сервисные возможности для мультимедийных услуг многоадресной рассылки информации.

11.2.3. Взаимодействие стандартизирующих организаций

В разработке технологий, используемых в IMS, участвует, помимо 3GPP и 3GPP2, ряд международных стандартизирующих организаций. В то время как 3GPP/3GPP2 концентрируют свои усилия на создании архитектуры IMS и спецификации нескольких базовых услуг, OMA (*Open Mobile Alliance*) занимается стандартизацией услуг для IMS. В OMA пришли к выводу, что каждому шлюзу услуг (*service enabler*) между IT-приложениями и сетевыми узлами нецелесообразно иметь собственные механизмы обеспечения безопасности, качества обслуживания, начисления платы, управления сеансом и т.п.

Шлюзы услуг должны иметь возможность использовать общую инфраструктуру, предоставляющую эти базовые возможности. Различные шлюзы услуг, разработанные в OMA, могут взаимодействовать с IMS, использовать ее собственные возможности и через нее – ресурсы нижележащей сетевой инфраструктуры. Использование IMS существенно сокращает время стандартизации шлюзов услуг, и можно предположить, что взаимодействие OMA и 3GPP в будущем станет еще более тесным, причем OMA, вероятно, даже возьмет на себя всю ответственность за разработку услуг и приложений, реализуемых поверх IMS.

Как уже было сказано, одним из базовых принципов IMS является использование существующих протоколов Интернет. Однако не все выбранные протоколы полностью подходили для работы в среде IMS. В ряде случаев в IETF вообще не было готового протокольного решения для некоторых специфических задач IMS, а в задачу 3GPP/3GPP2 входило не создание новых технологий, а применение IP-технологий, позволяющих использовать все преимущества как существующих услуг Интернет, так и тех, которые будут созданы в будущем. Поэтому наибольшее значение приобрело взаимодействие 3GPP/3GPP2 с IETF, принципы которого были документированы в RFC 3113 и RFC 3131.

В результате этого сотрудничества было создано несколько спецификаций протоколов и расширений протоколов в виде документов RFC. Основной областью, в которой велась активная работа, было использование в IMS протоколов IPv6, DNS, COPS, Diameter и, разумеется, SIP.

Отдельного рассмотрения, которое будет приведено в этой главе чуть позже, требует взаимодействие 3GPP с ETSI. Это взаимодействие осуществляется в рамках проекта TISPAN (*Telecommunication and Internet converged Services and Protocols for Advanced Networking*). Проект появился в сентябре 2003 года как результат слияния проекта SPAN (*Services and Protocols for Advanced Networking*) и известного проекта TIPHON, существовавшего с 1997 года. Проект TISPAN предусматривает 8 рабочих групп,

отвечающих, соответственно, за услуги, архитектуру, протоколы, нумерацию и маршрутизацию, обеспечение QoS, тестирование, безопасность, эксплуатационное управление сетью. Задача этих групп – доработать архитектуру 3GPP IMS так, чтобы она могла стать основой NGN в стационарных сетях и способствовать конвергенции стационарных и мобильных сетей.

11.3. Функциональные возможности IMS

В этом параграфе мы постараемся последовательно рассмотреть задачи, стоявшие перед разработчиками, и причины появления IMS. Это поможет лучше понять роль, которую IMS должна играть в глобальной инфокоммуникационной структуре. Из определения IMS следует, что она предназначена для того, чтобы предоставлять Интернет-услуги повсюду и в любое время с использованием технологий сотовых сетей.

Но дело в том, что современные сотовые сети уже и так могут предоставлять достаточно широкий спектр Интернет-ориентированных услуг. В сетях UMTS существует два домена обслуживания трафика: домен коммутации каналов и домен коммутации пакетов. Домен коммутации каналов в UMTS является эволюционным развитием технологий, уже использующихся в 2G, и ориентирован на передачу речи и видео.

Домен коммутации пакетов предоставляет IP-доступ в Интернет. С использованием этих двух доменов пользователь уже может получить различные мультимедийные услуги, в том числе и Интернет-ориентированные. Зачем же тогда разрабатывать IMS? Ответ можно дать такой: чтобы обеспечить QoS, начисление платы, интеграцию и персонализацию различных услуг. Поясним это.

Предоставление разнообразных услуг на базе единой пакетной сети требует гибкой поддержки качества этих услуг. IMS, устанавливая каждое соединение, следит, чтобы пользователям было обеспечено соответствующее качество обслуживания.

Другой предпосылкой IMS является усложнение системы начисления платы за мультимедийные сеансы связи. Если Оператор не принимает во внимание характер трафика мультимедийного сеанса, он может начислить плату за него только очень поверхностно – на основании объема переданных данных. При этом пользователю не выгодно пользоваться одними услугами (создающими большой объем трафика, например видео), а Оператору не выгодно предоставлять другие (создающие незначительный объем трафика, например Instant Messaging). Если Оператор осведомлен о характере передаваемого трафика, то он может использовать в системе начисления платы более эффективные бизнес-модели, несущие выгоду и ему, и пользователям.

В IMS применен новый подход к предоставлению услуг, позволяющий Оператору внедрять услуги, созданные сторонними разработчиками или даже самим Оператором, а не производителями телекоммуникационного оборудования. Это позволяет интегрировать различные услуги и предоставляет широкие возможности персонализации и увеличения количества услуг.

В настоящее время, до внедрения IMS, в мобильных сетях используются так называемые «вертикальные сервисные платформы», показанные на рис. 11.1, которые успешно справляются с предоставлением небольшого числа ключевых услуг.

Подход IMS предполагает горизонтальную архитектуру (рис. 11.2), позволяющую Оператору просто и экономично внедрять новые персонализированные услуги, причем пользователи могут в рамках одного сеанса связи получить доступ к разным услугам.

Перечислим некоторые функциональные возможности IMS.

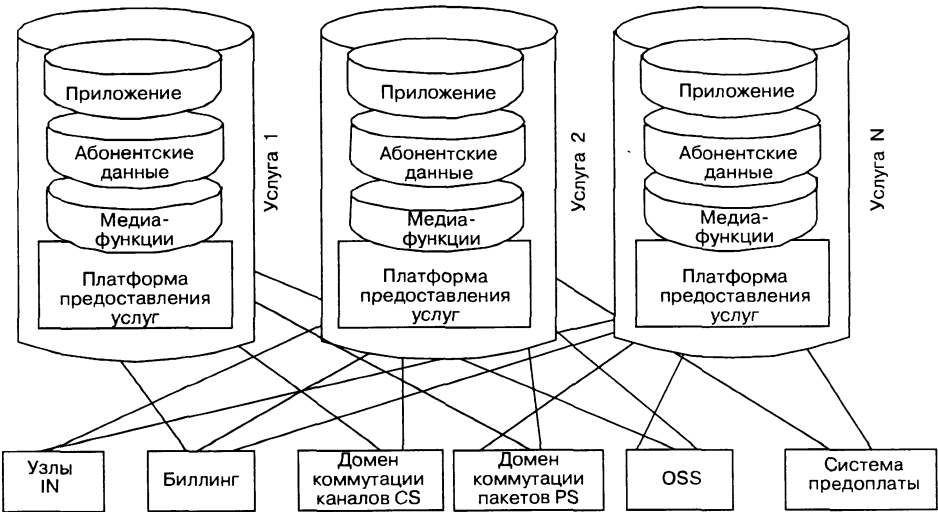


Рис. 11.1. Вертикальные сервисные платформы

11.3.1. Мультимедийные IP-сеансы

IMS может предоставлять широкий спектр услуг, но одна из них безусловно сохраняет ведущую роль – двусторонняя аудио/видео связь. Для этого архитектура IMS должна поддерживать сеансы мультимедийной связи в IP сетях, причем такая связь должна быть доступна пользователям как в домашней, так и в гостевой сети. Мультимедийная связь была стандартизована уже в ранних документах 3GPP, еще до появления IMS, но предоставлялась только доменом коммутации каналов.

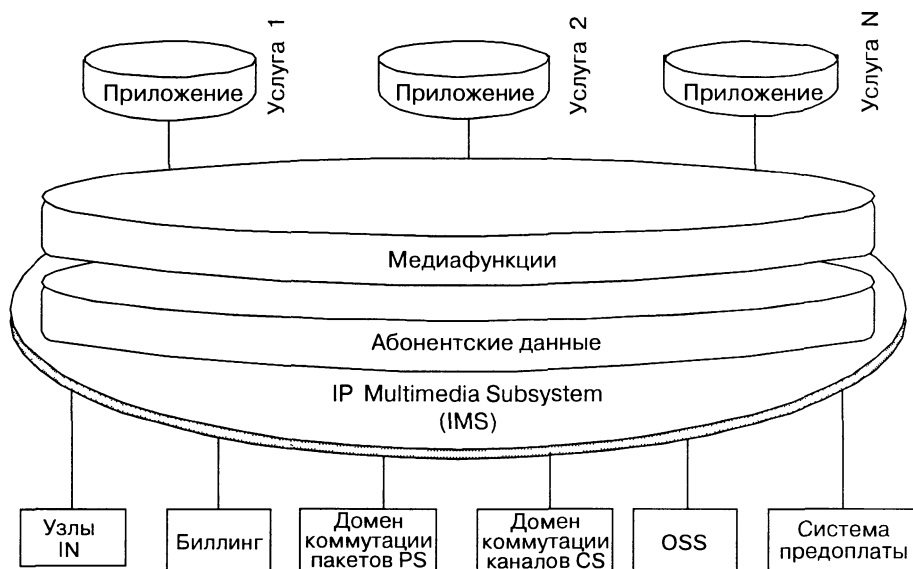


Рис. 11.2. Горизонтальная сервисная архитектура, применяемая в IMS

11.3.2. Качество обслуживания

Поддержка QoS является фундаментальным требованием к IMS. При организации сеанса пользовательское оборудование извещает IMS о своих возможностях и своих требованиях к QoS. Как было показано в главе 4, при помощи протокола SIP возможно учесть такие параметры, как тип и направление передачи данных, битовая скорость, размер пакетов, использование RTP, требуемая ширина полосы пропускания. IMS позволяет управлять качеством связи, которое получит тот или иной пользователь, и таким образом дифференцировать пользователей и услуги.

11.3.3. Взаимодействие с другими сетями

Функция поддержки взаимодействия с сетью Интернет очевидна, т.к. благодаря общим протоколам пользователи IMS могут устанавливать мультимедийные сеансы связи с разными службами глобальной сети. Поскольку переход к NGN и IMS будет постепенным и более или менее длительным, то IMS должна также иметь возможность взаимодействия с сетями предыдущих поколений – стационарными (ТФОП) и мобильными (2G) сетями с коммутацией каналов. Функции взаимодействия с сетями коммутации каналов не имеют, разумеется, дальней перспективы, но они абсолютно необходимы в течение долгого периода существования конвергентных сетей.

11.3.4. Инвариантность доступа

Функциональные возможности IMS инвариантны относительно разных технологий доступа к ней, отличных от GPRS, например, использующих WLAN, xDSL, HFC (Hybrid Fiber Coax), кабельный модем и т.п. Здесь нет ничего необычного. Как и любая IP-сеть, IMS инвариантна относительно протоколов нижних уровней и технологий доступа. Но поскольку 3GPP сконцентрировал свои усилия на эволюции GSM сетей, спецификация первой версии IMS (Release 5) содержала некоторые GPRS-ориентированные опции. В следующих версиях, уже с шестой, функции доступа были отделены от ядра сети, и началась разработка инвариантности доступа к IMS, получившая название *IP connectivity access* и предполагающая применение любой технологии доступа, которая может обеспечить транспортировку IP-трафика между пользовательским оборудованием и объектами IMS.

11.3.5. Создание услуг и управление услугами

Необходимость быстро внедрять разнообразные услуги, поскольку именно они должны стать основным источником доходов Оператора в XXI веке, потребовала пересмотреть процесс создания услуг в IMS. Чтобы уменьшить время внедрения услуги и обеспечить ее предоставление в гостевой сети, когда пользователь находится в роуминге, в IMS ведется стандартизация не услуг, а возможностей предоставления услуг (*service capability*). Таким образом, Оператор может внедрить любую услугу, соответствующую *service capability*, причем эта услуга будет поддерживаться и при перемещении пользователя в гостевую сеть, если эта сеть обладает аналогичными стандартизованными *service capability*.

Это достигается благодаря тому, что в IMS принято управление услугой из домашней сети, то есть устройство, имеющее доступ к базе данных пользователей и непосредственно взаимодействующее с сервисной платформой, всегда находится в домашней сети. Для управления услугами Оператор может применять разную общую политику сети, распространяющуюся на всех пользователей сети (например, ограничение использования в сети широкополосных кодеков типа G.711), и разную индивидуальную политику, распространяющуюся на того или иного пользователя (например, запрет пользования видеосвязью).

11.3.6. Роуминг

Функции роуминга существовали уже в мобильных сетях 2G, и IMS, естественно, эти функции унаследовала. Однако само понятие «роуминг» теперь существенно расширилось и включает в себя:

- GPRS-роуминг – гостевая сеть предоставляет RAN и SGSN, а в домашней находятся GGSN и IMS;

- IMS-роуминг – гостевая сеть предоставляет IP-соединение и точку входа (например P-CSCF), а домашняя сеть обеспечивает все остальные функции;
- CS-роуминг – роуминг между сетью IMS и сетью коммутации каналов.

11.3.7. Безопасность

Функции обеспечения безопасности необходимы каждой телекоммуникационной системе, и IMS предоставляет уровень безопасности, по крайней мере, не меньший, чем GPRS-сети и сети коммутации каналов. IMS производит аутентификацию пользователей перед началом предоставления услуги, предоставляет пользователю возможность запросить конфиденциальность информации, передаваемой во время сеанса, и др.

11.3.8. Начисление платы

Как было отмечено выше, IMS позволяет Оператору или провайдеру услуг гибко назначать тарифы для мультимедийных сеансов. IMS сохраняет возможность начислять плату за сеанс наиболее простым способом – в зависимости от длительности сеанса или от объема трафика, но может также использовать более сложные схемы, учитывающие разную пользовательскую политику, компоненты медиа-данных, предоставляемые услуги и т.п. Требуется также, чтобы две IMS-сети при необходимости могли обмениваться информацией, нужной для начисления платы за сеанс связи. IMS поддерживает начисление платы в режиме как online, так и offline.

11.4. Архитектура IMS

11.4.1. Уровни IMS

Для IMS разработана многоуровневая архитектура с разделением транспорта для переноса трафика и сигнальной сети IMS для управления сеансами (рис. 11.3). Таким образом, 3GPP при разработке IMS фактически перенес на мобильные сети основную идеологию Softswitch. Хотя некоторые функции не всегда легко отнести к тому или иному уровню, но такой подход обеспечивает минимальную зависимость между уровнями. В IMS можно выделить:

- User Plane – пользовательский уровень или уровень передачи данных;
- Control Plane – уровень управления;
- Application Plane – уровень приложений.

Прежде чем переходить к детальному рассмотрению элементов IMS-архитектуры, отметим, что 3GPP, по примеру IPCC, специфицирует не узлы сети, а функции. Это означает, что IMS-архитектура, как и Softswitch, представляет собой набор функций, соединенных стандартными интерфейсами. Разработчики вправе комбинировать несколько функций в одном физическом объекте или, наоборот, реализовать одну функцию распределенно, однако чаще всего физическую архитектуру ставят в соответствие функциональной и реализуют каждую функцию в отдельном узле.

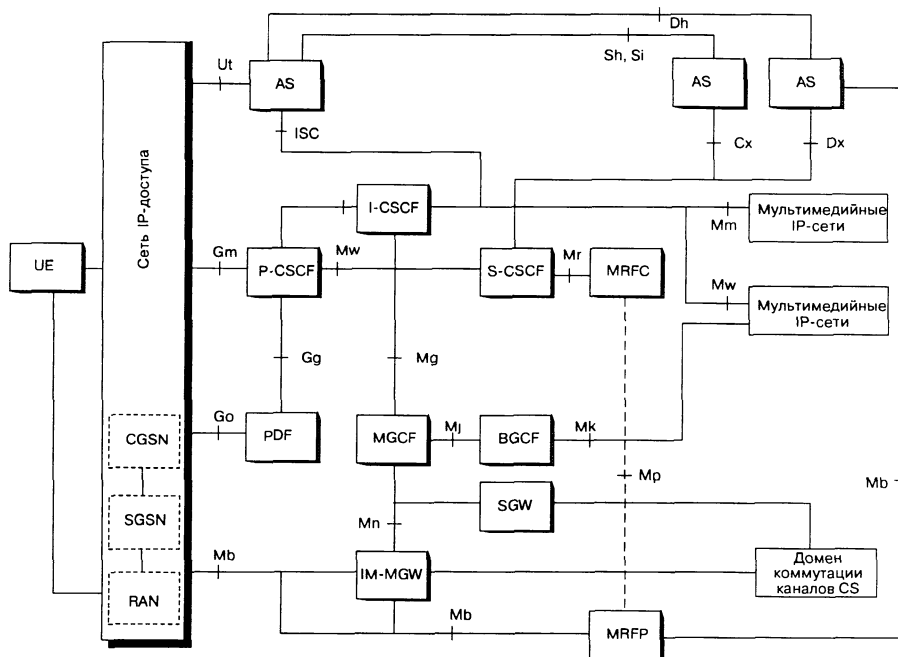


Рис. 11.3. Архитектура IMS

11.4.2. Пользовательские базы HSS и SLF

Каждая IMS-сеть содержит один или более серверов пользовательских баз данных **HSS** (*Home Subscriber Server*). По сути, HSS представляет собой централизованное хранилище информации об абонентах и услугах и является эволюционным развитием **HLR** (*Home Location Register*) из архитектуры сетей GSM. В HSS хранится вся информация, которая может понадобиться при установлении мультимедийного сеанса: информация о местонахождении пользователя, информация для обеспечения безопасности (аутентификация и авторизация), информация о пользовательских профилях, об обслуживающей пользователя **S-CSCF**, и о триггерных точках обращения к услугам. Функции, выполняемые HSS, показаны в общем виде на рис. 11.4.

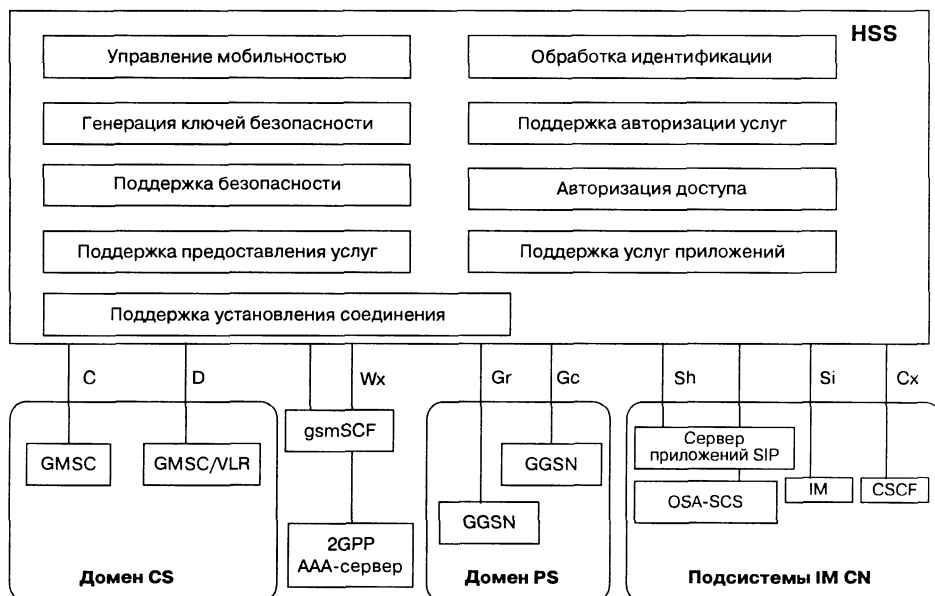


Рис. 11.4. Логические функции HSS

Сеть может содержать более одного HSS в том случае, если количество абонентов слишком велико, чтобы поддерживаться одним HSS. Такая сеть, наряду с несколькими HSS, должна будет иметь в своем составе функцию *SLF* (*Subscriber Location Function*), представляющую собой простую базу данных, которая хранит данные и соответствие информации HSS адресам пользователей. Узел, передавший к *SLF* запрос с адресом пользователя, получает от нее сведения о том HSS, который содержит информацию об этом пользователе. Как HSS, так и *SLF* используют для взаимодействия с прочими элементами IMS протокол *Diameter*. Помимо функций, специфических для IMS, HSS имеет модули, являющиеся полноценными HLR и AUC для поддержки инфраструктуры мобильных сетей 2G.

11.4.3. Функция SIP-сервера

Функция управления сеансами *CSCF* (*Call/Session Control Function*) является центральной частью системы IMS, представляет собой, по сути, SIP-сервер и обрабатывает SIP-сигнализацию в IMS. Существуют функции *CSCF* трех типов:

- Proxy-CSCF (P-CSCF);
- Interrogating-CSCF (I-CSCF);
- Serving-CSCF (S-CSCF).

Первая из перечисленных, функция *P-CSCF*, – это первая точка взаимодействия (на сигнальном уровне) пользовательского IMS-терминала и IMS-сети. С позиций главы 4, т.е. с точки зрения SIP, она является входящим/исходящим прокси-сервером, через который проходят все запросы, исходящие от IMS-терминала или направляемые к нему. Однако *P-CSCF* может вести себя и как агент пользователя *UA*, что необходимо для прерывания сеансов в нестандартных ситуациях, и для создания независимых SIP-транзакций, связанных с процессом регистрации. *P-CSCF* прикрепляется к пользовательскому терминалу при регистрации в сети и не меняется в течение всего срока регистрации. Основным назначением *P-CSCF* является маршрутизация запросов и ответов SIP между пользовательским терминалом и узлами IMS-сети (*I-CSCF*, *S-CSCF* и др.).

P-CSCF выполняет также ряд требований, относящихся к обеспечению безопасности. Она устанавливает несколько ассоциаций IPsec, обеспечивающих целостность информации, передаваемой к IMS-терминалу. Создание этих ассоциаций предусматривает аутентификацию пользователя, и, выполнив ее, *P-CSCF* извещает об этом пользователе остальные узлы сети, чтобы им не нужно было повторно выполнять ту же процедуру.

В задачи *P-CSCF* входит и проверка правильности построения сообщений SIP, передаваемых IMS-терминалом. Кроме того, *P-CSCF* производит компрессию и декомпрессию сообщений SIP для того, чтобы ускорить время их передачи по узкополосным каналам (например, на радиоучастке) и, тем самым, уменьшить время установления соединения или предоставления услуги. К тому же, *P-CSCF* обнаруживает запросы соединений с аварийными службами и либо сообщает об ошибке (Release 5), либо выбирает *S-CSCF*, необходимую для организации такой связи. Еще одной задачей *P-CSCF* является создание учетной информации и отправка ее к узлу, отвечающему за начисление платы.

Чтобы обеспечивались масштабируемость и надежность, IMS-сеть обычно содержит несколько *P-CSCF*, каждая из которых обслуживает некоторое количество IMS-терминалов, зависящее от емкости узла. IMS-архитектура предусматривает, что *P-CSCF* может находиться как в домашней, так и в гостевой сети. Если сеть базируется на технологии GPRS, то *P-CSCF* должна находиться там же, где и *GGSN* (*Gateway GPRS Support Node*), т.е. в домашней сети, но мере распространения IMS это условие не будет обязательным для обоих этих узлов.

Теперь перейдем к рассмотрению *I-CSCF* – еще одного SIP-прокси, расположенного на границе административного операторского домена. Когда SIP-сервер определяет следующую пересылку для некоторого SIP-сообщения, он получает от службы DNS адрес

I-CSCF соответствующего домена. Кроме исполнения функций SIP-прокси, I-CSCF взаимодействует по протоколу Diameter с HSS и SLF, получает от них информацию о местонахождении пользователя и об обслуживающей его S-CSCF. Если никакая S-CSCF еще не назначена, I-CSCF производит ее назначение.

Дополнительно I-CSCF может шифровать части SIP-сообщений, содержащие важную информацию о домене, такую как число серверов в домене, их DNS-имена и т.п. Эта группа функций называется *THIG (Topology Hiding Inter-network Gateway)* – межсетевой шлюз сокрытия топологии. Поддержка THIG опциональна и не всегда нужна; в частности, она не требуется, если провайдер на границе своей сети устанавливает рассмотренный в главе 9 контроллер SBC (Session Border Controller). Обычно, чтобы обеспечивалась масштабируемость и надежность, в сети присутствует несколько I-CSCF. Типичным местонахождением I-CSCF является домашняя сеть, однако в ряде специфических случаев, таких как поддержка THIG, она может быть вынесена и в гостевую.

И, наконец, обслуживающая функция *S-CSCF* – центральная интеллектуальная функция на сигнальном уровне, т.е. функция SIP-сервера, который управляет сеансом. Помимо функции SIP-сервера, S-CSCF выполняет функцию регистрирующего сервера сети SIP (SIP-registrar), то есть поддерживает привязку местоположения пользователя (например, IP-адреса терминала, с которого пользователь получил доступ в сеть) к его SIP-адресу (PUI-Public User Identity), что подробно обсуждалось в главе 4.

Аналогично I-CSCF, S-CSCF взаимодействует по протоколу Diameter с HSS, получает от него аутентификационные данные пользователя, пытающегося получить доступ к сети, и данные о профиле пользователя, то есть перечень доступных ему услуг – набор триггерных точек для маршрутизации сообщения SIP к серверам приложений. В свою очередь, S-CSCF информирует HSS о том, что этот пользователь прикреплен к нему на срок своей регистрации, и о срабатывании таймера регистрации.

Вся сигнальная информация SIP, передаваемая и принимаемая пользовательским IMS-терминалом, проходит через S-CSCF, к которой прикреплен пользователь. S-CSCF анализирует каждое сообщение и определяет, должно ли оно, по пути к пункту назначения, пройти через серверы приложений, предоставляющие пользователю услуги. S-CSCF поддерживает сеанс в течение всего времени его продолжения и, по мере надобности, взаимодействует с сервисными платформами и с функциями начисления платы.

Одной из основных функций S-CSCF является маршрутизация SIP-сообщений. Если пользователь набирает телефонный номер вместо SIP URI, то S-CSCF производит преобразование номера

Рассмотрим эти три типа серверов приложений:

- *SIP AS (SIP Application Server)* – классический сервер приложений, предоставляющий мультимедийные услуги на базе протокола SIP;
- *OSA-SCS (Open Service Access – Service Capability Server)* предоставляет интерфейс к серверу приложений OSA и функционирует как сервер приложений со стороны S-CSCF и как интерфейс между сервером приложений OSA и OSA API – с другой стороны;
- *IM-SSF (IP Multimedia Service Switching Function)* позволяет использовать в IMS услуги *CAMEL (Customized Applications for Mobile Network Enhanced Logic)*, разработанные для GSM сетей, а также позволяет управляющей функции *gsmSCF (GSM Service Control Function)* управлять IMS-сеансом. Со стороны S-CSCF сервер IM-SSF функционирует как сервер приложений, а с другой стороны – как функция *SSF (Service Switching Function)*, взаимодействующая с *gsmSCF* по протоколу CAP.

Помимо обязательного для серверов приложений всех типов SIP-интерфейса со стороны IMS, они могут также иметь интерфейсы к HSS, причем SIP AS и OSA-SCS взаимодействуют с HSS по протоколу Diameter для получения данных о пользователе или для обновления этих данных в HSS, а информационный обмен между IM-SSF и HSS ведется по протоколу MAP.

Серверы приложений могут находиться либо в домашней, либо в любой другой сети, с которой у провайдера есть сервисное соглашение. Но если сервер приложений находится во внешней сети, он не может иметь интерфейс с HSS.

11.4.6. MRF

Теперь рассмотрим *MRF (Media Resource Function)*, являющуюся источником медиа-информации в домашней сети и позволяющую воспроизводить разные объявления, смешивать медиа-потoki, транскодировать битовые потоки кодеков, получать статистические данные и анализировать медиа-информацию. Функция MRF делится на две части:

- *MRFC – Media Resource Function Controller*
- *MRFP – Media Resource Function Processor*

MRFC находится на сигнальном уровне и взаимодействует с S-CSCF по протоколу SIP. Используя полученные инструкции, MRFC управляет по протоколу MEGACO/H.248 процессором MRFP, находящимся на уровне передачи данных, а тот выполняет все манипуляции с медиа-информацией. Сама MRF всегда находится в домашней сети.

Шлюз сигнализации *SGW* представляет собой интерфейс для связи с уровнем сигнализации в сети коммутации каналов, производит преобразование нижних протокольных уровней систем сигнализации для двустороннего сигнального обмена между сетью IP и сетью ТфОП. При этом *SGW* никак не обрабатывает сообщения прикладного уровня.

Функция управления медиа-шлюзом – центральная часть распределенного шлюза *PSTN/CS*. Она преобразует сообщения *ISUP* и *ВІСС*, которые поступают со стороны ТфОП, в сообщения *SIP*, которые *IMS* использует для управления сеансом связи через границу между сетями (рис. 11.7). Кроме мэппинга сигнальных протоколов, *MGCF* управляет по протоколу *MEGACO/H.248* ресурсами медиа-шлюза, участвующего в создании соединения.

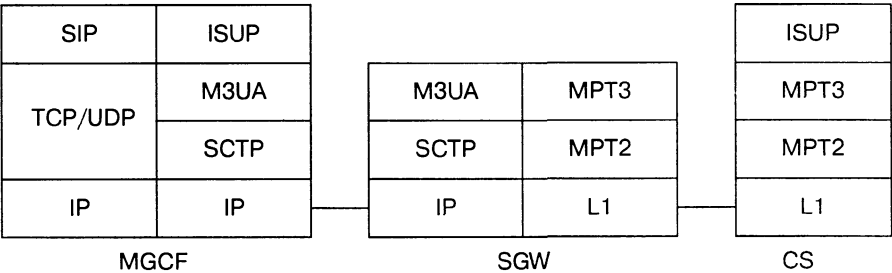


Рис. 11.7. Управление сеансом связи

Транспортный шлюз *MGW* соединяет сеть IP с сетью коммутации каналов на уровне передачи трафика, выполняя двустороннее преобразование пользовательского трафика, проходящего через границу между сетями. Со стороны *IMS*-сети шлюз *MGW* ведет передачу и прием данных в виде *RTP*-пакетов, а со стороны сети с коммутацией каналов реализует стандартный *TDM*-интерфейс. Кроме того, *MGW* может производить транскодирование информации, если в *IMS* и в сети коммутации каналов используются разные речевые кодеки (обычно в *IMS* используется *AMR*, а в ТфОП *G.711*).

11.4.9. Шлюз безопасности *SEG*

Для того чтобы защитить уровень управления в домене безопасности (*security domain*), представляющем собой область сети, которая принадлежит одному провайдеру услуг, и в которой действуют единые административные правила и сетевая политика, трафик на входе в этот домен и на выходе из него будет проходить через шлюз безопасности *SEG (Security Gateway)*. Как правило, границы домена безопасности совпадают с границами сети провайдера, а шлюзов *SEG* в сети провайдера обычно присутствует несколько. В качестве *SEG* часто выступают пограничные контроллеры *SBC*, рассматривавшиеся в главе 9.

11.4.10. Модули GPRS

Основные GPRS-модули в контексте IMS представлены на рис. 11.8.

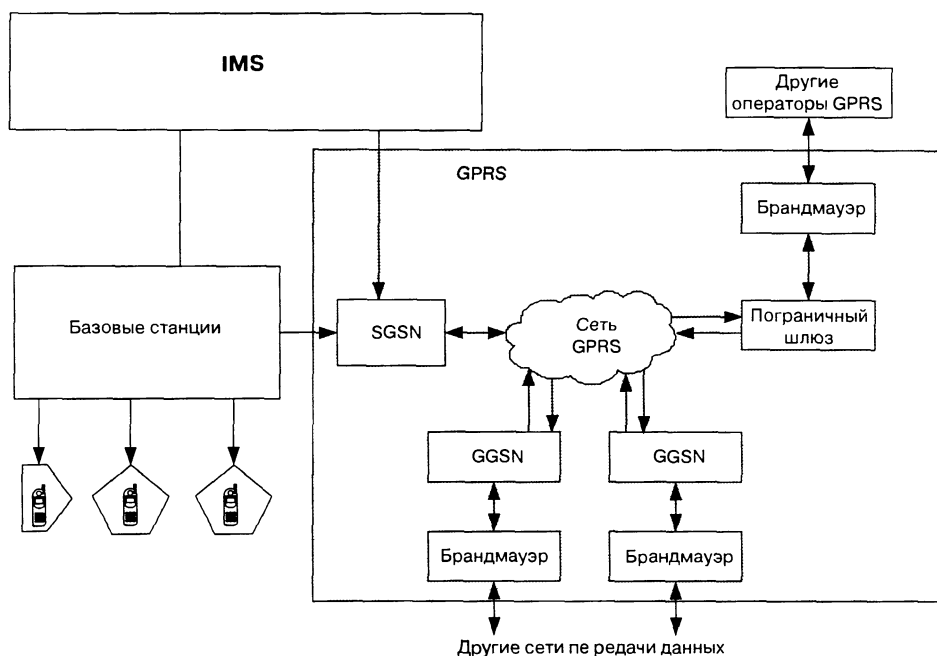


Рис. 11.8. Архитектура GPRS

Обслуживающий узел GPRS, *serving GPRS support node* (SGSN) – основной компонент домена коммутации пакетов, который транслирует IP-пакеты, передаваемые/получаемые мобильной станцией. По своей сути, это такой же центр коммутации, как и MSC в GSM, но в отличие от последнего, он коммутирует пакеты, а не каналы. SGSN управляет не только пакетными сеансами связи, но и мобильностью GPRS-пользователей, а также может следить за качеством предоставления услуг и генерировать информацию, необходимую для начисления платы.

Узел поддержки шлюза GPRS, *gateway GPRS support node* (GGSN), отвечает за прием/передачу данных внешних сетей, например, Интернет или IMS-сети другого Оператора связи. С точки зрения внешней сети узел GGSN выглядит как обычный маршрутизатор и выполняет маршрутизацию IP-пакетов, переносящих сигнальные сообщения SIP между пользовательским терминалом и P-CSCF. Помимо маршрутизации, GGSN отвечает за раздачу IP-адресов, реализацию политики и начисление оплаты за услуги.

11.5. Идентификация в IMS

В любой сети связи необходима идентификация пользователей или пользовательских терминалов, по крайней мере, для того, чтобы устанавливать соединения между пользователями, однозначно определенными с помощью идентификаторов. Кроме того, при предоставлении разных услуг зачастую необходимо идентифицировать сами услуги. В этом параграфе мы рассмотрим вопросы идентификации пользователей и услуг в IMS.

Основным идентификатором, присваиваемым пользователю, является Private User Identity (PrUI), имеющий формат NAI (Network Access Identifier), определенный в RFC 2486. Формат выглядит следующим образом: *username@operator.com*.

Заметим, что PrUI используются для идентификации пользователя и для его аутентификации, но в отличие от телефонных номеров в ТфОП не служат для маршрутизации. Сравнивая сети 3G с 2G можно провести параллель между PrUI и IMSI (*International Mobile Subscriber Identifier*). Пользователю не обязательно знать свой идентификатор PrUI, он может храниться на идентификационной карте, о которой речь пойдет ниже.

3GPP Release 5 предписывал каждому пользователю иметь один уникальный PrUI, но в Release 6 это ограничение убрано, и теперь пользователь может иметь несколько разных PrUI. И хотя на одну идентификационную карту, используемую в UMTS, по-прежнему можно поместить только один PrUI, пользователь может иметь несколько таких карт и несколько терминалов, что в комбинации с использованием другого идентификатора, а именно, *Public User Identity (PuUI)*, предоставляет пользователю большую гибкость выбора адресов.

Каждому PrUI Оператор ставит в соответствие один или несколько PuUI, имеющих формат SIP URI по RFC 3261 или TEL URL по RFC 2806. В IMS идентификатор PuUI используется для маршрутизации сигнальных SIP-сообщений и в качестве контактной информации для других абонентов. Можно и тут провести параллель с идентификатором *MSISDN (Mobile Subscriber ISDN Number)* мобильных сетей 2G.

Когда PuUI представлен в формате SIP URI, то он имеет вид *sip:alexander@operator.com*. В SIP URI можно поместить телефонный номер – *sip:+7-812-960-6293@operator.com;user=phone*. Этот формат необходим, поскольку при регистрации SIP требует наличия SIP URI, и, следовательно, нельзя зарегистрировать TEL URL, но можно SIP URI, содержащий телефонный номер. С другой стороны, чтобы пользователь мог вызывать терминалы ТфОП и принимать вызовы от них, он должен иметь TEL URL, имеющий вид *tel:+7-812-960-6293*.

Таким образом, пользователю обычно требуется минимум два разных PuUI. Другая причина иметь несколько PuUI – привлекательная для пользователя возможность иметь разные номера для разных контактов или услуг.

Идентификационная карта IMS-терминала *UICC (Universal Integrated Circuit Card)* хранит один PrUI и, как минимум, один PuUI. Полная структура взаимосвязи нескольких PrUI и PuUI хранится в абонентском профиле HSS. Пример такой структуры приведен на рис. 11.9.

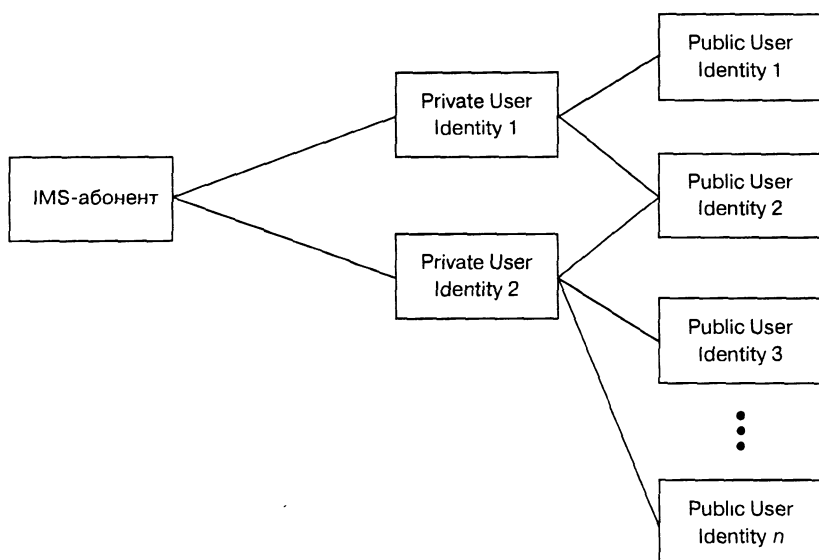


Рис. 11.9. Идентификация IMS-абонентов

Заметим, что *UICC* – термин, означающий сменную идентификационную карту, имеющую стандартизованный интерфейс с терминалом, а физически карта *UICC* может содержать несколько логических приложений, таких как хорошо известный *SIM (Subscriber Identity Module)*, который используется при идентификации пользователей сетей GSM, *USIM (Universal Subscriber Identity Module)* который применяется для идентификации в сетях UMTS, и *ISIM (IP Multimedia Services Identity Module)* – наиболее важное приложение в контексте этой главы, поскольку служит для идентификации, авторизации и конфигурации терминала при работе в IMS-сети.

Получить доступ к услугам IMS пользователь может только при условии, что в его *UICC* содержится *USIM* или *ISIM*, причем использование последнего предпочтительнее. Структура *ISIM* приведена на рис. 11.10.

Home Network Domain URI – SIP URI, определяющий имя домашней сети. Он используется для поиска домашней сети при регистрации. В *ISIM* может храниться только один *Home Network Domain URI*.

Long-term Secret – поле, используемое в целях аутентификации, проверки целостности, расчета ключей шифрования.

Поля всех идентификаторов доступны терминалу только для чтения.

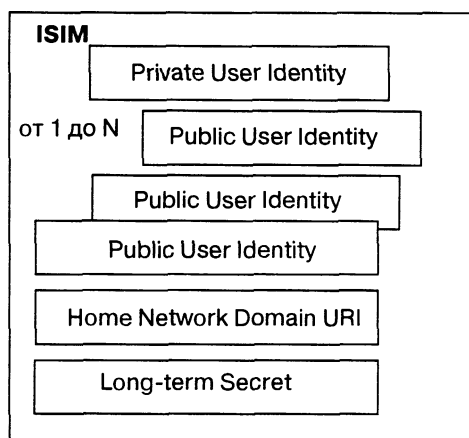


Рис. 11.10. Модуль ISIM

Чтобы рассказ об идентификации в IMS приобрел некую полноту, упомянем еще об одном идентификаторе – *Public Service Identity (PSI)*, – появившемся только в 3GPP Release 6. В отличие от описанных выше идентификаторов, PSI присваивается не пользователям, а услугам, размещенным на серверах приложений. Так же, как и PuUI, идентификаторы PSI могут иметь формат SIP URI или TEL URL.

11.6. IMS в стационарных сетях

Хорошо проработанные спецификации IMS, а также успешное внедрение IMS рядом Операторов мобильных сетей, привлекли внимание специалистов в области стационарных сетей к этой архитектуре. Основным моментом, выгодно отличающим IMS от других концепций построения сетей NGN, является как раз наличие стандартов, которые дают возможность иметь единообразные и поэтому способные эффективно взаимодействовать сети. До появления архитектуры IMS в 3GPP определенные работы велись и в других упоминавшихся в книге стандартизирующих организациях. В ETSI и в ITU-T разрабатывались элементы архитектуры NGN, в IETF стандартизировались протоколы, в MSF и в IPCC решались вопросы, необходимые рынку, DSL Forum создавал спецификации для своей области, но никто не брался за создание целостной системы. В это время в 3GPP «почти случайно» создали завершенную систему NGN, включая архитектуру, начисление платы и биллинг,

управление, причем все это – с использованием исключительно открытых стандартных интерфейсов. Технический прогресс на этом, разумеется, не останавливается. В области применения IMS в стационарных сетях можно выделить два направления дальнейших исследований: использование IMS для предоставления новых услуг пользователям в качестве альтернативы Softswitch и использование IMS как основы для конвергенции стационарных и мобильных сетей *FMC (Fixed-Mobile Convergence)*. Практической реализацией тех или иных решений в том и другом направлении производители и Операторы занимаются на свой страх и риск, а стандартизация использования IMS в стационарных сетях и построения NGN на базе IMS-архитектуры ведется по упомянутому в начале главы проекту TISPAN комитета ETSI.

Аналогично процессу стандартизации и развития концепции UMTS-сети в 3GPP, в TISPAN стандартизация делится на этапы, результатом каждого из которых в 3GPP и в TISPAN является очередной Release. Завершение первого Release в проекте TISPAN планировалось на середину 2005 года, но потом было отодвинуто к концу года. Этот Release должен решить вопросы мобильности пользователей стационарной сети и доступа к IMS с использованием проводных технологий. В дальнейшем Release 2 должен будет решить задачу оптимизации ресурсов сети доступа, а Release 3 – обеспечить межсетевую мобильность пользователей и увеличение ширины полосы пропускания в технологиях доступа (VDSL, FTTH, Wi-max).

Основной упор в Release 1 делается на использование для доступа к IMS технологий ADSL и WLAN. Он базируется на 3GPP Release 6, на наработках по Release 7 и на исследованиях, выполненных в проекте TISPAN. В TISPAN решено сохранить принцип деления функций сети на подсистемы, как это определено в 3GPP, что позволяет добавлять для поддержки изменяющихся требований и наборов услуг новые подсистемы, в частности, подсистемы, специфицированные другими организациями.

Поддержку разнотипного доступа в Release 1 обеспечивают две новые подсистемы:

- *Network Attachment Subsystem (NASS)* производит: назначение IP-адресов (например, используя *DHCP – Dynamic Host Configuration Protocol*); аутентификацию на уровне IP, авторизацию доступа к сети, определение местонахождения на уровне IP и др.;
- *Resource and Admission Control Subsystem (RACS)* выполняет управление доступом.

Благодаря совместным усилиям TISPAN и 3GPP, архитектура IMS адаптируется к xDSL-доступу, для которого поддерживаются мультимедийные услуги, и обеспечивается симуляция услуг PSTN/ISDN, перечень которых приведен в табл. 11.1. Определены те из этих

услуг, симуляция которых обязательна, которых – рекомендована, которых – опциональна. В таблице показано также соответствие услуг, предоставляемых в IMS, аналогичным услугам в ТфОП/ISDN, причем, во избежание путаницы, названия всех услуг даны в оригинальном англоязычном варианте, поскольку устоявшиеся русскоязычные названия есть не у всех услуг ТфОП/ISDN, не говоря уж об услугах IMS.

Таблица 11.1. Услуги IMS по TISpan и 3GPP

Приоритет	Симулируемая в IMS услуга	Эквивалентная услуга ТфОП/ISDN
Обязательно	Originating Identification Presentation (OIP)	Calling Line Identification Presentation (CLIP)
Обязательно	Originating Identification Restriction (OIR)	Calling Line Identification Restriction (CLIR)
Обязательно	Terminating Identification Presentation (TIP)	Connected Line Identification Presentation (COIP)
Обязательно	Terminating Identification Restriction (TIR)	Connected Line Identification Restriction (COIR)
Обязательно	Malicious Communication Identification (MCID)	Malicious Call Identification (MCID)
Обязательно	Anonymous Communication Rejection (ACR)	Anonymous Call Rejection (ACR)
Рекомендовано	Communication Diversion (CDiv)	Call Diversion (CDiv)
Рекомендовано	Communication Forwarding Unconditional (CFU)	Call Forwarding Unconditional (CFU)
Рекомендовано	Communication Forwarding on Busy user (CFB)	Call Forwarding Busy (CFB)
Рекомендовано	Communication Forwarding on no Reply (CFNR)	Call Forwarding No Reply (CFNR)
Рекомендовано	Communication Deflection (CD)	Call Deflection (CD)
Рекомендовано	Communication Forwarding on Not-Logged On (CFNL)	Call Forwarding on Mobile Subscriber Not Reachable
Рекомендовано	Communication Waiting (CW)	Call Waiting (CW)
Рекомендовано	Communication Hold (HOLD)	Call Hold (HOLD)
Рекомендовано	Communication Barring (CB) (Outgoing CB, Selective Outgoing CB, Incoming CB)	Outgoing Call Barring (OCB)
Рекомендовано	Completion of Communications to Busy Subscriber (CCBS)	Completion of Calls to Busy Subscriber (CCBS)
Рекомендовано	Follow Me (FM)	Follow Me (FM)
Рекомендовано	Message Waiting Indicator (MWI)	Message Waiting Indicator (MWI)
Опционально	Conferencing (CONF)	Conference Calling (CONF)
Опционально	Advice of Charge (AoC)	Advice of Charge (AoC)
Опционально	Closed User Group (CUG)	Closed User Group (CUG)
Опционально	Fixed Destination Communication	
Опционально	Inhibition of Incoming Forwarded Communications (IIFC)	
Опционально	Direct Dial In (DDI)	Direct Dial In (DDI)
Опционально	Explicit Communication Transfer (ECT)	Explicit Call Transfer (ECT)
Опционально	Trunk Hunting (TH)	

Отдельно TISPAN определяет для IMS подсистему эмуляции услуг ТфОП/ISDN, которая позволяет заменить TDM-оборудование коммутации каналов средствами IMS, сохранив в сети традиционные абонентские терминалы. Здесь разница между симуляцией и эмуляцией следующая. Симуляция заключается в предоставлении ТфОП/ISDN услуг на базе IMS только интеллектуальным терминалам (например, IP-телефонам).

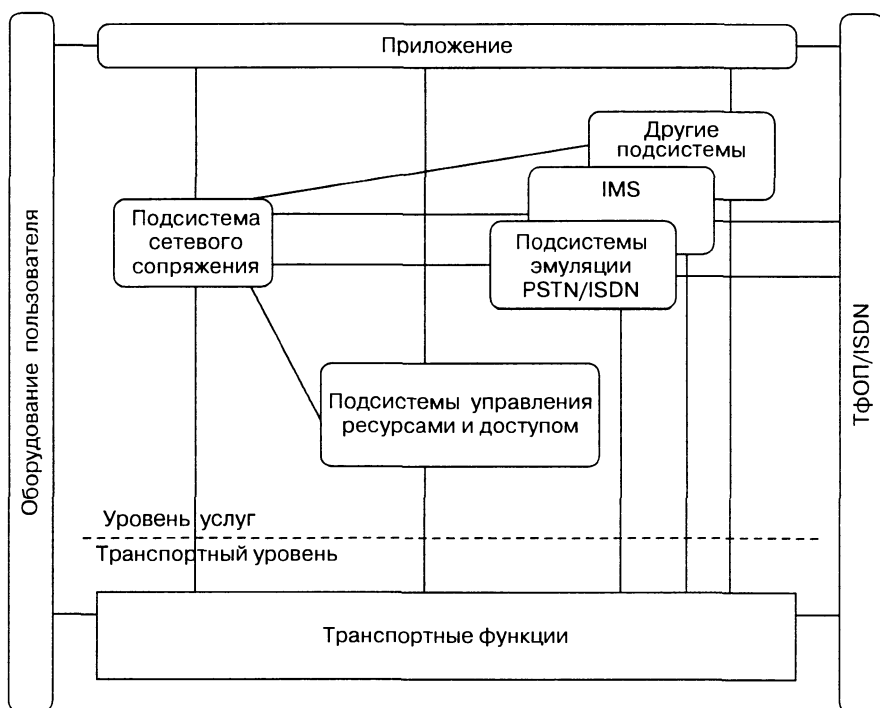


Рис. 11.11. Архитектура NGN сети в проекте TISPAN

При этом не обязательно строго выполнять все требования, предъявляемые к этим услугам, и не предоставлять весь спектр услуг, а ограничиться лишь некоторыми из них, наиболее популярными, возможно, с иными эргономическими характеристиками.

Эмуляция же заключается в том, что IP-сеть создает для окончного оборудования видимость того, что она является ТфОП/ISDN сетью. Пользователи не ощущают того, что они подключаются к IP-сети, а не к ТфОП/ISDN, и следовательно, обеспечивается возможность использования и интеллектуальных, и не интеллектуальных терминалов.

Существует два подхода к созданию подсистемы эмуляции ТфОП/ISDN в современных IP-сетях. Один – применение Softswitch, требующего стандартизации не внутренней структуры, а лишь

внешних интерфейсов. Этот подход и используется в TISpan NGN Release 1. Второй подход – использование (полностью или частично) функциональной архитектуры IMS для определения внутренней структуры подсистемы эмуляции ТФОП/ISDN.

В реальных сетях и, возможно, в будущих стандартах, могут применяться компромиссные варианты, например стандартизация внешних интерфейсов IMS; к тому же, функциональная архитектура IMS позволяет создавать реальную физическую архитектуру сети на оборудовании Softswitch (MGC) и медиа-шлюзах (MG).

В TISpan NGN Release 2, все же, будет, скорее всего, использован второй подход. Но для обоих подходов уже определен сигнальный протокол – SIP-I.

Еще одна новая подсистема – NASS, по сути, замещает функции домена коммутации пакетов 3GPP и GPRS-процедуры аутентификации и управления определением местоположения. При создании этой подсистемы еще предстоит решить ряд проблем – взаимодействия с механизмами аутентификации на уровне SIP, соблюдения соответствия стандартам Форума DSL, использования одной NASS для каждой из сетей доступа или одной NASS для нескольких сетей доступа.

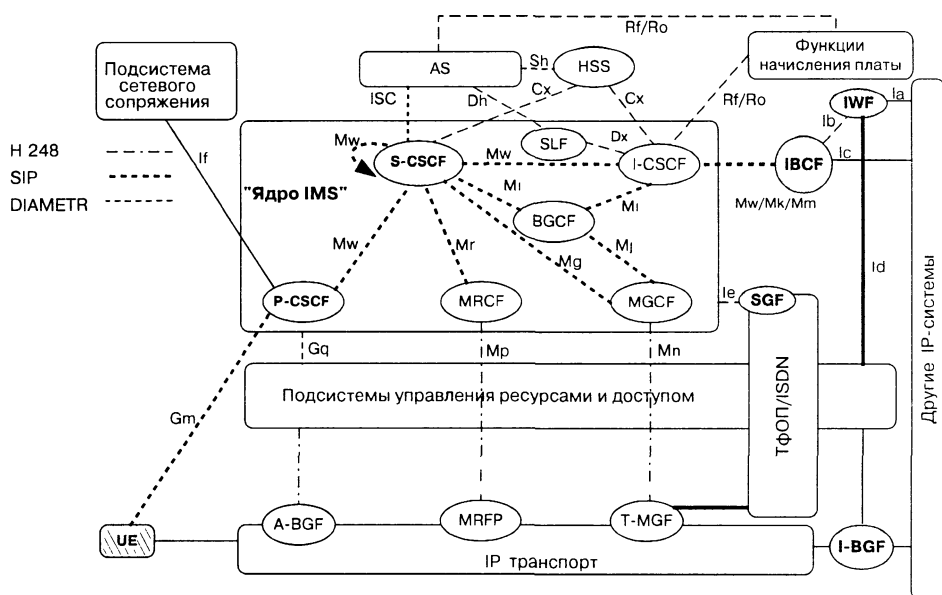


Рис. 11.12. Изменения структуры 3GPP IMS в проекте TISpan

Серым цветом показаны функциональные элементы, которые были определены проектом TISPAN, штриховкой отмечены элементы, подвергшиеся изменению, остальная структура IMS осталась прежней, как она описана в стандартах 3GPP.

Функция *IBCF (Interconnect Border Control Function)* обеспечивает полную управляемость на границе между сетями разных провайдеров. Она может содержать в себе THIG, выполняет согласование IPv4 и IPv6, может, в случае необходимости, обращаться к функции IWF, может управлять доступом и назначать полосу пропускания в соответствии с собственной политикой или обращаясь к подсистеме RACS.

Функция *IWF (Inter-Working Function)* обеспечивает взаимодействие протокола SIP сети IMS с сигнальными протоколами IP-сетей других провайдеров, такими как H.323 или другие реализации SIP.

Функция *I-BGF (Interconnect Border Gateway Function)* управляет передачей данных на 3 и 4 уровнях через границу провайдерских сетей. Эта функция играет роль межсетевого экрана и NAT, она защищает ядро сети провайдера, фильтруя пакеты на основании информации транспортного уровня. Она использует NAT для сокрытия транспортных адресов элементов ядра сети IMS.

Опциональными возможностями I-BGF являются: маркировка трафика в целях обеспечения QoS, реализация заданной политики управления шириной полосы пропускания и объемом сигнальной информации, измерение загрузки ресурсов и определение параметров QoS.

Различия между мобильными и стационарными сетями в плане реализации IMS в проекте выглядят следующим образом: существует разница в ширине полосы, безопасности, задержках при передаче; к терминалам стационарной сети предъявляются менее строгие требования (такие как поддержка IPv6, USIM/ISIM, некоторых кодеков); оборудование пользователя не должно хранить информацию о его местонахождении, в терминалах стационарной сети нет явного резервирования сетевых ресурсов; терминалы жестко не привязаны к пользователям; не реализуется сжатие сигнальной информации; индикация ширины полосы RTCP в SDP обычно не требуется; аутентификация производится без *UISC (Universal Integrated Service Card)*.

11.7. Вместо заключения

Для распространения идеологии IMS на стационарные сети связи, с которых начиналась эта книга, и для регулирования конвергенции стационарных и мобильных сетей крупными Операторами был создан FMCA-альянс (*Fixed-Mobile Convergence Alliance*), в который первоначально вошли British Telecom, Swisscom, NTT Com, Korea Telecom, Rogers Wireless и Brasil Telecom.

Ожидается, что широкое применение Softswitch и распространение IMS для конвергенции стационарных и мобильных сетей принесет существенные преимущества всем участникам рынка: пользователям, Операторам и провайдером услуг, а также производителям оборудования.

Этим, впрочем, не ограничиваются ожидания множества людей, занимающихся современными инфокоммуникациями, включая и авторов этой книги.

Ожидания грандиозные, частично пока еще остающиеся в области научной фантастики (как, например, телепортация), но частично начавшие осуществляться уже сегодня. И это начало столь впечатляюще, что авторам так и не удалось написать для этой книги раздел «Заключение», хотя они очень старались. Скорее всего, для сколько-нибудь осмысленного заключения время пока не пришло...

Литература

1. Варакин Л. Телекоммуникационный феномен России // Вестник связи International, 1999. — №4.
2. Гольдштейн А.Б. Устройства управления мультисервисными сетями: Softswitch. // Вестник связи, 2002. — №4.
3. Гольдштейн А.Б., Гольдштейн Б.С. Технология и протоколы MPLS — СПб.: БХВ – Санкт-Петербург, 2005.
4. Гольдштейн Б.С. Сигнализация в сетях связи. Том 1. 4-е изд. — СПб.: БХВ – Санкт-Петербург, 2005.
5. Гольдштейн Б.С. Протоколы сети доступа. Том 2. 3-е изд. — СПб.: БХВ – Санкт-Петербург, 2005.
6. Гольдштейн Б.С. Системы коммутации. Учебник для ВУЗов. 2-е издание, перераб. и доп. — СПб.: БХВ – Санкт-Петербург, 2004.
7. Гольдштейн Б.С., Ехриель И.М., Рерле Р.Д. Интеллектуальные сети — М.: Радио и связь, 2000.
8. Гольдштейн Б.С., Пинчук А.В., Суховицкий А.Л. IP-телефония — М.: Радио и связь, 2003.
9. Гольдштейн Б.С., Фрейнкман В.А. Call-центры и компьютерная телефония — СПб.: БХВ – Санкт-Петербург, 2002.
10. Гольдштейн Б.С., Зарубин А.В., Саморезов В.В. Протокол SIP. Справочник — СПб.: БХВ – Санкт-Петербург, 2005.
11. Гольдштейн Б.С., Ехриель И.М., Кадыков В.Б., Рерле Р.Д. Протоколы V5.1 и V5.2. Справочник — СПб.: БХВ – Санкт-Петербург, 2003.
12. Гольдштейн Б.С., Ехриель И.М., Рерле Р.Д. Стек OKC7. Подсистема ISUP. Справочник — СПб.: БХВ – Санкт-Петербург, 2003.
13. Журавлев С.В., Щербакова Е.Н. Применение технологии гибкой коммутации для реализации интеллектуальных услуг. // Информ Курьер Связь, 2003. — №3.
14. Зарубин А.А. Современные инфокоммуникационные услуги и концепция Open System Access. Методические рекомендации к практическим занятиям. СПб.: СПбГУТ им.проф. М.А. Бонч-Бруевича. — 2003.
15. Кульгин М. Технологии корпоративных сетей. — Изд. «Питер», 1999.
16. Ломакин Д. Технические решения IP-телефонии // Мобильные системы, 1999. — № 8.
17. Мюнх Б., Скворцова С. Сигнализация в сетях IP-телефонии. — Части I, II // Сети и системы связи, 1999. — №13(47), 14(48).
18. РД 45.046-99. «Аппаратура связи, реализующая функции передачи речевой информации по сетям передачи данных с протоколом IP. Технические требования» — 1999.

19. РД 45.079-99 «Оборудование связи, реализующее функции совместного узла коммутации и управления услугами SSCP платформы интеллектуальной сети связи. Общие технические требования» — 1999.
20. РД 45.080-99. «Аппаратура цифровых систем передачи абонентского доступа. Технические требования» — 1999.
21. РД 45.129-2000 «Телематические службы» — 2000.
22. РД 45.217-2001 «Технические спецификации ОКС 7. Книга 1 – Подсистема пользователя ЦСИС (ISUP) для национальной сети России (ISUP-R-2000)» — 2001.
23. РД. 45.302-2002 «Аппаратно-программные средства поддержки специализированных прикладных услуг CAMEL для абонентов федеральных сетей сотовой подвижной связи диапазонов 900/1800 МГц, работающих по стандарту GSM ФАЗА+2. Общие технические требования» — 2002.
24. РД. 45.333-2002 «Оборудование связи, реализующее функции гибкого коммутатора (Softswitch). Технические требования» — 2002.
25. Татенбам Э. Компьютерные сети. 4-е изд. — Сб.: Питер, 2005.
26. Уиллис Д. Хороший стандарт – плохой стандарт // Сети и системы связи, 1999. — №14.
27. Шнепс-Шнеппе М.А. NGN: Softswitch умирает. // Connect! Мир связи, 2003. — №5.
28. Шнепс-Шнеппе М.А. Архитектура OSA/PARLAY: от роуминга вызова к роумингу приложений // Мобильные системы, 2004 — № 4.
29. Шнепс-Шнеппе М.А. Протокол сигнализации SIP в сети 3G: нерешенные вопросы // Мобильные системы, 2005. — № 1.
30. 3GPP TS 23.107 V5.1.0. 3rd Generation Partnership Project: QoS Concept and Architecture (Release 5), 2001.
31. 3GPP TS 23.228 Stage 2. Service requirements for the IP Multimedia Core Network Subsystem.
32. 3GPP TS 24.229. IP Multimedia Call Control Protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP).
33. Alain Le Roux. Directions for TISPAN_NGN Project/ITU/ITC Regional Seminar on Network Evolution to Next Generation Networks and Fixed Mobile Convergence, Moscow, 27 – 30 April 2004.
34. Anquetil L-P., Bouwen J., Conte A., Van Doorselaer. B. Media Gateway Control Protocol and Voice over IP Gateway. – Alcatel Telecommunications Review, 2nd Quarter 1999.
35. Arlein R., Gurbani V. An Extensible Framework for Constructing Session Initiation Protocol User Agents Bell Labs Tech. J., 9:3 (2004), 87-100.
36. Armitage Grenville. Quality of Service in IP Networks. – Macmillan Technical Publishing, 2000.

37. Black Uyless. Voice Over IP. – Prentice Hall, 08/99. 0130224634.
38. Caputo R. Cisco Packetized Voice and Data Integration. – McGraw-Hill Cisco Technical Expert, 2000.
39. Collins Daniel. Carrier Grade Voice over IP. Second edition. – McGraw-Hill Cisco Technical Expert, 2000.
40. Comer D. Computer Networks and Internet. Upper Saddle River – Prentice-Hall, Inc., 1997.
41. Curtin P., Whyte B. Tigris – A gateway between circuit-switched and IP networks c Ericsson Review, 1999. — №2.
42. Davidson J., Peters J. Voice Over IP Fundamentals. – Cisco Press, 2000.
43. DeMartino K. ISDN and Internet. – Computer Networks, 1999.
44. Douskalis B. IP Telephony. The Integration of Robust VoIP Services. – Prentice Hall, 1999.
45. draft-ietf-sigtran-sua-14.txt. Signaling Connection Control Part User Adaptation Layer SUA, 2002.
46. draft-ietf-sigtran-v5ua-03.txt. V5.2-User Adaptation Layer V5UA , 2002.
47. Durham D., Yavatkar R.. Inside the Internet's Resource Reservation Protocol: Foundations for Quality of Service, 2000.
48. Emako B., Glitho R.H., Pierre S. A Mobile Agent based Advanced Service Architecture for Wireless Internet Telephony: Design, Implementation and Evaluation // IEEE Transactions on Computers. Vol. 52, No.6, June 2003.
49. Faynberg I., Gabuzda L., Lu Hui-Lan. Converged Networks and Services: Internetworking IP and PSTN. – John Wiley & Sons, 2000.
50. Garcia-Martin M. 3rd-Generation Partnership Project (3GPP) Release 5 Requirements on the Session Initiation Protocol (SIP, IETF Internet Draft, Oct. 2002, <<http://www.ietf.org/Internet-drafts/draft-ietf-sipping-3gpp-r5-requirements-00.txt>>.
51. Glitho R. H. Alternatives to Today's IETF and ITU-T Advanced Service Architectures for Internet Telephony: IN and Beyond, Computer Networks 35 (2001), Elsevier, April 2001, pp. 551-563.
52. Glitho R. H., Khendek F., DeMarco A. Creating Value Added Services in Internet Telephony: An Overview and a Case Study on a High Level Service Creation Environment, // IEEE Transactions on Man, Cybernetics and Systems, Part C, Vol.33, No4, 2003, pp. 445 – 457.
53. Glitho R.H., Sylla K., Developing Applications for Internet Telephony: A Case Study on the Use of Parlay Call Control APIs in SIP Networks, // IEEE Network Magazine, May/June 2004, Vol. 18, No. 3, pp. 48 – 55.
54. Goncalves M. Voice Over IP Networks. – McGraw Hill Publishing, 1998.
55. Goralski W., Kolon M. IP Telephony. – McGraw Hill Publishing, 1999.

56. Gurbani V., Liu K. Session Initiation Protocol: Service Residency and Resiliency // Bell Labs Tech. J., 8:1 2003, 83-94.
57. Gurbani V., Chiang T.-C., Reid J. The Need for Third-Party Call Control // Bell Labs Tech. J., 7:1 2002, 41c46.
58. Hersent O, Gurle D., Petit Jean-Pierre. IP Telephony: Packet-Based Multimedia Communications Systems. – Addison-Wesley Pub Co, 2000.
59. Hilt V., Hofmann M., Approaches to implementing Services in the SIP Networks // Bell Labs Tech. J., 9:3 2004, 39–44.
60. Horak R. Communications systems & networks. Second Edition. – M Et T Books and IDG Books Worldwide, Inc., 2000.
61. Houghton T. F., Schloemer E. C., Szurkowski E. S., Weber W. P. A packet telephony gateway for public network operators. // Bell Laboratories, Lucent Technologies – U.S.A., XVI World Telecom Congress Proceeding, 1997.
62. International Softswitch Consortium. Reference Architecture, June 2002, v 1.2 Reference Architecture. San Ramon, CA: Softswitch Consortium, 2002.
63. Isenberg David. Rise of the Stupid Network // Computer Telephony, August 1997. p. 16-26.
64. ITU-T Recommendation E.164. Numbering Plan for the ISDN Era. — 1991.
65. ITU-T Recommendation E.860, Framework of a service level agreement — 2002.
66. ITU-T Recommendation G.711. General Aspects of Digital Transmission Systems: Terminal Equipments. Pulse Code Modulation of 3kHz Audio Channel. Geneva: International Telecommunications Union. 1988.
67. ITU-T Recommendation G.723.1: General Aspects of Digital Transmission Systems: Dual Rate Speech Coder for Multimedia Communications Transmitting at 5.3 and 6.3 kbit/s. Geneva: International Telecommunications Union. 1996.
68. ITU-T Recommendation G.726: General Aspects of Digital Transmission Systems: 40, 32, 24, 16 kbit/s Adaptive Differential Pulse Code Modulation (ADPCM). Geneva: International Telecommunications Union. 1990.
69. ITU-T Recommendation G.728: General Aspects of Digital Transmission Systems: Coding of Speech at 16 kbit/s using Low-Delay Code Excited Linear Prediction LD-CELP). Geneva: International Telecommunications Union. 1992.
70. ITU-T Recommendation G.729: General Aspects of Digital Transmission Systems: Coding of Speech at 8 kbit/s using Conjugate-Structure Algebraic-Code-Excited Linear-Prediction (CS-ACELP). Geneva: International Telecommunications Union. 1996.

71. ITU-T Recommendation H.225.0. Call signaling protocols and media stream packetization for packet-based multimedia communication systems. Geneva: International Telecommunications Union. 1998.
72. ITU-T Recommendation H.245. Control protocol for multimedia communication. Geneva: International Telecommunications Union. 1998.
73. ITU-T Recommendation H.248. Series H: Audiovisual and Multimedia Systems: Infrastructure of audiovisual services – Communication procedures: Gateway control protocol. Geneva: International Telecommunications Union. 2000.
74. ITU-T Recommendation H.248.1 Gateway Control Protocol: Version 2, May 2002, <<http://www.itu.int/rec/recommendation.asp?type=items&lang=E&parent=T-REC-H.248.1-200205-1>>.
75. ITU-T Recommendation H.320. Narrow-band Visual Telephone Systems and Terminal Equipment. Geneva: International Telecommunications Union. 1996.
76. ITU-T Recommendation H.321. Adaptation of H.320 Visual Telephone Terminals to B-ISDN Environments. Geneva: International Telecommunications Union. 1996.
77. ITU-T Recommendation H.322. Visual Telephone Systems and Terminal Equipment for Local Area Networks which Provide a Guaranteed Quality of Service. Geneva: International Telecommunications Union. 1996.
78. ITU-T Recommendation H.323: Infrastructure of audiovisual services – Systems and terminal equipment for audiovisual services: Packet-based multimedia communications systems. Geneva: International Telecommunications Union. 1999.
79. ITU-T Recommendation H.324. Terminal for Low Bit Rate Multimedia Communications. Geneva: International Telecommunications Union. 1996.
80. ITU-T Recommendation Q.700: Specifications of Signalling System No. 7: Introduction to CCITT Signalling System No. 7. Geneva: International Telecommunications Union. 1993.
81. ITU-T Recommendation Q.763: Specifications of Signalling System No. 7 – ISDN user part: Signalling System No. 7 – ISDN user part formats and codes. Geneva: International Telecommunications Union. 1997.
82. ITU-T Recommendation Q.931: Digital Subscriber Signalling System No. 1 – Network layer: ISDN user-network interface layer 3 specification for basic call control. Geneva: International Telecommunications Union. 1998.
83. Lee J. Implementing Voice Over IP. – McGraw Hill Text, 2000.
84. Luczywek M. Cisco Voice over IP Handbook. – IDG Books Worldwide, 2000.

85. McDysan D. Qos & Traffic Management in Ip & Atm Networks. – McGraw Hill, 2000.
86. Miller M. Voice over IP: Strategies for the Converged Network. – IDG Books Worldwide, 2000.
87. Minoli D., Minoli E. Delivering Voice over IP Networks – John Willey & Sons, Inc., 1998.
88. Multiparty Multimedia Session Control Working Group (MMUSIC) Minutes from the 37th IETF Meeting, Dec. 9-10, 1996, San Jose, CA, <http://www.ietf.org/ietf/mmusic-minutes-96dec.txt>.
89. Multiparty Multimedia Session Control Working Group (MMUSIC) Minutes from the 35th IETF Meeting, Mar. 4-8, 1996, Los Angeles, CA, [http://www.ietf.org/proceedings/96 mar/area.and.wg.reports/tsv/mmusic-minutes-96mar.html](http://www.ietf.org/proceedings/96%20mar/area.and.wg.reports/tsv/mmusic-minutes-96mar.html).
90. Multiservice Switching Forum MSF-ARCH-001.00-FINAL-1A. System Architecture Implementation Agreement, May, 2000.
91. Regis B., Donald G. Voice & Data Communications Handbook Third Edition. – McGraw Hill Publishing, 2000.
92. Reid M. Multimedia conferencing over ISDN and IP networks using ITU-T H-series recommendations: architecture, control and coordination/Computer Networks, 1999. — №31.
93. RFC 0768. Postel, J. User Datagram Protocol, 1980.
94. RFC 1006, M. Rose, D. Cass. ISO Transport Service on Top of the TCP, Version: 3, IETF May 1987, <[http://www.ietf.org/rfc/rfc1006.txt? number=1006](http://www.ietf.org/rfc/rfc1006.txt?number=1006)>.
95. RFC 1631 Egevang K., Francis P. The IP Network Address Translator (NAT), IETC, May 1994, <<http://www.ietf.org/rfc/rfc1631.txt>>.
96. RFC 1777. Lightweight Directory Access Protocol. Yeong, W., T. Howes, S. Kille. Internet Engineering Task Force. 1995. Retrieved December 25, 2002.
97. RFC 2205. Resource Reservation Protocol (RSVP). Ver.1. Functional Specification. — September 1997.
98. RFC 2327 Handley M., Jacobson V. SDP: Session Description Protocol, IETF, Apr. 1998, <<http://www.ietf.org/rfc/rfc2327.txt>>.
99. RFC 2543. Handley M., Schulzrinne H., Schooler E., Rosenberg J. SIP: Session Initiation Protocol. — March 1999.
100. RFC 2570. Case J., Mundy R., Partain D., Stewart B. Introduction to Version 3 of the Internet-standard Network Management Framework, 1999.
101. RFC 2616. Hypertext Transfer Protocol – HTTP/1.1. Fielding R., Gettys J., Mogul J., Frystyk H., Masinter L., Leach P., Berners-Lee T. – June 1999.

102. RFC 2705. Media Gateway Control Protocol (MGCP) Version 1.0. M. Arango, A. Dugan, I. Elliott, C. Huitema, S. Pickett. — October 1999.
103. RFC 2833. RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals. May 2000.
104. RFC 2865. Remote Authentication Dial In User Service (RADIUS). C. Rigney, S. Willens, A. Rubens, W. Simpson. June 2000.
105. RFC 2885. Megaco Protocol 0.8. F. Cuervo, N. Greene, C. Huitema, A. Rayhan, B. Rosen, J. Segers. August 2000.
106. RFC 2960 Stream Control Transmission Protocol. May 2004.
107. RFC 2974 Session Announcement Protocol, M. Handley, C. Perkins, E. Whelan, IETF, Oct. 2000, <<http://www.ietf.org/rfc/rfc2974.txt>>.
108. RFC 2976 The SIP INFO Method, S. Donovan, IETF, Oct. 2000, <<http://www.ietf.org/rfc/rfc2976.txt>>.
109. RFC 3015. Megaco Protocol Version 1.0. Cuervo, F., N. Greene, A. Rayhan, C. Huitema, B. Rosen, J. Segers, 2000.
110. RFC 3057. ISDN Q.921-User Adaptation Layer. 2001.
111. RFC 3086. Definition of Differentiated Services Per Domain Behaviors and Rules for their Specification. Nichols, K., B. Carpenter, 2001.
112. RFC 3204. MIME media types for ISUP and QSIG Objects. 2001.
113. RFC 3235 Network Address Translator (NAT)-Friendly Application Design Guidelines, D. Senie, IETF Jan. 2002, <<http://www.ietf.org/rfc/rfc3235.txt>>.
114. RFC 3621 Session Initiation Protocol (SIP), J. Rosenberg, H. Schulzrinne, J. Peterson, G. Camarillo, R. Sparks, M. Handley, and E. Schooler. June 2002, <<http://www.ietf.org/rfc/rfc3621.txt>>.
115. RFC 3265 Session Initiation Protocol (SIP)-specific event notification, A. Roach, IETF June 2002, <<http://www.ietf.org/rfc/rfc3265.txt>>.
116. RFC 3331. Signaling System 7 (SS7) Message Transfer Part 2 (MTP2) – User Adaptation Layer). September 2002.
117. RFC 3332. Signaling System 7 (SS7) Message Transfer Part 3 (MTP3) – User Adaptation Layer (M3UA), 2002.
118. RFC 3372. Session Initiation Protocol for Telephones (SIP-T): Context and Architectures, 2002.
119. RFC 3398 Integrated Services Digital Network (ISDN) User Part (ISUP) to Session Initiation Protocol (SIP) Mapping), 2002.
120. RFC 3428 Session Initiation Protocol Extensions for Instant Messaging, 2003.
121. RFC 3455 Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd Generation Partnership Project (3GPP), M. Garcia-Martin, E. Henrikson, D. Mills, IETF, Jan. 2003, <<http://www.ietf.org/rfc/rfc3455.txt>>.

122. RFC 3550 RTP: A Transport for Real-Time Applications, H. Schulzrinne, S. Casner, R. Frederick, V. Jacobson, IETF July 2003, <<http://www.ietf.org/rfc/rfc3550.txt>>.
123. RFC 3581 An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing, J. Rosenberg, H. Schulzrinne, IETF Aug. 2003, <<http://www.ietf.org/rfc/rfc3581.txt>>.
124. RFC 3611 RTP Control Protocol Extended Reports (RTCP XR) T. Friedman, Ed, November 2003.
125. RFC 3714 IAB Concerns Regarding Congestion Control for Voice Traffic in the Internet, March 2004.
126. Stanwyck, D. Profitably Deploying Services in the Next Generation Network. Voice-on-the-Net Japan, 2002. Tokyo: Key3Media.
127. Tang J., White T., Pagurek B., Glitho R. H. Advanced service architecture for H.323 Internet Telephony Protocol, Computer Communications, Elsevier, April 2000, Vol.23, No8, pp. 740-753.
128. Toga J., Ott J. ITU-T standardization activities for interactive multimedia communications on packet-based networks: H.323 and related recommendations/Computer Networks, 1999.
129. Uyless Black. Voice over IP – Prentice Hall PTR, 2000.
130. Walter J. Goralski, Matthew C. Kolon. IP telephony – The McGraw-Hill Co., Inc., 2000.
131. www.niits.ru

Глоссарий

2G	2nd Generation systems. Системы мобильной связи 2-го поколения.
3G	3d Generation systems. Системы мобильной связи 3-го поколения.
3GPP	3G Partnership Project UMTS. Проект универсальной системы подвижной связи объединения 3GPP.
AAA	Authentication, Authorization, and Accounting. Функции аутентификации, авторизации и учета (IETF).
ABNF	Augmented Backus-Naur Form. Форма Бэкуса-Наура.
ADSL	Asymmetric Digital Subscriber Line. Асимметричная цифровая абонентская линия.
A-F	Accounting Function. Функции учета стоимости сеансов связи.
AG	Access Gateway. Шлюз доступа.
AGS-F	Access Gateway Signaling Function. Функциональный объект сигнализации шлюза доступа (IPCC).
ALG	Application Layer Gateway. Шлюз уровня приложений.
AN	Access Network. Сеть доступа.
ANSI	American National Standards Institute. Американский национальный институт стандартов.
API	Application Programming Interface. Интерфейс прикладного программирования
ARIB	Association of Radio Industries and Businesses. Ассоциация радиопромышленности и бизнеса.
AS	Application server. Сервер приложений.
AS-F	Application Server Function. Функциональный объект сервера приложений (IPCC).
ASP	Application Server Process. Процесс сервера приложений.
ATM	Asynchronous Transfer Mode. Асинхронный режим переноса информации.
AuC	Authentification Center. Центр аутентификации.
AVT	Audio/Video Transport. Группа транспортировки аудио/видео информации (AEFT)
BCF	Bearer Control Function. Функции управления носителем (BICC).
BC-IWF	Bearer Control Interworking Function. Функции взаимодействия BCF, использующих разные протоколы (BICC).

BER	Basic Encoding Rules. Основные правила шифрования.
BGCF	Breakout Gateway Control Function. Сервер, выполняющий функции управления пограничным шлюзом (IMS).
BHCA	Busy Hour Call Attempts. Число вызовов в ЧНН.
BICC	Bearer Independent Call Control. Протокол управления обслуживанием вызова, независимый от носителя (Q.1901 ITU-T).
B-ISDN	Broadband ISDN. Широкополосная ISDN.
BIWF	Bearer InterWorking Function. Функции взаимодействия внутри SN (BICC).
BRN	Bearer Relay Node. Узел ретрансляции носителя (BICC).
BSSAP	Base Station Subsystem Application Part. Прикладная подсистема системы базовых станций (GSM, 3GPP).
CA	Call Agent. Устройство управления соединениями.
CAC	Call Admission Control. Управление допуском вызова к обслуживанию.
CA-F	Call Agent Function. Функциональный объект CA (IPCC).
CAG	Core Access Gateway. Шлюз доступа к транзитной IP-сети.
CAMEL	Customized Applications for Mobile Network Enhanced Logic (GSM). Настраиваемое программное приложение для предоставления интеллектуальных услуг в сетях мобильной связи стандарта GSM.
CAP	CAMEL Application Part. Подсистема ОКС 7 для обеспечения приложений CAMEL (GSM, 3GPP).
CAS	Channel Associated Signaling. Сигнализация по выделенным сигнальным каналам.
CBR	Constant Bit Rate. Постоянная скорость передачи битов.
CC	Content of Communication. Контент связи.
CDMA	Code Division Multiple Access. Множественный доступ с кодовым разделением каналов.
CDR	Call Detail Record. Запись подробной учетной информации о вызове.
CIC	Channel Identification Code. Код идентификации канала (ОКС7).
CLIP	Calling Line Identification Presentation. Предоставление номера вызывающей линии.
CLIR	Calling Line Identification Restriction. Запрет идентификации вызывающей линии.
CNG	Comfort Noise Generator. Генератор комфортного шума.

CORBA	Common Object Request Broker Architecture. Архитектура брокера запросов к объектам.
COPS	Common Open Policy Service. Протокол взаимодействия серверов сетевой политики (например, RSVP-маршрутизатор).
CPE	Customer Premise Equipment. Оборудование в помещении абонента.
CPL	Cambridge Programming Language. Кэмбриджский язык программирования.
CSCF	Call/Session Control Function. Функции управления сеансами.
CS-i	Capabilities Set. Набор функциональных возможностей №1.
CSF	Call Service Function. Функции обслуживания вызовов (BICC).
CSRC	Contributing source. Информационный источник.
CWTS	China Wireless Telecommunication Standard Group. Китайская Группа стандартизации беспроводной связи.
Diameter	Протокол аутентификации и учета.
DiffServ	Differentiated Services. Система дифференцированного обслуживания трафика разных классов.
DHCP	Dynamic Host Configuration Protocol. Протокол динамической конфигурации хоста.
DNS	Domain Name System. Система имен доменов. Прикладной протокол для связи с этой системой.
DPC	Destination Point Code. Код пункта назначения (ОКЧ7).
DPNSS	Digital Private Network Signaling System. Система сигнализации для частных цифровых сетей.
DS0	Digital Signal of level 0. Цифровой сигнал уровня 0, т.е. канал 64 Кбит/с.
DSL	Digital Subscriber Line. Цифровая абонентская линия.
DSLAM	DSL Access Multiplexer. Мультиплексор доступа DSL.
DSP	Digital Signal Processor. Процессор цифровой обработки сигналов.
DSS1	Digital Signaling System 1. Цифровая система сигнализации в доступе ISDN пользователь-сеть.
DTMF	Dual Tone Multiple Frequency. Многочастотная система «2 из n» для кодирования цифр номера.
DTX	Discontinuous Transmission. Прерывистая передача (подавление периодов молчания). Используется для экономии полосы пропускания.
E-DSS1	Европейская версия DSS1.

ENUM	E.164 Numbering (IETF RFC 2916). План нумерации E.164.
ETSI	European Telecommunications Standards Institute. Европейский институт стандартов в области связи.
FDM	Frequency Division Multiplexing. Мультиплексирование с частотным разделением каналов.
FEC	Forwarding Equivalence Class. Класс эквивалентности пере-сылки (MPLS).
FISU	Fill-In Signal Unit. Заполняющая сигнальная единица (ОКС7).
FMC	Fixed-Mobile Convergence. Конвергенция стационарных и мо-бильных сетей и услуг.
FMCA	Fixed-Mobile Convergence Alliance. Объединение по вопросам конвергенции стационарных и мобильных сетей.
FR	Frame Relay. Режим переноса информации путем ретрансля-ции кадров.
FTP	File Transfer Protocol. Протокол переноса файлов.
FTTx	Fiber-To-The-x, x=Building, Curb, Desk, Home etc. Оптоволокну до здания, до тротуара, до столба, до дома и т.п.
GGSN	Gateway GPRS Support Node. Узел поддержки шлюза GPRS.
GII	Global Infocommunication Infrastructure. Глобальная инфоком-муникационная инфраструктура.
GK	Gatekeeper. Привратник. Устройство управления в сетях H.323.
GPRS	General Packet Radio Service. Услуга пакетной передачи дан-ных через радиointерфейс.
GSM	Global System for Mobility. Общеввропейский стандарт мо-бильной связи.
GSN	Gateway Serving Node. Пограничный узел обслуживания.
GTT	Global Title Translation. Преобразование глобального адреса.
HFC	Hybrid Fiber/Coax. Комбинированная оптико-коаксиальная сеть.
HLR	Home Location Register. Домашний регистр местоположения пользователя (GSM, 3GPP).
HSS	Home Subscriber Server. Сервер абонентов домашней сети.
HTTP	Hypertext Transport Protocol. Гипертекстовой транспортный протокол (IETF).
IAD	Integrated Access Device. Устройство интегрированного доступа.
IANA	Internet Assigned Numbers Authority. Администрация адресно-го пространства Интернет.

I-BCF	Interconnect Border Control Function. Функции управления на границе между сетями разных провайдеров (TISPAN).
I-BGF	Interconnect Border Gateway Function. Функции шлюза на границе между сетями разных провайдеров (TISPAN).
ICQ	«I seek you». «Я ищу тебя». Система мгновенного обмена сообщениями.
IETF	Internet Engineering Task Force. Группа инженерных проблем Интернет.
IMS	IP Multimedia Subsystem. IP-подсистема мультимедийной связи.
IMSI	International Mobile Subscriber Identifier. Международный идентификатор мобильного абонента.
IM-SSF	IP Multimedia Service Switching Function. Сервер, выполняющий функции коммутации мультимедийных IP-услуг и используемый IMS.
IN	Intelligent Network. Интеллектуальная сеть.
INAP	Intelligent Network Application Protocol. Прикладной протокол IN (стек протоколов ОКС7).
IP	Internet Protocol. Протокол межсетевой связи. Протокол сети Интернет.
IPBCP	IP Bearer Control Protocol. Протокол управления IP-носителем (BICC).
IPCC	International Packet Communication Consortium. Международный консорциум по вопросам пакетной связи (бывший ISC).
IPDC	Internet Protocol Device Control. Интернет-протокол управления устройствами.
IRI	Intercept Related Information. Информация, связанная с перехватом.
ISC	International Softswitch Consortium. Международный консорциум Softswitch (теперь IPCC).
ISDN	Integrated Services Digital Network. Цифровая сеть интегрального обслуживания.
ISIM	IP Multimedia Services Identity Module. Модуль идентификации мультимедийных IP-услуг (3GPP).
ISM	Interconnection and Switching Module. Модуль взаимодействия и коммутации.
ISN	Interface Serving Node. Интерфейсный узел обслуживания (BICC).
ISP	Internet Service Provider. Провайдер услуг Интернет.

ISUP	Integrated Services Digital Network User Part. Подсистема-пользователь услугами MTP и SCCP, поддерживающая сигнализацию ISDN (OKC7).
ITU	International Telecommunications Union. Международный союз электросвязи.
ITU-T	International Telecommunication Union – Telecommunications Standardization Sector. Сектор стандартизации электросвязи ITU.
IUA	ISDN User Adaptation. Протокол адаптации протокола SCTP к протоколу DSS1.
IVR	Interactive Voice Response. Интерактивная речевая система.
IW-F	Interworking Function. Функциональный объект взаимодействия (IPCC).
IWU	Interworking Unit. Модуль взаимодействия BICC с SIP.
JAIN	Java Application Intelligent Network. Открытый интерфейс прикладного программирования для реализации приложений на сетях операторов связи.
JTAPI	Java Telephony Application Programming Interface. Интерфейс программирования CTI приложений на языке JAVA.
LAN	Local Area Network. Локальная вычислительная сеть.
LDAP	Lightweight Directory Access Protocol. Облегченный протокол доступа к сетевому каталогу (IETF).
LD-CELP	Low delay code excited linear prediction. Линейное предсказание с малой задержкой.
LDP	Label Distribution Protocol. Протокол распределения меток (MPLS).
LEA	Law Enforcement Agency. Организация, имеющая законное право доступа к частной информации.
LEC	Local Exchange Carrier. Оператор местной связи.
LI	Lawful Interception. Законный перехват информации.
LI AF	Lawful Intercept Admin Function. Административные функции законного перехвата.
LSP	Label Switched Path. Коммутируемый по меткам тракт (MPLS).
LSR	Label Switching Router. Маршрутизатор коммутации по меткам (MPLS).
LSSU	Link Status Signal Unit. Сигнальная единица состояния звена (OKC7).
M2PA	MTP2 Peer-to-Peer Adaptation Layer. Уровень адаптации SCTP к MTP3 для случая взаимодействия между объектами одного ранга (IETF Sigtran).

M2UA	MTP2-User Adaptation Layer. Уровень адаптации SCTP к MTP3 для случая взаимодействия между объектами разных рангов (IETF Sigtran).
M3UA	MTP3 User Adaptation. Уровень адаптации SCTP к тем протоколам OKC7, которые являются пользователями MTP3 (IETF Sigtran).
MAN	Metropolitan Area Network. Региональная вычислительная сеть.
MAP	Mobile Application Part. Прикладная подсистема подвижной связи (OKC7).
MA-F	Mozilla Archive Format. Мастер файл. Архив Mozilla
MC	Multipoint Control. Multipoint Controller. Управление конференциями. Контроллер управления конференциями.
MCU	Multipoint Control Unit. Устройство управления конференциями.
MD	Mediation Device. Посредник CORM.
MEGACO	Media Gateway Control. Протокол управления транспортным шлюзом (IETF RFC 3015 или ITU H.248).
MG	Media Gateway. Транспортный шлюз (медиашлюз).
MGC	Media Gateway Controller. Контроллер транспортных шлюзов (медиашлюзов).
MGC-F	Media Gateway Controller Function. Функциональный объект контроллера транспортных шлюзов (IPCC).
MGCP	Media Gateway Control Protocol. Протокол управления транспортными шлюзами (IETF RFC 2705).
MG-F	Media Gateway Function. Функциональный объект транспортного шлюза (IPCC).
MMUSIC	Multiparty Multimedia Session Control. Управление мультимедийным сеансом многосторонней связи.
MMSF	Media mapping and switching function. Функции мэппинга и коммутации (BICC).
MOS	Mean Opinion Score. Среднее значение оценки экспертов, которую каждый из них выразил по пятибалльной системе.
MP3	MPEG Layer 3. MPEG, или Motion Picture Expert Group – организация, разрабатывающая форматы сжатия мультимедийной информации.
MP	MC processor. Процессор управления конференциями.
MPLS	Multiprotocol Label Switching. Многопротокольная коммутация по меткам.
MPS	Multiple Payload Stream. Поток с полезной нагрузкой разных видов.

MRF	Media Resource Function. Функция медиаресурсов .
MS	Media Server. Транспортный сервер (медиасервер).
MSC	Mobile Services Switching Center. Центр коммутации подвижной связи (GSM, 3GPP).
MSF	MultiService Forum – форум мультисервисной коммутации.
MS-F	Media Server Function. Функциональный объект транспортно-го сервера (IPCC).
MSISDN	Mobile Subscriber ISDN Number. ISDN-номер мобильного абонента.
MSU	Message Signal Unit. Значащая сигнальная единица (ОКС7).
NAPT	Network Address Port Translation. Преобразователь номеров портов.
NASS	Network Attachment Subsystem. Подсистема привязки к сети иного типа.
NAT	Network Address Translator. Преобразователь сетевых адресов.
NFAS	Non-Facility Associated Signaling. Сигнализация, не связанная с устройством.
NGN	Next-Generation Network. Сеть следующего поколения.
NWO/AP/ SvP	NetWork Operator/Access Provider/Service Provider. Оператор сети/ провайдер доступа/услуг.
OMA	Open Mobile Alliance. Открытый союз организаций мобильной связи.
OMS	Operation and Management Supervisor. Модуль эксплуатационного управления.
OPM	Optical Peripheral Module. Оптический периферийный модуль.
OSA	Open Service Architecture. Открытая архитектура создания услуг.
OSI	Open Systems Interconnection. Взаимодействие открытых систем.
OSS	Operation Support System. Система эксплуатационной поддержки.
PARLAY	Открытый интерфейс прикладного программирования для создания инфокоммуникационных услуг/приложений.
PC	Personal Computer. Персональный компьютер.
PCM	Pulse Code Modulation. Импульсно-кодовая модуляция – ИКМ.
PDD	Post-Dial Delay. Время ожидания после набора номера.
PES	PSTN/ISDN Emulation Subsystem (ETSI).
PDF	Policy Decision Function. Функция принятия решений на основе известной ей политики.
PHS	Protocol Handler Server. Сервер обработки протоколов.

PINT	PSTN and Internet Interworking. Взаимодействие ТФОП и Интернет.
PLMN	Public Land Mobile Network. Сеть сотовой подвижной связи (3GPP, UMTS).
PoP	Point of Presence. Точка присутствия.
POTS	Plain Old Telephone Service. Услуги традиционной телефонии.
RADIUS	Remote Access Dial-In User Service. Протокол аутентификации и учета при удаленном доступе пользователя.
RACS	Resource and Admission Control Subsystem (ETSI).
RAN	Radio Access Network. Беспроводные сети доступа.
RANAP	Radio Access Network Application Protocol. Прикладной протокол RAN.
RAS	Registration, Admission & Status protocol. Протокол регистрации, допуска и определения статуса (H.323).
RFC	Request For Comment. Выпускаемые IETF документы, определяющие устройство Интернет-стандартов, инструкций, отчетов рабочих групп и т.д.
R-F	Routing Function. Функции маршрутизации.
RS-F	Redirect Server Function. Функции сервера перенаправления.
RSVP	Resource Reservation Protocol. Протокол резервирования ресурсов (IETF).
RTCP	Real-Time Control Protocol. Протокол контроля транспортировки информации в реальном времени (IETF).
RTP	Real-Time Transport Protocol. Протокол транспортировки информации в реальном времени (IETF RFC 1889).
RTSP	Real-Time Streaming Protocol. Протокол поточной передачи в реальном времени.
SAP	Session Announcement Protocol. Протокол объявления сеансов связи. Service Access Point. Точка доступа к услуге (BICC).
SAU	Subscriber Access Unit. Модуль абонентского доступа.
SBC	Session Border Controller. Пограничный контроллер сеансов связи.
SCCP	Signaling Connection Control Part. Подсистема управления сигнальными соединениями (ОКС7).
SC-F	Service Control Function. Функции управления услугами.

SCIP	Simple Conference Invitation Protocol. Простой протокол приглашения к конференции.
SCP	Service Control Point. Узел управления услугами (IN).
SCS	Service Capability Server. Сервер приложений, используемый IMS.
SCTP	Stream Control Transmission Protocol. Протокол передачи с управлением потоками.
SDP	Session Description Protocol. Протокол описания сеансов связи.
SEG	Security Gateway. Шлюз безопасности (IMS).
SET	Simple Endpoint Type. Упрощенный терминал пользователя.
SG	Signaling Gateway. Шлюз сигнализации.
SGCP	Signaling Gateway Control Protocol. Протокол управления сигнальными шлюзами.
SG-F	Signaling Gateway Function. Функциональный объект шлюза сигнализации (ISC).
SGSN	Serving GPRS Support Node. Обслуживающий узел GPRS.
SIGTRAN	Signaling Transport. Транспортировка сигнальной информации согласно IETF M3UA, IUA, SUA, V5UA Drafts. Название рабочей группы.
SIM	Subscriber Identity Module. Модуль идентификации абонента.
SIP	Session Initiation Protocol. Протокол инициирования сеансов связи (IETF).
SIP-T	SIP for Telephony. Протокол SIP для телефонной связи.
SLA	Service Level Agreement. Соглашение о качестве обслуживания.
SLF	Subscriber Location Function. Функция определения местоположения абонента.
SLS	Signaling Link Selection. Селектор сигнального звена (OKC7).
SMTP	Simple Mail Transport Protocol. Простой протокол транспортировки почты.
SN	Serving Node. Узел обслуживания (BICC).
SNMP	Simple Network Management Protocol. Простой протокол эксплуатационного управления сетью.
SP	Signaling point. Пункт сигнализации (OKC7).
SPAN	Services and Protocols for Advanced Networking. Услуги и протоколы для перспективных сетей
SPINS	Softswitch Platform for Intelligent Network. Платформа Soft-switch для IN.

SPIRITS	Service in the PSTN/IN Requesting Internet Service. Услуга запроса из ТфОП/IN услуг Интернет.
SPS-F	SIP Proxy Server Function. Функциональный объект прокси-сервера SIP (ISC).
SPVC	Semi-Permanent Virtual Connection. Полупостоянное виртуальное соединение.
SS7	Signaling System 7. Система общеканальной сигнализации №7 – (ОКС7).
SSL	Secure Sockets Layer. Протокол защиты данных, пересылаемых между Web-браузерами и Web-серверами.
SSP	Service Switching Point. Узел коммутации услуг (IN).
STC	Signaling Transport Converter. Функции преобразования транспортируемой сигнальной информации.
STP	Signaling Transfer Point. Транзитный пункт сигнализации (ОКС7).
STUN	Simple Traversal of UDP Through NAT. Простой протокол проведения UDP через NAT.
SU	Switching Unit. Коммутационный модуль.
SUA	SCCP User Adaptation. Адаптация SCTP к SCCP (IETF Sigtran).
SVC	Switched Virtual Connection. Коммутируемое виртуальное соединение.
SVI	Status Verification Interface. Интерфейс верификации статуса.
SYN-attack	Непрерывные злонамеренные попытки создать TCP-соединение с атакуемым объектом с целью истощить его ресурсы.
SWN	Switching Node. Коммутирующий узел (BICC).
TAR	Temporary Alternative Route. Временный альтернативный маршрут (BICC).
TCAP	Transaction Capabilities Application Part. Подсистема поддержки транзакций (ОКС7).
TCP	Transmission Control Protocol. Протокол управления передачей.
TDM	Time Division Multiplexing. Мультиплексирование с временным разделением каналов.
TE	Terminal Equipment. Терминал пользователя, соответствующий стандарту DSS1.
TG	Trunk Gateway. Шлюз между сетью ТфОП и сетью IP.
THIG	Topology Hiding Inter-network Gateway. Межсетевой шлюз сокрытия топологии.

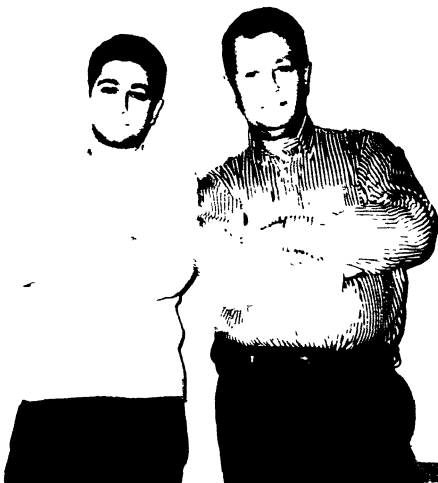
TIPI	Telecommunications and Information Policy Institute. Институт телекоммуникций и информационной политики.
TIPHON	Рабочая группа IETF.
TISPAN	Telecommunication and Internet converged Services and Protocols for Advanced Networking. Конвергентные телекоммуникационные и Интернет услуги и протоколы.
TLS	Transport Layer Security. Протокол, обеспечивающий безопасность на транспортном уровне.
TLV	Type-length-value. Тип-длина-значение (конструкция, используемая в форматах параметров сообщений, например, в протоколе LDP).
TRIP	Telephone Routing through IP. Телефонная маршрутизация через сеть IP.
TSAP	Transport Service Application Point. Точка доступа к транспортным услугам.
TSN	Transmission Sequence Number. Порядковый номер передачи (Sigtran).
TSN	Transit Serving Node. Транзитный узел обслуживания (BICC).
TUA	TCAP User Adaptation. Адаптация SCTP к TCAP (IETF Sigtran).
TURN	Traversal Using Relay NAT. Протокол переноса с использованием NAT.
UA	User Agent. Агент пользователя.
UAC	User Agent Client. Агент пользователя – клиент.
UAS	Usr Agent Server. Агент пользователя – сервер.
UDP	User Datagram Protocol. Протокол передачи дейтаграмм пользователя.
UICC	Universal Integrated Circuit Card. Универсальная идентификационная карта.
UMTS	Universal Mobile Telecommunications Systems. Универсальная система мобильной связи.
UPL	Upper Layer protocol. Протокол верхнего уровня (IETF Sigtran).
URI	Universal Resource Identificator. Универсальный идентификатор ресурса.
URL	Uniform Resource Locator. Унифицированный указатель ресурса.
USIM	Universal Subscriber Identity Module. Модуль универсальной идентификации абонента.
V5	Open access network protocol. Открытый протокол сети доступа.

V5UA	V5 User Adaptation. Адаптация SCTP к V5 (IETF Sigtran).
VAD	Voice Activity Detection. Детектор активных периодов речи.
VBR	Variable Bit Rate. Переменная скорость передачи битов.
VLR	Visitor Location Register. Гостевой регистр местоположения (GSM, 3GPP).
VoATM	Voice over ATM. Технология передачи речевой информации по сети ATM.
VoDSL	Voice over DSL. Технология передачи речевой информации по DSL.
VoIP	Voice over IP. Технология передачи речевой информации по IP-сети.
VTCH	Virtual Termination Call Handler. Модуль обработки вызовов в виртуальных линейных окончаниях.
WAP	Wireless Application Protocol. Прикладной протокол беспроводной связи.
WCDMA	Wireless Code Division Multiple Access. Беспроводный множественный доступ с кодовым разделением каналов.
WLAN	WireLess Access Network. Сеть беспроводного доступа.
WLL	WireLess Loop. Беспроводная абонентская линия.
XML	Extensible Markup Language. Расширяемый язык разметки.
WiMax	Worldwide Interoperability for Microwave Access. Международное взаимодействие по микроволновому доступу.

Предметный указатель

- 3**
 - 3G, 7, 12, 29, 84, 233, 274, 305, 318, 324, 350
 - 3GPP, 7, 12, 84, 317-322, 324-326, 335, 337-341, 344, 345, 345, 350
- A**
 - AAA, 31, 290, 350
 - ADSL, 255, 338, 350
 - A-F, 30-32, 35-38, 147, 350
 - AG, 234, 235, 301, 350
 - AGS-F, 30, 32, 33, 350
 - ALG, 64, 350
 - AN, 236, 350
 - ANSI, 240, 284, 307, 350
 - API, 16, 26, 28, 31, 37, 245-247, 250, 270, 284, 289, 295, 331, 350
 - AS, 182, 184, 188, 234, 242, 330, 331, 350
 - AS-F, 30-34, 37
 - ASP, 182-184, 186, -189, 191, 193, 350
 - ATM, 17, 32, 34, 118, 122, 162, 198-200, 203, 201, 221, 230, 285, 290, 348
 - AvT, 40
 - Aus, 32, 38, 325, 352
- B**
 - BCF, 200-202, 207, 217, 218, 227, 229
 - BC-IWF, 226
 - BGCF, 8, 332
 - BHCA, 299, 300, 302
 - BICC, 6, 18, 32, 82, 117, 197-132, 234, 285, 290, 303, 393, 359-362
 - B-ISDN, 40, 347
 - BIWF, 352, 201, 202, 207, 217-219, 223, 227, 230
 - BRN, 200, 352
- C**
 - CA, 50, 117, 282, 301
 - CAC, 267, 352
 - CA-F, 30, 31, 35-38, 352
 - CAG, 244, 245, 352
 - CAMEL, 290, 294, 331, 344, 352
 - CAP, 31-38, 331, 352
 - CAS, 63, 129, 150, 291, 299, 307, 352
 - CC, 253, 254, 352
 - CDMA, 352
 - CDR, 242, 275, 276, 299, 301, 307, 310, 311, 352
 - CIC, 179, 182, 184, 188, 210, 211, 214, 227, 352
 - CLIP, 205, 293, 339, 352
 - CLIR, 205, 293, 339, 352
 - CNG, 45, 47, 151, 352
 - CORBA, 246, 247, 291, 301, 309, 353
 - COPS, 245, 268, 270, 320, 353
 - CSCF, 325-331, 334, 353
 - CS-i, 17, 18, 198-202, 203, 206, 207, 214-221, 223, 226, 230, 288, 303, 353
 - CSF, 200-202, 206-211, 217, 219, 222, 227, 229, 353
 - CWTS, 353, 318
- D**
 - Diameter, 320, 327, 329, 353
 - DiffServ, 22, 272, 276, 353
 - DHCP, 338, 353
 - DNS, 58, 64, 84, 320, 328, 329, 354
 - DPC, 182, 184, 188, 214, 353
 - DPNSS, 198, 300, 353
 - DS0, 120, 287, 288, 295, 353
 - DSL, 28, 118, 236, 244, 324, 338, 341, 337, 353, 363
 - DSLAM, 236, 353
 - DSP, 42, 44, 353
 - DSS1, 6, 17, 54, 62, 69, 107, 118, 167, 285, 288, 290, 303, 309, 353, 356, 361
 - DTMF, 12, 34, 47, 72, 108, 123, 124, 126, 127, 134, 147, 153, 307, 349, 353
 - DTX, 45, 47, 353
- E**
 - E-DSS1, 15, 16, 353
 - ENUM, 32, 38, 84, 353
 - ETSI, 7, 26, 217, 250-256, 260, 261, 263, 284, 314S
- F**
 - FDM, 354
 - FEC, 354
 - FISU, 190, 354
 - FMC, 338, 342, 354
 - FMCA, 342, 354
 - FR, 47, 285, 299, 354
 - FTR, 25, 256, 258, 354
 - FTTx, 244, 354
- G**
 - GGSN, 330, 324, 334, 354
 - GII, 255, 354
 - GK, 13, 309, 354
 - GPRS, 8, 253, 319, 324, 325, 328, 334, 341, 354, 360
 - GSN, 199, 202, 354
 - GTT, 190, 195, 354
- H**
 - HFC, 324, 354
 - HSS, 8, 326, 327, 331, 336
 - HTTP, 33, 37, 58, 76, 258, 354
- I**
 - IAD, 29, 82, 118, 132, 133, 236, 281, 305, 354
 - IANA, 191, 354
 - IBCF, 341, 354
 - IMS, 7, 8, 12, 84, 271, 273, 274, 285, 317-342
 - IMSI, 335, 355
 - IM-SSF, 330, 331, 355
 - IN, 37, 84, 286, 202, 203, 246, 291, 303, 355, 360
 - INAP, 16, 23, 31-33, 37, 38, 163, 285, 288-290, 294, 308, 355
 - IP, 3-5, 7, 10-12, 16-38, 39-51, 53-58, 61, 63-67, 82-87, 94-96, 107, 111, 114-120, 130-134, 150-157, 163-168, 170-174, 180-192, 196, 198, 199, 214, 217, 221-223, 232, 234-240, 244, 246, 251, 256-261, 264-266, 271, 274, 276, 280-299, 303, 343-346, 348, 350, 352, 355, 361
 - IPBCP, 6, 198, 221, 222, 226, 227, 355
 - IPCC, 3, 26, 67, 83, 233, 242, 279, 326, 337, 355
 - IPDC, 13, 118, 284-285, 355
 - IRI, 252-257, 262, 355
 - ISC, 25, 27, 35
 - ISIM, 317, 318, 335, 342, 356
 - ISM, 205, 288, 356
 - ISN, 199, 201, 202, 205, 206, 222-230
 - ISUP, 6, 11, 31, 38, 52, 58, 83, 91, 107, 163-169, 179, 181-188, 195, 284-290, 294, 302, 308, 310, 356
 - ITU, 232, 344, 356, 357
 - ITU-T, 197, 199, 205, 207, 214, 215, 221, 345, 350
 - IUA, 33, 167, 184, 196, 361
 - IW-F, 30, 31, 35, 36, 37
 - IWU, 225, 226
- J**
 - JAIN, 16, 31, 33, 37, 38, 246, 290, 295, 298, 357
 - JTAPI, 185, 290, 295, 357
- L**
 - LDAP, 29, 33, 37, 66, 289, 303
 - LI, 252, 261, 357
 - LSSU, 190, 191, 357
- M**
 - M2PA, 16, 167, 181, 185, 189, 191, 237, 309, 357

- M2UA, 6, 16, 166, 167, 181, 185, 187-191, 237, 358
 M3UA, , 16, 32, 37, 167, 179, 181, 183,-189, 191-195, 237, 296, 303, 309, 350, 358, 361
 MAP, 31-33, 37, 38, 163, 257, 331, 358
 MC, 48, 92, 358
 MCU, 63, 358
 MD, 202, 260, 262, 358
 MEGACO, 3, 5, 10, 15, 34, 41, 50 53, 57, 58, 62, 82, 115, 117-119, 131, 132, 136, 139, 141, 144, 145, 147, 149, 150-164, 244, 284, 289, 290, 294, 301, 303, 309, 331, 333, 350, 358
 MGC, 217, 234, 242
 MGC-F, 31-38
 MGCP, 31-37, 41, 50-58, 62, 82, 115-135, 162, 284, 290-299, 303-309
 MG-F, 31, 33, 37, 38, 358
 MIDCOM, 64, 358
 MMUSIC, 40, 49
 MMSF, 217, 218, 221
 MPS, 106, 107
 MRF, 9, 331, 359
 MS, 34, 37, 285, 290, 359
 MSC, 317, 319, 334, 359
 MSF, 6, 279, 337
 MS-F, 30, 33, 359
 MSU, 190, 359
- N**
 NASS, 338, 341, 359
 NFAC, 90, 359
 NGN, 222, 225, 230, 232-236, 242, 243-248, 255, 260, 267, 277, 278
 NWO/AP/SvP, 250, 252, 253, 254-258
- O**
 OMS, 288, 358
 OSA, 318, 330-332
 OSI, 257, 267, 272
 OSS, 16, 36, 302, 303, 359
- P**
 PARLAY, 31, 33, 37, 39
 PDF, 8, 330, 360
- R**
 RADIUS, 17, 32, 38, 289, 309, 310, 311
 RAS, 48, 55, 57, 86, 90, 93-98, 100
 RFC, 64, 66, 83, 118, 119, 125, 126, 127, 137, 149, 150, 165, 168, 196, 309, 320, 330, 335, 349, 350
 R-F, 30-33, 36-38
 RSVP, 23, 48, 49, 62
- RTCP, 93, 111-114, 150, 342, 360
 RTSP, 49, 62, 360
- S**
 SAP, 207, 209
 SAU, 293
 SBC, 11, 12, 266-269, 293, 316, 329
 SCCP, 16, 163, 167, 170, 190-195, 284, 290, 296, 308, 361
 SC-F, 30, 33, 37
 SCIP, 60, 361
 SCP, 17, 22, 242, 284, 290, 309
 SCS, 330, 331, 361
 SCTP, 7, 17, 32, 33, 37, 54, 62, 131, 149, 165, 166, 174-191, 195, 288, 296, 303, 309
 SDP, 199, 217, 221, 238-240, 271, 273, 274, 342
 SEG, 33, 49, 58, 60, 62-64, 71, 74, 78, 79, 90, 130, 149, 156-160
 SET, 88, 198, 203, 214
 SG, 15, 50, 52, 54, 118, 164, 167, 179, 181-188, 190, 192, 196, 217, 235, 237
 SGCP, 13, 118, 361
 SG-F, 30, 32, 37
 Sigtran, 11, 15, 16, 23, 32, 37, 54, 82, 117, 235, 237, 240, 361
 SIP, 3-8, 336-337, 341, 342
 SIP-T, 15, 17-18, 31, 38, 61, 83, 85, 361
 SLA, 267, 272
 SLF, 326, 327, 329, 361
 SLS, 182, 189, 361
 SN, 199, 201, 211, 215-219
 SNMP, 16, 29, 128, 291, 299, 301, 308
 SPAN, 320, 362
 SPINS, 284, 362
 SPIRITS, 84, 362
 SPS-F, 30, 32, 37, 38
 SS7, 186, 187, 193
 SSL, 58, 30, 251
 SSP, 284, 361
 STC, 199, 202, 204, 207, 210, 211, 214, 227, 361
 STC, 199, 202, 204, 207, 210, 211, 214, 227, 361
 STP, 16, 51, 117, 164, 167, 181, 183, 361
 STUN, 64, 361
 SUA, 6, 16, 32, 37, 167, 181, 186, 191, 192, 193-195, 309, 345, 360, 361
 SVC, 286, 361
 SVI, 294
 SWN, 200, 202, 361
- T**
 TAR, 361, 362
 TCAP, 16, 31, 38, 163, 167, 170, 191-192, 284, 290, 294, 302, 308
 TG, 234, 235, 244, 361
 THIG, 271, 329, 341, 361
 TIPPHON, 217, 303, 320, 361
 TISPAN, 320, 338, 339, 340, 341, 344, 354, 355, 362
 TLS, 58, 362, 251, 274
 TRIP, 32, 38, 84, 362
 TSAP, 4, 86, 362
 TSN, 169, 178, 200, 202, 222, 223, 362
 TUA, 32, 37, 366
 TURN, 64, 362
- U**
 UA, 66, 67, 328, 362
 UAC, 49, 66, 362
 UAS, 49, 66, 362
 UICC, 336, 362
 UMTS, 321, 338, 351, 359
 UPL, 168, 177, 362
 URI, 71, 329, 335, 336, 337
 URL, 4, 63, 64, 70, 84, 87, 335, 337, 362
 USIM, 336, 342, 362
- V**
 V5, 9, 33, 15, 16, 23, 235, 362
 V5UA, 6, 33, 37, 167, 196, 235, 309, 345, 360, 362
 VAD, 362, 45, 47
 VoATM, 363
 VTCH, 288, 363
- W**
 WAP, 363
 WCLMA, 318, 363
 WLAN, 319, 324, 338, 369
 WLL, 244, 363



Авторы получили дипломы инженеров и ученые степени в Санкт-Петербургском государственном университете телекоммуникаций им. проф. М. А. Бонч-Бруевича, преподают там же, опубликовали совместно монографию «Протоколы и технологии MPLS».

Борис Гольдштейн – доктор технических наук, профессор. В прошлом занимался программным обеспечением систем коммутации каналов, операционными системами, теорией телетрафика. В 1982 году защитил кандидатскую диссертацию «Исследование и разработка телефонной операционной системы электронного узла коммутации», а в 1994 году – докторскую диссертацию «Численные методы анализа

и проектирования программного обеспечения систем коммутации». В настоящее время его внимание сосредоточено на различных аспектах конвергенции сетей и услуг связи при переходе к сетям связи следующего поколения NGN. С результатами этих исследований можно познакомиться на сайте www.niits.ru. Многие годы работает заместителем директора ЛОНИИС, изо всех сил стараясь при этом не превратиться в бюрократа от науки. По этой причине давно и активно преподает, а в последние годы – и заведует кафедрой систем коммутации в СПбГУТ. Его аспиранты, многие из которых успешно защитили кандидатские диссертации, активно работают сегодня в телекоммуникационной индустрии России, Узбекистана, США, Монголии, Германии и других стран. Опубликовал более 200 печатных работ в области инфокоммуникаций, дюжину книг, в числе которых «Сигнализация в сетях связи», «Протоколы сети доступа», «Evolution of Telecommunication Protocols», «Системы коммутации» и др., получил две дюжины авторских свидетельств и патентов, в том числе на несколько весьма успешных на сегодняшнем телекоммуникационном рынке продуктов, являлся членом оргкомитета ряда международных симпозиумов, среди которых наиболее памятным был Международный конгресс по телетрафику ITC-15 в Вашингтоне. Приглашался в качестве автора в IEEE Selected Areas of Communications, в IEEE Communications Magazine и др. Возглавляет советы директоров двух крупных петербургских научно-технических центров, является членом редколлегий двух отраслевых журналов. Является членом IEEE, одним из первых обладателей премии «Факел Бирмингема», академиком МАС, МАИ, «Мастер связи».

Александр Гольдштейн, кандидат технических наук, доцент кафедры СПбГУТ им. проф. М. А. Бонч-Бруевича, начальник сектора ЛОНИИС. Родился в 1980 г., в 2001 г. окончил СПбГУТ, а в 2004 г. защитил кандидатскую диссертацию «Исследование механизма туннелирования мультимедийного трафика в сети MPLS». В 2005 г. окончил финансово-экономический институт по специальности бизнес-менеджмента. Член IEEE, опубликовал порядка 25 печатных работ по перспективным направлениям современных инфокоммуникаций – MPLS, Softswitch и др.

Гольдштейн Александр Борисович
Гольдштейн Борис Соломонович

SOFTSWITCH

ИБ № 3004 ЛР № 065953 от 15.08.98

Подписано в печать

Формат 70×100 $\frac{1}{16}$.

Бумага офсетная.

Гарнитура прагматика. Печать офсетная.

Объем 23 печ. л.

Тираж 4000 экз. Зак № 4513

Издательство «БХВ — Санкт-Петербург», 190005, Санкт-Петербург, Измайловский пр., д. 29

Отпечатано с готовых диапозитивов
в ГУП «Типография «Наука»
199034, Санкт-Петербург, 9 линия, 12

Гибкие коммутаторы Softswitch составили хорошую альтернативу традиционным АТС по цене и функциональным возможностям, по масштабируемости, качеству обслуживания, габаритам, энергопотреблению и стоимости техобслуживания. Но основная причина успеха Softswitch на рынке - его умение согласовывать разные протоколы сигнализации как сетей одного типа, например, при сопряжении сетей H.323 и SIP, так и при взаимодействии сетей коммутации каналов (протоколы ОКС7) с IP-сетями (протоколы SIP, MGCP, Megaco, H.323).

Взаимосвязь сетей ОКС7 и IP рассматривается в книге в контексте технологии Sigtran, имитирующей ОКС7 средствами IP-протоколов, а также весьма близким к ОКС7 протоколом BICC. Анализируются варианты построения сетей следующего поколения NGN на базе Softswitch, как для схем IP-TDM-IP, так и для прямых схем IP-IP. Для поддержки последних в состав NGN включается новый элемент SBC (Session Border Controller), рассматриваемый в книге вместе с архитектурой IMS (IP Multimedia SubSystem).



Книги

Системы коммутации. Учебник для ВУЗов
Сигнализация в сетях связи. Том 1
Протоколы сети доступа. Том 2
Интеллектуальные сети
Call-центры и компьютерная телефония
IP-телефония
Технология и протоколы MPLS



Справочники по протоколам телекоммуникаций

ОКС7: Подсистема МТР
ОКС7: Подсистема ISUP
Интерфейсы V5.1 и V5.2
Сигнализация R1.5
Протокол SIP

Планируется выход в 2006 году

ОКС7: Подсистема SCCP
Протокол MEGACO/H.248

КНИГА ПОЧТОЙ:

196240
Россия
Санкт-Петербург
Абонентский ящик 277

Факс: (812) 389 29 72
Телефон: (812) 389 68 97
E-mail: nio1@niits.ru
Internet: www.niits.ru

ISBN 5-8206-0117-3

