



Б.С. Гольдштейн, А.А. Зарубин, В.В. Саморезов



**СПРАВОЧНИК
ПО ТЕЛЕКОММУНИКАЦИОННЫМ ПРОТОКОЛАМ**

Протокол SIP

Б.С. Гольдштейн, А.А. Зарубин, В.В. Саморезов

**Серия справочников
«Телекоммуникационные протоколы ВСС РФ»**

Протокол SIP

Справочник

Санкт-Петербург
«БХВ-Петербург»

2014

УДК 621.395
Г63
ББК 32.88

Б.С. Гольдштейн, А.А. Зарубин, В.В. Саморезов

Протокол SIP: Справочник. – СПб.: БХВ-Петербург, 2014. – 456 с.: ил.

ISBN 978-5-9775-1593-1

Приводятся сведения о принципах организации и функционирования протокола SIP (Session Initiation Protocol), широко используемого сегодня в IP-телефонии и являющегося наиболее вероятным кандидатом на ведущую роль в сетях связи следующего поколения NGN. Описываются сообщения SIP, процедуры управления соединениями в IP-сети и между сетями IP и ТфОП, процедуры аутентификации, защиты информации, обеспечения безопасности. Рассматриваются расширения SIP, обеспечивающие взаимодействие сети IP с телефонной сетью при создании и поддержке сеансов связи ТфОП-IP-ТфОП, ТфОП-IP и IP-ТфОП. Излагаются задачи преобразования сигнализации SIP при взаимодействии с другими протоколами сетей NGN. Освещаются вопросы тестирования SIP и пути реализации на базе этого протокола ряда известных и новых инфокоммуникационных услуг.

Справочник

ISBN 978-5-9775-1593-1

© Гольдштейн Б.С., Зарубин А.А., Саморезов В.В., 2005, 2014

Содержание

Предисловие	14
Глава 1. Принципы и возможности SIP	18
1.1. Протокол SIP в IP-сетях	19
1.2. Адресация в сетях SIP	23
1.3. Уровни протокола SIP	23
1.4. SIP и HTTP	25
1.5. Вызовы SIP	26
Глава 2. Агент пользователя	29
2.1. Логический объект Агент пользователя	29
2.2. Клиент агента пользователя UAC	29
2.2.1. Создание запроса	30
2.2.1.1. Формирование поля Request-URI	30
2.2.1.2. Формирование заголовка To	30
2.2.1.3. Формирование заголовка From	31
2.2.1.4. Формирование заголовка Call-ID	32
2.2.1.5. Формирование заголовка Cseq	33
2.2.1.6. Формирование заголовка Max-Forwards	33
2.2.1.7. Формирование заголовка Via	33
2.2.1.8. Формирование заголовка Contact	34
2.2.1.9. Формирование заголовков Supported и Require	34
2.2.1.10. Дополнительные компоненты сообщения	35
2.2.1.11. Передача запроса	35
2.2.2. Обработка ответов	36
2.2.2.1. Ошибки уровня транзакций	37
2.2.2.2. Неизвестные ответы	37
2.2.2.3. Заголовки Via	37
2.2.2.4. Обработка ответов группы 3xx	37
2.2.2.5. Обработка ответов группы 4xx	39
2.3. Сервер агента пользователя (UAS)	40
2.3.1. Процедура обработки запросов	41
2.3.1.1. Определение типа запроса	41
2.3.1.2. Определение типа заголовка	41
2.3.1.3. Обработка полей To и Request-URI	41
2.3.1.4. Обработка одинаковых запросов	42

2.3.1.5.	Обработка заголовка Require.....	42
2.3.1.6.	Обработка содержимого тела сообщения	43
2.3.1.7.	Применение расширений.....	43
2.3.2.	Создание ответа	44
2.3.2.1.	Передача предварительного ответа	44
2.3.2.2.	Заголовки и параметры «tag»	44
2.3.2.3.	Действие UAS без сохранения состояний.....	45

Глава 3. Сообщения протокола SIP 46

3.1.	Структура сообщений.....	46
3.2.	Заголовки сообщений	47
3.2.1.	Формат заголовка.....	47
3.2.2.	Заголовок Accept	51
3.2.3.	Заголовок Accept-Encoding	51
3.2.4.	Заголовок Accept-Language	51
3.2.5.	Заголовок Alert-Info.....	51
3.2.6.	Заголовок Allow.....	52
3.2.7.	Заголовок Allow-Events.....	52
3.2.8.	Заголовок Authentication-Info	53
3.2.9.	Заголовок Authorization	53
3.2.10.	Заголовок Call-ID	53
3.2.11.	Заголовок Call-Info	54
3.2.12.	Заголовок Contact.....	54
3.2.13.	Заголовок Content-Disposition	55
3.2.14.	Заголовок Content-Encoding	56
3.2.15.	Заголовок Content-Language.....	57
3.2.16.	Заголовок Content-Length	57
3.2.17.	Заголовок Content-Type	58
3.2.18.	Заголовок Cseq.....	58
3.2.19.	Заголовок Date	58
3.2.20.	Заголовок Error-Info	59
3.2.21.	Заголовок Event	59
3.2.22.	Заголовок Expires.....	60
3.2.23.	Заголовок From.....	60
3.2.24.	Заголовок In-Reply-To	60
3.2.25.	Заголовок Max-Forwards	61
3.2.26.	Заголовок Min-Expires	61
3.2.27.	Заголовок MIME-Version.....	61

3.2.28.	Заголовок Organization	62
3.2.29.	Заголовок Path	62
3.2.30.	Заголовок Priority	63
3.2.31.	Заголовок Privacy	63
3.2.32.	Заголовок Proxy-Authenticate	64
3.2.33.	Заголовок Proxy-Authorization	64
3.2.34.	Заголовок Proxy-Require	65
3.2.35.	Заголовок P-Asserted-Identity	65
3.2.36.	Заголовок P-Preferred-Identity	66
3.2.37.	Заголовок P-Media-Authorization	66
3.2.38.	Заголовок The P-Associated-URI	67
3.2.39.	Заголовок P-Called-Party-ID	67
3.2.40.	Заголовок P-Visited-Network-ID	68
3.2.41.	Заголовок P-Access-Network-Info	68
3.2.42.	Заголовок P-Charging-Function-Addresses	69
3.2.43.	Заголовок P-Charging-Vector	70
3.2.44.	Заголовок P-DCS-Trace-Party-ID	70
3.2.45.	Заголовок P-DCS-OSPS	71
3.2.46.	Заголовки P-DCS-BILLING-INFO	72
3.2.47.	Заголовок P-DCS-LAES и P-DCS-REDIRECT	72
3.2.48.	Заголовок RACK	73
3.2.49.	Заголовок Reason	73
3.2.50.	Заголовок Record-Route	74
3.2.51.	Заголовок Refer-To	74
3.2.52.	Заголовок Reply-To	74
3.2.53.	Заголовок Require	75
3.2.54.	Заголовок Retry-After	75
3.2.55.	Заголовок Route	75
3.2.56.	Заголовок Rseq	76
3.2.57.	Заголовки Security-Client, Security-Server, Security-Verify	76
3.2.58.	Заголовок Server	77
3.2.59.	Заголовок Service-Route	77
3.2.60.	Заголовок Subject	78
3.2.61.	Заголовок Subscription-State	78
3.2.62.	Заголовок Supported	79
3.2.63.	Заголовок Timestamp	79
3.2.64.	Заголовок To	79
3.2.65.	Заголовок Unsupported	79

3.2.66.	Заголовок User-Agent	80
3.2.67.	Заголовок Via	80
3.2.68.	Заголовок Warning	81
3.2.69.	Заголовок WWW-Authenticate.....	81
3.3.	Назначение и формат запросов.....	89
3.3.1.	Структура запросов	89
3.3.2.	Запрос INVITE	90
3.3.3.	Сообщение ACK	91
3.3.4.	Сообщение CANCEL.....	91
3.3.5.	Сообщение BYE.....	92
3.3.6.	Сообщение REGISTER.....	92
3.3.7.	Сообщение OPTIONS	92
3.3.8.	Сообщение INFO	93
3.3.9.	Сообщение PRACK.....	94
3.3.10.	Сообщение UPDATE	95
3.3.11.	Сообщения SUBSCRIBE и NOTIFY.....	98
3.3.12.	Сообщение REFER	101
3.3.13.	Сообщение MESSAGE.....	102
3.4.	Назначение и формат ответов на запросы	106
3.4.1.	Информационные ответы 1xx.....	107
3.4.2.	Ответы об успешной обработке запроса 2xx	108
3.4.3.	Ответы о перенаправлении вызова 3xx	109
3.4.4.	Ответы об ошибке в запросе 4xx	110
3.4.5.	Ответы об отказе сервера 5xx	113
3.4.6.	Ответы о полной невозможности установить соединение 6xx	114

Глава 4. Процедуры управления соединением..... 115

4.1.	Диалоги.....	115
4.2.	Процедура создания диалога	116
4.2.1.	Действия UAS	116
4.2.2.	Действия UAC	118
4.3.	Процедура передачи и приема запросов в ходе диалога	118
4.3.1.	Действия UAC при создании запроса	119
4.3.2.	Действия UAC при обработке ответов	121
4.3.3.	Действия UAS	121
4.3.4.	Процедура завершения диалога	122

4.4. Транзакции	122
4.4.1. Процедуры функционирования клиентских транзакций.....	124
4.4.2. Клиентская INVITE-транзакция	125
4.4.3. Конечный автомат клиентской INVITE-транзакции.....	125
4.4.4. Формирование запроса ACK.....	128
4.4.5. Клиентская не-INVITE-транзакция	129
4.4.6. Конечный автомат клиентской не-INVITE транзакции	130
4.4.7. Соответствие ответов клиентским транзакциям.....	132
4.4.8. Процедуры функционирования серверных транзакций	132
4.4.9. Серверная INVITE-транзакция.....	133
4.4.10. Серверная не-INVITE-транзакция.....	135
4.4.11. Соответствие запросов серверным транзакциям.....	136
4.5. SDL-диаграммы для конечных автоматов транзакций.....	139
4.5.1. Клиентская INVITE-транзакция	139
4.5.2. Клиентская не-INVITE-транзакция	143
4.5.3. Серверная INVITE-транзакция	146
4.5.4. Серверная не-INVITE-транзакция.....	149
4.6. Процедура регистрации	152
4.6.1. Процедура формирования запроса REGISTER	154
4.6.2. Создание связей	156
4.6.2.1. Продолжительность действия контактного адреса	157
4.6.2.2. Приоритеты среди контактных адресов	157
4.6.3. Удаление связей	158
4.6.4. Обновление связей	158
4.6.5. Определение адреса registrar	159
4.6.6. Отправка запроса	159
4.7. Процедура обработки запроса REGISTER.....	160
4.8. Процедура запроса информации о функциональных возможностях	164
4.8.1. Создание запроса OPTIONS	165
4.8.2. Обработка запроса OPTIONS	165
4.9. Процедура отмены запроса.....	167
4.9.1. Действия клиента	167
4.9.2. Действия сервера	168
4.10. Инициирование сеансов связи	169
4.10.1. Процедуры UAC. Создание начального запроса INVITE	171
4.10.2. Процедуры UAC. Обработка ответов на запрос INVITE.....	173
4.10.2.1. Ответы 1xx.....	173

4.10.2.2.	Ответы 3xx.....	174
4.10.2.3.	Ответы 4xx, 5xx и 6xx	174
4.10.2.4.	Ответы 2xx.....	174
4.10.3.	Процедуры UAS. Обработка запроса INVITE	175
4.10.3.1.	Текущая стадия обработки	176
4.10.3.2.	Перенаправление запроса INVITE.....	177
4.10.3.3.	Отклонение запроса INVITE	177
4.10.3.4.	Прием запроса INVITE	177
4.11.	Процедуры модификации сеансов связи	178
4.11.1.	Действия UAC	179
4.11.2.	Поведение UAS	180
4.12.	Процедуры разрушения сеансов связи.....	183
4.12.1.	Разрушение сеанса с помощью запроса BYE. Работа UAC	183
4.12.2.	Разрушение сеанса с помощью запроса BYE. Работа UAS	183

Глава 5. Прокси-серверы SIP 184

5.1.	Назначение прокси-сервера-SIP	184
5.2.	Функции прокси-сервера с сохранением состояний.....	186
5.2.1.	Проверка правильности составления запроса	187
5.2.1.1.	Проверка корректности синтаксиса.....	187
5.2.1.2.	Проверка схемы URI	188
5.2.1.3.	Проверка заголовка Max-Forwards.....	188
5.2.1.4.	Проверка наличия замкнутого пути	188
5.2.1.5.	Проверка заголовка Proxy-Require	189
5.2.1.6.	Проверка заголовка Proxy-Authorization	189
5.2.2.	Предварительная обработка маршрутной информации	189
5.2.3.	Определение адресов пересылки	190
5.2.4.	Пересылка запроса	192
5.2.4.1.	Копирование запроса.....	193
5.2.4.2.	Обновление содержимого поля Request-URI	193
5.2.4.3.	Обновление содержимого заголовка Max-Forwards.....	193
5.2.4.4.	Добавление значения Record-Route (опционально).....	193
5.2.4.5.	Добавление дополнительных заголовков	195
5.2.4.6.	Заключительная обработка маршрутной информации	195
5.2.4.7.	Определение адреса, порта и транспортного протокола для пересылки следующему элементу	196
5.2.4.8.	Добавление значения в заголовки Via	199
5.2.4.9.	Добавление заголовка Content-Length (в случае необходимости).....	199
5.2.4.10.	Пересылка запроса	199
5.2.4.11.	Установка таймера C	199
5.2.5.	Обработка ответов	199
5.2.5.1.	Обнаружение буфера ответов	200

5.2.5.2.	Перезапуск таймера С при помощи предварительных ответов	200
5.2.5.3.	Удаление верхнего значения заголовка Via	200
5.2.5.4.	Добавление ответа в буфер ответов	201
5.2.5.5.	Проверка необходимости немедленной пересылки ответа	202
5.2.5.6.	Выбор «наилучшего» окончательного ответа из буфера ответов	202
5.2.5.7.	Объединение значений в заголовке Authorization	204
5.2.5.8.	Перезапись значений заголовка Record-Route	204
5.2.5.9.	Пересылка ответа	205
5.2.5.10.	Создание запросов CANCEL	206
5.2.6.	Обработка таймера С	206
5.2.7.	Обработка ошибок транспортного уровня SIP	207
5.2.8.	Обработка запроса CANCEL	207
5.3.	Функции прокси-сервера без сохранения состояний	208
5.4.	Работа с заголовком Route и полем Request-URI	210
5.5.	Работа с заголовком Route и полем Request-URI	211
5.5.1.	Взаимодействие через исходящий и входящий прокси-серверы	211
5.5.2.	Прохождение сообщений через strict-router	213
5.5.3.	Прохождение сообщений через прокси-сервер с перезаписью значения в заголовке Record-Route	215
5.6.	Назначение и функции сервера перенаправления	216
Глава 6.	Процедуры HTTP-аутентификации	218
6.1.	Аутентификация в SIP	218
6.2.	Процедуры аутентификации «пользователь-пользователь»	220
6.3.	Процедуры аутентификации «прокси-сервер-пользователь»	222
6.4.	Схема аутентификации «Digest»	223
Глава 7.	Защита тела сообщения средствами S/MIME	229
7.1.	S/MIME сертификаты	229
7.2.	Обмен ключами S/MIME	231
7.3.	Защита тела сообщения	234
7.4.	SIP-туннелирование	235
7.4.1.	Обеспечение целостности SIP сообщений	236
7.4.2.	Шифрование при туннелировании	238
Глава 8.	Процедуры обеспечения безопасности	240
8.1.	Типы угроз	241

8.1.1. Злоумышленная регистрация	241
8.1.2. Имитация сервера	242
8.1.3. Порча тела сообщения	243
8.1.4. Срыв сеансов связи	244
8.1.5. Отказ в обслуживании (DoS-атаки)	244
8.2. Механизмы обеспечения безопасности	246
8.2.1. Безопасность транспортного и сетевого уровней	247
8.2.2. Схема SIPS URI.....	248
8.2.3. HTTP-аутентификация.....	249
8.2.4. S/MIME	249
8.3. Реализация механизмов обеспечения безопасности.....	250
8.3.1. Требования для разработчиков оборудования SIP	250
8.3.2. Решения по обеспечению безопасности	250
8.3.2.1. Регистрация	251
8.3.2.2. Междоменные запросы	252
8.3.2.3. Запросы при отсутствии локального прокси-сервера.....	254
8.3.2.4. Защита от DoS-атак.....	256
Глава 9. Алгоритмы установления соединения	257
9.1. Установление соединения с участием прокси-сервера	257
9.2. Установление соединения с участием сервера перенаправления.....	267
Глава 10. Транспортный уровень протокола SIP	273
10.1. Назначение транспортного уровня	273
10.2. Работа клиента при передаче запросов	274
10.3. Работа клиента при получении ответов.....	276
10.4. Работа сервера при получении запросов.....	277
10.5. Работа сервера при передаче ответов	278
10.6. Длина тела сообщения	279
10.7. Обработка ошибок.....	280
Глава 11. Протокол SIP-T для телефонии	281
11.1. Назначение и особенности протокола SIP-T	281
11.2. Сценарии организации взаимодействия	282
11.2.1. Применение SIP-T при транзите (ТфОП-IP-ТфОП)	282

11.2.2.	Процедуры организации связи из ТфОП в IP-сеть	284
11.2.3.	Процедуры организации связи из IP-сети в ТфОП	285
11.3.	Компоненты протокола SIP-T	286
11.3.1.	Использование протокола SIP	286
11.3.2.	Процедуры инкапсуляции сигнальных сообщений	286
11.3.3.	Процедуры преобразования сигнальных сообщений	289
11.3.4.	Поддержка передачи сигнальных сообщений во время сеанса	290
11.4.	Согласование содержимого сообщений протокола SIP	290
11.5.	Процедуры обеспечения безопасности	293

Глава 12. Преобразование ISUP–SIP 294

12.1.	Общие принципы взаимодействия	294
12.2.	Требования к SIP при взаимодействии с ТфОП	295
12.2.1.	Процедуры прозрачной передачи сообщений ISUP	295
12.2.2.	Процедуры поддержки формата MIME	295
12.2.3.	Процедуры передачи многочастотного набора DTMF	295
12.2.4.	Процедуры проключения речевых трактов в предответном состоянии	296
12.2.5.	Обмен транзакциями во время активного сеанса	296
12.2.6.	Поддержка механизмов обеспечения конфиденциальности	297
12.2.7.	Информация о причинах, вызвавших передачу запроса CANCEL	297
12.3.	Процесс обмена сообщениями	297
12.3.1.	Установление соединения (быстрый ответ не используется)	298
12.3.2.	Установление соединения (быстрый ответ)	299
12.3.3.	Таймеры протокола SIP	300
12.3.4.	Срабатывание таймера ISUP T9	302
12.3.5.	Ошибки в сети SIP при установлении соединения	303
12.3.6.	Перенаправление запросов в сети SIP	304
12.3.7.	Установление соединения прерывается со стороны ТфОП	306
12.4.	Конечные автоматы SIP-T при взаимодействии ISUP-SIP	308
12.4.1.	Начало получения адресной информации	308
12.4.2.	Процедуры преобразования сообщения IAM в запрос INVITE	308
12.4.3.	Сообщение 100	310
12.4.4.	Сообщения группы 18х	310
12.4.5.	Сообщения группы 2хх	312
12.4.6.	Сообщения группы 3хх	313
12.4.7.	Сообщения групп 4хх — 6хх	313

12.4.8.	Преобразование кодов ответов SIP в коды событий ISUP	313
12.4.9.	Получение сообщения REL.....	315
12.4.10.	Срабатывания таймера ISUP T11.....	316
12.5.	Примеры сценариев для случая соединения ТфОП — SIP	316
12.5.1.	Успешное соединение абонента ТфОП с пользователем сети SIP	317
12.5.2.	Соединение от абонента ТфОП к пользователю сети SIP, быстрый ответ	322
12.5.3.	Соединение от абонента УПАТС к пользователю сети SIP.....	327
12.5.4.	Неуспешное установление соединения из ТфОП в сеть SIP. Пользователь не найден ..	331
12.5.5.	Неуспешное установление соединения из ТфОП в сеть SIP. Линия занята	333
12.5.6.	Неуспешное установление соединения. Линия занята. IAM содержит параметр interworking	336
12.5.7.	Неуспешное установление соединения. Срабатывает таймер	339
12.5.8.	Неуспешное установление соединения. Срабатывает таймер. Прокси-сервер в режиме без сохранения состояния	342
12.5.9.	Неуспешное установление соединения. Вызывающий абонент кладет трубку, не дождавись установления соединения	344

Глава 13. Преобразование SIP–ISUP 349

13.1.	Процесс обмена сообщениями.....	349
13.1.1.	Установление соединения (быстрый ответ не используется)	349
13.1.2.	Установление соединения (быстрый ответ).....	351
13.1.3.	Срабатывание таймера T7	352
13.1.4.	Срабатывание таймеров SIP	353
13.1.5.	Ошибка установления соединения на стороне ТфОП	354
13.1.6.	В сообщении ACM содержится код причины	355
13.1.7.	Пользователь SIP прерывает установление соединения	356
13.2.	Конечные автоматы SIP-T при взаимодействии SIP-ISUP	358
13.2.1.	Получение запроса INVITE	358
13.2.2.	Процедуры преобразования INVITE в IAM.....	359
13.2.3.	Срабатывание таймера ISUP T7	362
13.2.4.	Получение сообщения CANCEL или BYE	362
13.2.5.	Получение сообщения REL.....	363
13.2.6.	Преобразование кодов причины ISDN в коды ответов сети SIP.....	364
13.2.7.	Получение предварительного ответа ACM	367
13.2.8.	Получение сообщения ACM	367
13.2.9.	Получение сообщений CON или ANM	368
13.2.10.	Срабатывание таймера T9	369

13.2.11. Получение сообщения CPG	369
13.2.12. Получение ACK.....	370
13.3. Примеры сценариев и сообщений для вызовов SIP-ТфОП	370
13.3.1. Успешное соединение из сети SIP в ТфОП.....	371
13.3.2. Успешное соединение из сети SIP к абоненту УПАТС	378
13.3.3. Соединение из сети SIP в ТфОП в условиях перегрузки шлюза.....	385
13.3.4. Соединения из сети SIP в SIP с использованием ENUM Query	393
13.3.5. Неуспешное соединение из SIP в ТфОП: сообщение об ошибке из ТфОП	398
13.3.6. Неуспешное соединение из сети SIP в ТфОП: ТфОП отклоняет вызов, передавая REL с кодом причины	404
13.3.7. Неуспешное соединение из сети SIP в ТфОП: срабатывает таймер ожидания шлюзом сообщения ANM.....	407
Глава 14. Формирование телефонных URI.....	413
14.1. Телефонные SIP URI	413
14.2. Процедура преобразования формата ISUP в формат tel URL	415
14.3. Процедура преобразования формата tel URL в формат ISUP	416
Глава 15. Преобразование, тестирование и реализация SIP	417
15.1. Подходы к преобразованию сигнализации SIP	417
15.2. Тестирование протокола SIP	421
15.3. Реализация услуг на базе SIP	422
15.4. PINT и SPIRITS	427
Глава 16. Quo Vadis?	430
16.1. Дальнейшее развитие SIP	430
16.2. SIP в мобильных сетях 3G	431
16.3. Работа с NAT.....	440
Список сокращений	443
Глоссарий	449
Литература	452

Предисловие

«Музыкой будущего» иронически именовали опубликованную Рихардом Вагнером в 1850 теорию музыки; это выражение и сегодня используется среди музыкантов как насмешка. Столь же критически был встречен первый опубликованный Инженерной проблемной группой Интернет (IETF) в феврале 1996 года документ *draft-ietf-mmusic-sip-00*, с которого начинались спецификации SIP, тоже весьма медленно внедрявшиеся в телекоммуникационную индустрию. Слово MMUSIC в названии документа не связывалось непосредственно с музыкой, а представляло собой аббревиатуру выражения *Multiparty Multimedia Session Control*. Сам же документ специфицировал лишь единственный запрос установления сеанса связи, но уже тогда ориентировался на интеграцию в создававшуюся в то время мультимедийную архитектуру Интернет-конференций. В состав протоколов ядра этой мультимедийной архитектуры входили Session Announcement Protocol (SAP), Session Description Protocol (SDP) [37], Real-Time Streaming Protocol (RTSP) [64] и Real-Time Transport Protocol (RTP) [61], рассмотрение которых выходит за рамки данной книги. Следом за документом *draft-ietf-mmusic-sip-00* в декабре 1996 г. появилась следующая версия — *draft-ietf-mmusic-sip-01*, — но и в ней еще не угадывалось в полной мере будущее протокола инициирования сеансов связи SIP (Session Initiation Protocol).

Дело в том, что к началу 1996 года в IETF соперничали два протокола установления сеансов связи: *Session Invitation Protocol*, который предложили Марк Хэндли (Handley) и Ева Шулер (Schooler), и протокол *Simple Conference Invitation Protocol (SCIP)*, который предложил Хеннинг Шульцрин (Schulzrinne). Протокол Session Invitation Protocol поддерживал только установление сеанса и элементарные возможности согласования. После того как сеанс начался, этот протокол не использовался вовсе. Протокол был рассчитан на работу только поверх протокола User Datagram Protocol (UDP) и использовал SDP для описания параметров сеанса.

Протокол SCIP базировался на Transmission Control Protocol (TCP) и обеспечивал также прекращение сеанса [69]. SCIP использовал такие существующие Internet-протоколы, как Hypertext Transport Protocol (HTTP) и Simple Mail Transport Protocol (SMTP), но не использовал SDP для описания своих сеансов. В отличие от Session Invitation Protocol, протокол SCIP был разработан с оглядкой на телефонные функции. В конце 1996 года оба эти протокола были объединены в протокол Session Initiation Protocol, который позаимствовал идеи у каждого из своих прародителей. У Session Invitation Protocol протокол SIP перенял базирование на UDP и использование SDP. У SCIP протокол SIP взял поддержку TCP и его близость к другим известным протоколам IETF (таким как SMTP и HTTP). Новый протокол назвали «SIP/2.0», чтобы отличить его от «SIP/1.0», *Session Invitation Protocol*.

За три следующих года было разработано 11 версий документа *draft-ietf-mmusic-sip*, что, в конечном итоге, привело к публикации в январе 1999 г. *draft-ietf-mmusic-sip-12*, предусматривавшего 6 запросов, которые и сегодня имеются в SIP, и составившего основу опубликованного IETF (Internet Engineering Task Force) в марте 1999 г. документа RFC 2543, уже существенно отличавшегося от первого варианта, который был составлен Розенбергом (Rosenberg) и его научным руководителем в аспирантуре Колумбийского университета Хеннингом Шульцрином.

С той поры RFC 2543 продолжал претерпевать многочисленные изменения и усовершенствования; работа по дальнейшему описанию и улучшению протокола SIP продолжается и сейчас. В настоящее время действующим стандартом SIP является RFC 3261, в котором отражены все эти изменения. К чести IETF, следует отметить, что стандарт RFC 3261 совместим с предыдущей версией, т.е. с RFC 2543, и, таким образом, предшествующие реализации SIP будут согласованно работать с более новыми реализациями.

В результате, SIP стал наиболее популярным у разработчиков сетей связи следующего поколения NGN (Next Generation Network) протоколом, поддерживающим установление, изменение и завершение сеансов связи: мультимедийных конференций, телефонных соединений и соединений пользователей с разнообразными приложениями. Пользователи могут принимать участие в уже существующих сеансах связи, а также приглашать и/или быть приглашенными другими пользователями к участию во вновь создаваемом сеансе. Приглашения могут быть адресованы одному пользователю или группам пользователей.

В основу протокола SIP рабочая группа IETF MMUSIC заложила следующие принципы:

- *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, сообщаемого серверу определения местоположения при помощи специального сообщения — REGISTER;
- *масштабируемость сети* и возможность увеличения количества элементов сети, построенной на базе протокола SIP;
- *расширяемость протокола SIP*, характеризуемая возможностью дополнять протокол функциями поддержки новых услуг и его адаптации к работе с различными приложениями;
- *интеграция в стек существующих протоколов Интернет*, разработанных IETF в составе глобальной архитектуры мультимедиа и включающих в себя протокол резервирования ресурсов RSVP (Resource Reservation Protocol, RFC 2205), транспортный протокол реального времени RTP (Real-Time Transport Protocol, RFC 1889), протокол передачи потоков в реальном времени RTSP (Real-Time Streaming Protocol, RFC 2326), протокол описания параметров связи SDP (Session Description Protocol, RFC 2327);
- *взаимодействие с протоколами сигнализации H.323, MGCP, MEGACO/H.248, DSS1 и OKC7*, включая возможность переносить в сигнальных сообщениях протокола SIP не только специфический SIP-адрес, но и телефонный номер формата E.164 или любого другого формата.

Следует отметить, что SIP не является первым и единственным протоколом IP-телефонии. Первой была зонтичная рекомендация H.323, принятая Сектором стандартизации телекоммуникаций Международного союза электросвязи (ITU-T), которая превратилась в серию довольно запутанных спецификаций, нигде не реализованных полностью, но успешно применявшихся в первых приложениях IP-телефонии при дальней связи для снижения расходов на междугородную и международную телефонную связь. И, все же, прогресс инфокоммуникаций и построение сетей связи следующего поколения NGN (Next Generation Network) связаны отнюдь не с H.323. Общеизвестно, что этим целям гораздо больше соответствует протокол SIP, предложенный IETF и определяющий алгоритмы установления, модификации и завершения телефонных соединений как в процессе конвергенции сетей и услуг связи, так и в будущих конвергентных сетях NGN.

Идеологические отличия протокола SIP и свойства, общие с рассмотренными в других книгах серии «Телекоммуникационные протоколы» системами сигнализации (OKC7, R1.5, E-DSS1, V5 и др.), представлены в табл. 1 и отчасти объясняют феноменальное распространение SIP в современных инфокоммуникациях. Среди других причин его успешного внедрения можно отметить легкость реализации и масштабируемость протокола, позволяющие пользователям с недорогими ресурсами подключаться к SIP-сетям и, даже более того, — участвовать в развитии протокола путем создания разнообразных SIP-приложений и в расширении числа сторонников SIP.

Таблица 1. Сравнение систем сигнализации

Характеристики	Сигнализация в традиционных телефонных сетях	Протокол SIP
Функции протоколов	Управление установлением и разрушением соединений, управление коммутационным (транспортным) оборудованием	
Тип сети	Разработан для телефонных сетей TDM	Разработан для IP-сетей
Место применения	Существуют две группы протоколов: <ul style="list-style-type: none"> • между оборудованием доступа и коммутационным узлом или Softswitch — это V5.1/V5.2 или MEGACO/H.248, MGCP, SIP • между коммутационными узлами или Softswitch — это протоколы OKC7, E-DDS1 или SIP/SIP-T, H.323 	
Сетевой интеллект	Интеллект в центральных узлах сети	Интеллект может быть рассредоточен по оконечным элементам сети
Набор сигнальных сообщений	Схожий набор сигнальных сообщений: запрос установления соединения; разрушение соединения; КПВ; Занято; Ответ и пр.	
Типы соединений	Ориентация на телефонные сеансы связи	Ориентация на мультимедийные сеансы связи (речь/видео/данные)
Вид коммутации	Ориентация на коммутацию каналов	Ориентация на коммутацию пакетов (прежде всего, на IP-сети)
Открытость	Используется исключительно в сетях сигнализации	Может использоваться и оконечными терминалами, вплоть до телефонных аппаратов

При рассмотрении основ SIP в главе 1 мы вернемся к приведенным в таблице характеристикам и перепишем саму табл. 1 в более полном объеме. В главе 2 вводятся ключевые для SIP понятия *клиент агента пользователя* и *сервер агента пользователя*.

Глава 3 посвящена сообщениям SIP, а в следующих восьми главах на основе этих сообщений рассматриваются процедуры и алгоритмы, функции прокси-сервера и сервера перенаправления SIP, аспекты транспорта, защиты и безопасности, т.е. фактически рассматривается сам протокол SIP. Каждое сообщение протокола SIP содержит две части — набор заголовков и тело сообщения. Структура тела сообщения SIP обеспечивает высокую гибкость приложений. Использувавшийся первоначально только для переноса параметров SDP-сеанса, таких как параметры кодека и IP-адреса терминалов пользователей, протокол SIP может теперь переносить в составе тела сообщения многочисленные параметры. Примером такого использования тела сообщения SIP является протокол SIP-T, рассматриваемый в главе 11 и ориентированный на организацию взаимодействия ТфОП–SIP–ТфОП. Самому этому взаимодействию и преобразованию протокола общеканальной сигнализации ISUP в протокол SIP, а также SIP в ISUP, посвящены главы 12 и 13, соответственно.

Глава 14 целиком связана с телефонной нумерацией и рассматривает телефонные SIP URI. В качестве оправдания изложенным там примерам можно напомнить, что телефонная нумерация возникла в позапрошлом веке по примеру картотеки пациентов одного американского врача, причем с тех времен так и не было создано более эффективной системы преобразования адресов, которая позволила бы вызывать абонентов по именам или, например, по прозвищам. При сегодняшнем изобилии более дружественных пользовательских интерфейсов телефонная нумерация выглядит анахронизмом, но, тем не менее, и сегодня ее преобразование в SIP URI абсолютно необходимо.

Изложенные в книге материалы основаны на исследовательских работах и опыте отладки первых реализаций протокола SIP в мультисервисных коммутаторах доступа Протей-МКД на базе фрагментов NGN в сетях ряда операторов ЕСЭ РФ, за что авторы выражают признательность специалистам НТЦ Протей, коллегам-связистам Северо-Западного и Уральского регионов, инженерам-разработчикам протокол-тестеров SNT, сотрудникам сертификационного центра ЛОНИИС и кафедры телефонии СПбГУТ им. проф. М. А. Бонч-Бруевича. Авторы должны также поблагодарить своих студентов и коллег — Антона Галактионова и Александра Спирина — за существенную помощь, оказанную ими при подготовке этой книги.

Глава 1. Принципы и возможности SIP

1.1. Протокол SIP в IP-сетях

Протокол SIP (Session Initiation Protocol) является текстовым протоколом сигнализации в IP-сети и предназначен для создания, модификации и завершения сеансов связи – телефонных соединений и мультимедийных конференций, а также рассылки мультимедийной информации. Он использует многие конструктивные элементы и принципы протоколов сети Интернет, таких как HTTP и SMTP.

Согласно принципам семиуровневой модели Взаимодействия открытых систем OSI (Open Systems Interconnection) особенностью протокола SIP является независимость от технологий его смежных уровней (рис. 1.1), в частности, структура сообщений SIP не зависит от выбранной транспортной технологии. В качестве транспортных 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.

По IP-сети может передаваться пользовательская информация практически любого вида: речь, видео и данные, а также любая их комбинация.

Во всех случаях при организации связи между терминалами пользователей необходимо известить встречную сторону о том, какого рода информация может приниматься/передаваться, а также об алгоритме ее кодирования и об адресе, по которому следует передавать информацию.



Рис. 1.1. Место протокола SIP в стеке протоколов TCP/IP

Таким образом, одним из обязательных условий организации связи при помощи протокола SIP является обмен между участниками предполагаемого сеанса связи данными об их функциональных возможностях. Для этой цели чаще всего используется отдельный *протокол описания сеансов связи SDP (Session Description Protocol)*. Сообщение протокола SDP 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 мультимедийной информации IETF предлагает использовать протокол RTP, но сам протокол SIP не исключает возможность применения для этих целей других протоколов.

В протоколе SIP реализованы механизмы управления потоками информации и предоставления гарантированного качества обслуживания.

SIP поддерживает пять аспектов организации и завершения сеансов мультимедийной связи: определение местоположения пользователя, определение готовности пользователя участвовать в сеансе, определение функциональных возможностей терминалов пользователей (т.е. определение того, какого рода информация может использоваться, и ее параметры), установление сеанса как для вызывающей, так и для вызываемой сторон и управление сеансом связи (т.е. поддержание и завершение сеанса, модификация его параметров и активизация услуг). Кроме того, протокол SIP предоставляет возможность передачи пользовательской информации. Протокол SIP предусматривает также организацию конференций трех видов:

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

Как уже отмечалось выше, протокол SIP дает возможность подключения к уже существующему сеансу связи новых участников, т.е. двусторонний сеанс может перейти в конференцию. Расширим представленную в предисловии таблицу, приведя ее к виду табл. 1.1. Практически все строки этой новой таблицы заслуживают отдельных пояснений. Мы начнем их со строки, касающейся адресации, чему посвящен следующий параграф этой главы.

Таблица 1.1. Сравнительные характеристики протокола SIP

Характеристики	SIP	H.323	MGCP	MEGACO H.248	ISUP
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
Преимственность	Не пытается воспроизвести ТфОП	Моделирует ТфОП по аналогии с Q.931 [25]	Не пытается воспроизвести ТфОП	Наследует базовые принципы MGCP	Лежит в основе ТфОП по Q.700 [26]
Стандарты	IETF-стандарт RFC	Рекомендации ITU-T	Информац. RFC	Рек. ITU-T и IETF	Рек. ITU-T
Версии	Разные	v1 -1996, v2- 1998, v3 -1999	Единств. версия	Единств. версия	Национ. специфик.
Интеллект	Распределен по элементам сети	В ядре сети	В ядре сети	В ядре сети	В ядре сети
Сложность	Еще простой, хотя уже содержит 13 запросов	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	Выс. степень масштаб.	Масштабируемый	-	-	Масштабируемый
Передача информации	Речь, данные и видео	Речь, данные и видео	Управление передачей речи, данных	Управление передачей речи, данных	Речь и данные
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 дифферен. обслуж. (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, мультисонная, многодоменная поддержка через привратник	Цифр. адресация терминалов пользователей, поддержка IP-адресов и имен доменов для транспор. шлюзов	Цифр. адресация терминалов пользователей, поддержка IP-адресов и имен доменов для транспор. шлюзов	Адреса по Рек.ITU-T E.164, статические
Обнаружение закодированных 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

1.2. Адресация в сетях SIP

Для организации взаимодействия с существующими приложениями IP-сетей и для обеспечения мобильности пользователей протокол SIP использует адрес, подобный адресу электронной почты. В качестве адресов рабочих станций используются специальные универсальные указатели ресурсов – URL (Universal Resource Locators), так называемые SIP URL. SIP-адреса бывают четырех типов

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

Таким образом, адрес состоит из двух частей. Первая часть – это имя пользователя, зарегистрированного в домене 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, рабочей станции или шлюза. Для определения IP-адреса устройства необходимо обратиться к службе доменных имен – Domain Name Service (DNS). Если же во второй части SIP-адреса размещается IP-адрес, то с узлом можно связаться непосредственно.

В начале SIP адреса ставится слово «sip:», указывающее, что это именно SIP-адрес, т.к. бывают и другие (например, «tel:»). Ниже приводятся примеры SIP-адресов:

```
sip: Alexander@niits.ru  
sip: User1@192.168.0.215  
sip: 333-26-27@sip-gateway.ru
```

1.3. Уровни протокола SIP

SIP представляет собой многоуровневый протокол, и если говорится, что элемент сети SIP содержит некий уровень, это означает, что поддерживается группа правил, определенных для этого уровня. Не каждый элемент, работающий по протоколу SIP, содержит все уровни, а сами элементы, специфицированные для работы в сети SIP, являются логическими, а не физическими. Физический элемент

SIP может выполнять функции разных логических элементов в зависимости от возложенных на него обязанностей.

Нижний уровень SIP отвечает за *синтаксис и кодирование*. Кодирование определено с использованием расширенных форм Бэкуса-Наура (Backus-Naur Form, BNF), кратко описанных в [26] в связи с языком SDL. Полное BNF-описание для SIP содержится в RFC 3261, а структура сообщений SIP будет рассмотрена в главе 3 книги.

Второй уровень программной реализации протокола является *транспортным*. Он определяет, как клиент передает запросы и принимает ответы и как сервер получает запросы и передает ответы по сети. Транспортный уровень протокола описан в главе 10.

Третий уровень – *уровень транзакций*. Транзакция – это запрос, переданный клиентской стороной серверной стороне с использованием транспортного уровня SIP, вместе со всеми ответами на этот запрос, переданными серверной стороной клиенту. Уровень транзакций производит повторную передачу сообщений прикладного уровня, определяет соответствие ответов запросу и уведомляет верхний уровень протокола о срабатывании таймера. Любая операция, которую выполняет клиент агента пользователя, реализуется с помощью серии транзакций. В спецификациях протокола SIP определены четыре основных функциональных элемента, которые, в зависимости от конкретных требований, либо реализуются в виде автономных компонентов, либо совмещаются 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.

Прокси-серверы (Proxy servers) могут быть двух типов – с сохранением состояний (stateful) и без сохранения состояний (stateless); эти серверы пересылают сообщения к агентам пользователей и позволяют предоставлять такие функции, как определение местоположения пользователей, авторизация и учет. В эталонной архитектуре Международного консорциума по пакетной коммутации (IPCC) им соответствуют функция маршрутизации и функция учета.

Серверы переадресации (Redirect servers) всегда являются серверами без сохранения состояний. Они просто отвечают на запросы с указанием местоположения – адреса, по которому вызывающий пользователь может связаться прямо с требуемым вызываемым пользователем.

Серверы определения местоположения пользователей (Registration servers) позволяют агентам регистрировать свое местоположение, обеспечивая тем самым реализацию с помощью протокола SIP широкого спектра услуг мобильности.

Как будет показано далее, агенты пользователя UA и прокси-серверы с сохранением состояний транзакций (stateful proxy-servers) содержат уровень транзакций, а прокси-серверы без сохранения состояний (stateless proxy-servers), в противоположность им, уровня транзакций не содержат. Уровень транзакций имеет клиентскую часть, называемую клиентской транзакцией, и серверную часть, называемую серверной транзакцией. Каждая из них представлена конечным автоматом (state machine), связанным с обработкой запроса определенного типа.

Уровень, находящийся выше уровня транзакций, называется *пользователем транзакций (transaction user, TU)*. Каждый из объектов SIP, кроме stateless прокси-сервера, является пользователем транзакций. Когда TU желает дать запрос, он создает отдельную клиентскую транзакцию и передает ей запрос вместе с IP-адресом, данными о портах и о типе транспортного протокола для места назначения, которые определяют, куда нужно отправить запрос. Пользователь транзакций TU, который создал клиентскую транзакцию, может отменить ее. Когда клиент отменяет транзакцию, он запрашивает, чтобы сервер прекратил дальнейшую обработку запроса, возвратился в исходное состояние и передал этой транзакции ответ с определенным кодом ошибки. Это делается посредством запроса CANCEL, который создает собственную транзакцию, но выполняет свои функции в отношении отменяемой транзакции.

1.4. SIP и HTTP

Работу SIP легче всего понять с помощью модели протокола HTTP, на котором он основан. Как SIP, так и HTTP являются протоколами запроса/ответа. Клиент UA, как логический объект протокола, генерирует запросы, а сервер UA, как логический объект протокола, возвращает ответы. Когда клиенту нужен некоторый

Web-сайт, он генерирует запрос в виде URL, например www.niits.ru. Сервер, на котором размещается Web-сайт, передает в ответ Web-страничку NIITS. Протокол SIP использует ту же процедуру. Клиент UA, который передает запрос, называется UAC, а сервер UA, который передает ответ, называется UAS. Такой обмен носит название транзакция SIP.

Таким образом, для UAC протокол SIP определяет процесс создания запроса, для UAS – обработки запроса и создания ответа. Поскольку в протоколе SIP важную роль играет возможность регистрации, UAS, который может работать с запросом REGISTER, имеет свое название – сервер регистрации (registrar). Раздел 4.6 описывает работу ядер UAC и UAS при запросе REGISTER. В разделе 4.8 освещается работа UAC и UAS с запросом OPTIONS, используемым для получения информации о функциональных возможностях UA. Остальные запросы, определенные в базовом документе SIP [57], передаются в режиме диалога.

1.5. Вызовы SIP

Диалог представляет собой равноправное взаимодействие двух агентов пользователя в виде последовательности SIP-сообщений между этими UA. Запрос INVITE является единственным определенным в рекомендации RFC 3261 запросом, устанавливающим диалог. Расширения протокола определили еще два таких запроса – SUBSCRIBE и REFER.

Устройство SIP обычно функционирует и как *клиент* UA (UAC), и как сервер UA (UAS). В качестве UAC устройство SIP может инициировать запросы SIP. В качестве сервера UA устройство может принимать запросы SIP и отвечать на них. Будучи автономным устройством, UA может инициировать и принимать вызовы, которые используют SIP при равноуровневых коммуникациях. На рис. 1.2 представлен простой сценарий диалога между UAC.

Когда UAC передает запрос в режиме диалога, он, помимо выполнения общих правил UAC, описанных в следующей главе, следует правилам работы с запросами в ходе диалога. Раздел 4.1 дает понятие о диалогах и описывает процедуры их создания и поддержания, в дополнение к процедурам создания запросов в режиме диалога.

Первый запрос протокола SIP на рис. 1.2 – сообщение INVITE, которое устанавливает сеанс связи между участниками соединения. Сеанс связи – это совокупность участников соединения и медиапоток между ними, созданных с целью обмена информацией. Раздел 4.10 описывает процедуры создания сеансов, приводящие к созданию одного или более диалогов. Раздел 4.11 повествует о том, как модифицируются параметры сеанса путем применения запроса INVITE в режиме диалога. В разделе 4.12 описано, как разрушается сеанс.

Агент пользователя вызывающей стороны преобразует имя вызываемой стороны в IP-адрес с помощью сервера доменных имен DNS (Domain Name System), доступного через его собственный домен. Команда INVITE передается в порт протокола UDP (User Datagram Protocol) протокола SIP и содержит информацию о формате среды и о том, от кого, кому, через кого передается запрос. Информационный ответ Trying (100) от UA вызываемой стороны аналогичен сообщению CALL PROCEEDING по стандарту Q.931 и означает, что производится маршрутизация вызова. В сценарии непосредственного вызова ответ Trying имеет другое значение, но в моделях прокси и переадресации (redirect) он используется для контроля процесса обработки вызова.

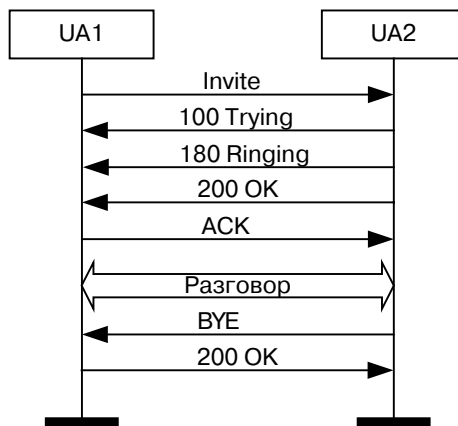


Рис. 1.2. Пример диалога UA

В табл. 1.1 сигнализация Q.931 [25] не представлена, поэтому ниже приведена табл. 1.2 соответствия сигналов SIP и DSS1 интерфейса ISDN.

Таблица 1.2. Соответствие сигналов SIP и DSS1

SIP	DSS1
INVITE	Q.931 SETUP
100 Trying	Q.931 CALL Processing
180 Ringing	Q.931 ALERTING
200 OK	Q.931 CONNECT

Когда вызов (рис. 1.2) поступает на UA2, там срабатывает вызывное устройство терминала и на UA1 передается ответ Ringing (180). Он аналогичен сообщению ALERTING, используемому в DSS1 Q.931. Временной интервал между моментом набора последней цифры и моментом получения вызывающей стороной ответа Ringing называется задержкой после набора номера PDD (postdial delay).

Когда вызываемая сторона отвечает, в UA вызывающей стороны передается ответ 200 OK. Этот UA передает сообщение ACK, подтверждающее получение ответа на запрос INVITE. В подтверждении ACK могут передаваться окончательные параметры SDP, которые поддерживает принимающий окончательный пункт. Сообщения INVITE и 200 OK аналогичны сообщениям SETUP и CONNECT по Q.931.

На этом этапе соединения транспортировка пользовательской информации обеспечивается по протоколу RTCP (*Real-Time Control Protocol*), который обеспечивает также контроль качества соединения и ведет статистику. Затем, как это и следует из его названия, запрос BYE с любой стороны заканчивает сеанс связи. Поскольку все сообщения переданы с помощью UDP, больше никаких действий не требуется.

В следующих главах книги будут представлены более сложные сценарии, но до этого следует подробно рассмотреть понятия UAC и UAS (глава 2) и сообщения протокола SIP (глава 3).

Глава 2. Агент пользователя

2.1. Логический объект Агент пользователя

Основным логическим объектом SIP является агент пользователя *UA (User Agent)*, который может выполнять как функции клиента агента пользователя *UAC (User Agent Client)*, генерирующего запросы, так и функции сервера агента пользователя *UAS (User Agent Server)*, который формирует ответы.

Работа *UAC* и *UAS* зависит от типа запроса и от того, происходит ли передача запроса или ответа в процессе диалога. Описанию агента пользователя посвящена следующая глава справочника.

2.2. Клиент агента пользователя *UAC*

Клиент агента пользователя – это часть программного обеспечения агента пользователя *UA*, которая создает новые запросы, отправляет их и обрабатывает принятые ответы. Запросы генерируются в результате внешних воздействий (нажатия кнопок на SIP-телефоне, сигнала из линии и т.п.).