Глава 7
Протокол инициирования сеансов связи – SIP

7.1 Принципы протокола SIP

Протокол инициирования сеансов – Session Initiation Protocol (SIP) является протоколом прикладного уровня и предназначается для организации, модификации и завершения сеансов связи: мультимедийных конференций, телефонных соединений и распределения мультимедийной информации. Пользователи могут принимать участие в существующих сеансах связи, приглашать других пользователей и быть приглашенными ими к новому сеансу связи. Приглашения могут быть адресованы определенному пользователю, группе пользователей или всем пользователям.

Протокол SIP разработан группой MMUSIC (Multiparty Multimedia Session Control) комитета IETF (Internet Engineering Task Force), а спецификации протокола представлены в документе RFC 2543 [54]. В основу протокола рабочая группа MMUSIC заложила следующие принципы:

Персональная мобильность пользователей. Пользователи могут перемещаться без ограничений в пределах сети, поэтому услуги связи должны предоставляться им в любом месте этой сети. Пользователю присваивается уникальный идентификатор, а сеть предоставляет ему услуги связи вне зависимости от того, где он находится. Для этого пользователь с помощью специального сообщения – **REGISTER** – информирует о своих перемещениях сервер определения местоположения.

Масштабируемость сети. Она характеризуется, в первую очередь, возможностью увеличения количества элементов сети при её расширении. Серверная структура сети, построенной на базе протокола SIP, в полной мере отвечает этому требованию.

Расширяемость протокола. Она характеризуется возможностью дополнения протокола новыми функциями при введении новых услуг и его адаптации к работе с различными приложениями.

В качестве примера можно привести ситуацию, когда протокол SIP используется для установления соединения между шлюзами, взаимодействующими с ТфОП при помощи сигнализации ОКС7 или DSS1. В настоящее время SIP не поддерживает прозрачную передачу сигнальной информации телефонных систем сигнализации. Вследствие этого дополнительные услуги ISDN оказываются недоступными для пользователей IP-сетей.

Расширение функций протокола SIP может быть произведено за счет введения новых заголовков сообщений, которые должны быть зарегистрированы в уже упоминавшейся ранее организации IANA. При этом, если SIP-сервер принимает сообщение с неизвестными ему полями, то он просто игнорирует их и обрабатывает лишь те поля, которые он знает.

Для расширения возможностей протокола SIP могут быть также добавлены и новые типы сообщений.

Интеграция в стек существующих протоколов Интернет, разработанных IETF. Протокол SIP является частью глобальной архитектуры мультимедиа, разработанной комитетом Internet Engineering Task Force (IETF). Эта архитектура включает в себя также протокол резервирования ресурсов (Resource Reservation Protocol – RSVP, RFC 2205), транспортный протокол реального времени (Real-Time Transport Protocol – RTP, RFC 1889), протокол передачи потоковой информации в реальном времени (Real-Time Streaming Protocol – RTSP, RFC 2326), протокол описания параметров связи (Session Description Protocol – SDP, RFC 2327). Однако функции протокола SIP не зависят ни от одного из этих протоколов.

Взаимодействие с другими протоколами сигнализации. Протокол SIP может быть использован совместно с протоколом H.323 (Главы 5 и 6). Возможно также взаимодействие протокола SIP с системами сигнализации ТфОП – DSS1 и ОКС7 [6,7]. Для упрощения такого взаимодействия сигнальные сообщения протокола SIP могут переносить не только специфический SIP-адрес, но и телефонный номер формата E.164 или любого другого формата. Кроме того, протокол SIP, наравне с протоколами H.323 и ISUP/IP, может применяться для синхронизации работы устройств управления шлюзами, о чем пойдет речь в следующей главе (рис. 8.2); в этом случае он должен взаи-

модействовать с протоколом MGCP. Другой важной особенностью протокола SIP является то, что он приспособлен к организации доступа пользователей сетей IP-телефонии к услугам интеллектуальных сетей [8], и существует мнение, что именно этот протокол станет основным при организации связи между указанными сетями.

7.2 Интеграция протокола SIP с IP-сетями

Одной из важнейших особенностей протокола SIP является его независимость от транспортных технологий. В качестве транспорта могут использоваться протоколы X.25, Frame Relay, AAL5/ATM, IPX и др. Структура сообщений SIP не зависит от выбранной транспортной технологии. Но, в то же время, предпочтение отдается технологии маршрутизации пакетов IP и протоколу UDP. При этом, правда, необходимо создать дополнительные механизмы для надежной доставки сигнальной информации. К таким механизмам относятся повторная передача информации при ее потере, подтверждение приема и др.

Здесь же следует отметить то, что сигнальные сообщения могут переноситься не только протоколом транспортного уровня UDP, но и протоколом TCP. Протокол UDP позволяет быстрее, чем TCP, доставлять сигнальную информацию (даже с учетом повторной передачи неподтвержденных 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 (firewall), а также 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 открываться отдельное TCP-соединение. На рисунке 7.1 показано место, занимаемое протоколом SIP в стеке протоколов TCP/IP.

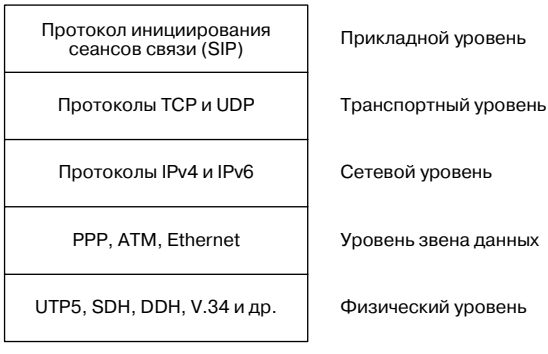

Рис. 7.1 Место протокола SIP в стеке протоколов TCP/IP

По сети с маршрутизацией пакетов IP может передаваться пользовательская информация практически любого вида: речь, видео и данные, а также любая их комбинация, называемая мультимедийной информацией. При организации связи между терминалами пользователей необходимо известить встречную сторону, какого рода информация может приниматься (передаваться), алгоритм ее кодирования и адрес, на который следует передавать информацию. Таким образом, одним из обязательных условий организации связи при помощи протокола SIP является обмен между сторонами данными об их функциональных возможностях. Для этой цели чаще всего используется протокол описания сеансов связи – SDP (Session Description Protocol). Поскольку в течение сеанса связи может производиться его модификация, предусмотрена передача сообщений SIP с новыми описаниями сеанса средствами SDP. Более подробно протокол SDP рассмотрен в главе 8.

Для передачи речевой информации комитет IETF предлагает использовать протокол RTP, рассмотренный в главе 4 настоящей книги, но сам протокол SIP не исключает возможность применения для этих целей других протоколов.

В протоколе SIP не реализованы механизмы управления потоками информации и предоставления гарантированного качества обслуживания. Кроме того, протокол SIP не предназначен для передачи пользовательской информации, в его сообщениях может переноситься информация лишь ограниченного объема. При переносе через сеть слишком большого сообщения SIP не исключена его фрагментация на уровне IP, что может повлиять на качество передачи информации.

В глобальной информационной сети Интернет уже довольно давно функционирует экспериментальный участок Mbone, который образован из сетевых узлов, поддерживающих режим многоадресной рассылки мультимедийной информации. Важнейшей функцией Mbone является поддержка мультимедийных конференций, а основным способом приглашения участников к конференции стал протокол SIP.

Протокол SIP предусматривает организацию конференций трех видов:

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

- путем соединения каждого пользователя с каждым в режиме точка-точка.

Протокол SIP дает возможность присоединения новых участников к уже существующему сеансу связи, т.е. двусторонний сеанс может перейти в конференцию.

И, в заключение рассказа об интеграции протокола SIP с IP-сетями, следует отметить то, что разработаны методы совместной работы этого протокола с преобразователем сетевых адресов – Network Address Translator (NAT).

7.3 Адресация

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 рабочей станцией можно связаться напрямую.

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

sip: als@rts.loniis.ru

sip: user1@192.168.100.152

sip: 294-75-47@gateway.ru

7.4 Архитектура сети SIP

В некотором смысле прародителем протокола SIP является протокол переноса гипертекста – HTTP (Hypertext Transfer Protocol, RFC 2068). Протокол SIP унаследовал от него синтаксис и архитектуру «клиент-сервер», которую иллюстрирует рис. 7.2.

Рис. 7.2 Архитектура "клиент-сервер"

Клиент выдает запросы, в которых указывает, что он желает получить от сервера. Сервер принимает запрос, обрабатывает его и выдает ответ, который может содержать уведомление об успешном выполнении запроса, уведомление об ошибке или информацию, затребованную клиентом.

Управление процессом обслуживания вызова распределено между разными элементами сети SIP. Основным функциональным элементом, реализующим функции управления соединением, является терминал. Остальные элементы сети отвечают за маршрутизацию вызовов, а в некоторых случаях предоставляют дополнительные услуги.

7.4.1 Терминал

В случае, когда клиент и сервер взаимодействуют непосредственно с пользователем (т.е. реализованы в оконечном оборудовании пользователя), они называются, соответственно, клиентом агента пользователя – User Agent Client (UAC) – и сервером агента пользователя – User Agent Server (UAS).

Следует особо отметить, что сервер UAS и клиент UAC могут (но не обязаны) непосредственно взаимодействовать с пользователем, а другие клиенты и серверы SIP этого делать не могут. Если в устройстве присутствуют и сервер UAS, и клиент UAC, то оно называется агентом пользователя – User Agent (UA), а по своей сути представляет собой терминальное оборудование SIP.

Кроме терминалов определены два основных типа сетевых элементов SIP: прокси-сервер (proxy server) и сервер переадресации (redirect server).

7.4.2 Прокси-сервер

Прокси-сервер (от английского proxy – представитель) представляет интересы пользователя в сети. Он принимает запросы, обрабатывает их и, в зависимости от типа запроса, выполняет определенные действия. Это может быть поиск и вызов пользователя, маршрутизация запроса, предоставление услуг и т.д. Прокси-сервер состоит из клиентской и серверной частей, поэтому может принимать вызовы, инициировать собственные запросы и возвращать ответы. Прокси-сервер может быть физически совмещен с сервером определения местоположения (в этом случае он называется registrar) или существовать отдельно от этого сервера, но иметь возможность взаимодействовать с ним по протоколам LDAP (RFC 1777), rwhois (RFC 2167) и по любым другим протоколам.

Предусмотрено два типа прокси-серверов – с сохранением состояний (stateful) и без сохранения состояний (stateless).

Сервер первого типа хранит в памяти входящий запрос, который явился причиной генерации одного или нескольких исходящих запросов. Эти исходящие запросы сервер также запоминает. Все запросы хранятся в памяти сервера только до окончания транзакции, т.е. до получения ответов на запросы.

Сервер первого типа позволяет предоставить большее количество услуг, но работает медленнее, чем сервер второго типа. Он может применяться для обслуживания небольшого количества клиентов, например, в локальной сети. Прокси-сервер должен сохранять информацию о состояниях, если он:

– использует протокол TCP для передачи сигнальной информации;
– работает в режиме многоадресной рассылки сигнальной информации;
– размножает запросы.

Последний случай имеет место, когда прокси-сервер ведет поиск вызываемого пользователя сразу в нескольких направлениях, т.е. один запрос, который пришел к прокси-серверу, размножается и передается одновременно по всем этим направлениям.

Сервер без сохранения состояний просто ретранслирует запросы и ответы, которые получает. Он работает быстрее, чем сервер первого типа, так как ресурс процессора не тратится на запоминание состояний, вследствие чего сервер этого типа может обслужить большее количество пользователей. Недостатком такого сервера является то, что на его базе можно реализовать лишь наиболее простые услуги. Впрочем, прокси-сервер может функционировать как сервер с сохранением состояний для одних пользователей и как сервер без сохранения состояний – для других.

Алгоритм работы пользователей с прокси-сервером выглядит следующим образом. Поставщик услуг IP-телефонии сообщает ад-

рес прокси-сервера своим пользователям. Вызывающий пользователь передает к прокси-серверу запрос соединения. Сервер обрабатывает запрос, определяет местоположение вызываемого пользователя и передает запрос этому пользователю, а затем получает от него ответ, подтверждающий успешную обработку запроса, и транслирует этот ответ пользователю, передавшему запрос. Прокси-сервер может модифицировать некоторые заголовки сообщений, которые он транслирует, причем каждый сервер, обработавший запрос в процессе его передачи от источника к приемнику, должен указать это в SIP-запросе для того, чтобы ответ на запрос вернулся по такому же пути.

7.4.3 Сервер переадресации

Сервер переадресации предназначен для определения текущего адреса вызываемого пользователя. Вызывающий пользователь передает к серверу сообщение с известным ему адресом вызываемого пользователя, а сервер обеспечивает переадресацию вызова на текущий адрес этого пользователя. Для реализации этой функции сервер переадресации должен взаимодействовать с сервером определения местоположения.

Сервер переадресации не терминирует вызовы как сервер RAS и не инициирует собственные запросы как прокси-сервер. Он только сообщает адрес либо вызываемого пользователя, либо прокси-сервера. По этому адресу инициатор запроса передает новый запрос. Сервер переадресации не содержит клиентскую часть программного обеспечения.

Но пользователю не обязательно связываться с каким-либо SIP-сервером. Он может сам вызвать другого пользователя при условии, что знает его текущий адрес.

7.4.4 Сервер определения местоположения пользователей

Пользователь может перемещаться в пределах сети, поэтому необходим механизм определения его местоположения в текущий момент времени. Например, сотрудник предприятия уезжает в командировку, и все вызовы, адресованные ему, должны быть направлены в другой город на его временное место работы. О том, где он находится, пользователь информирует специальный сервер с помощью сообщения **REGISTER**. Возможны два режима регистрации: пользователь может сообщить свой новый адрес один раз, а может регистрироваться периодически через определенные промежутки времени. Первый способ подходит для случая, когда терминал, доступный пользователю, включен постоянно, и его не перемещают по сети, а второй – если терминал часто перемещается или выключается.

Для хранения текущего адреса пользователя служит *сервер определения местоположения пользователей,* представляющий собой базу данных адресной информации. Кроме постоянного адреса пользователя, в этой базе данных может храниться один или несколько текущих адресов.

Этот сервер может быть совмещен с прокси-сервером (в таком случае он называется registrar) или быть реализован отдельно от прокси-сервера, но иметь возможность связываться с ним.

В RFC 2543 сервер определения местоположения представлен как отдельный сетевой элемент, но принципы его работы в этом документе не регламентированы. Стоит обратить внимание на то, что вызывающий пользователь, которому нужен текущий адрес вызываемого пользователя, не связывается с сервером определения местоположения напрямую. Эту функцию выполняют SIP-серверы при помощи протоколов LDAP (RFC 1777), rwhois (RFC 2167), или других протоколов.

7.4.5 Пример SIP- сети

Резюмируя все сказанное выше, отметим, что сети SIP строятся из элементов трех основных типов: терминалов, прокси-серверов и серверов переадресации. На рис. 7.3 приведен пример возможного построения сети SIP.

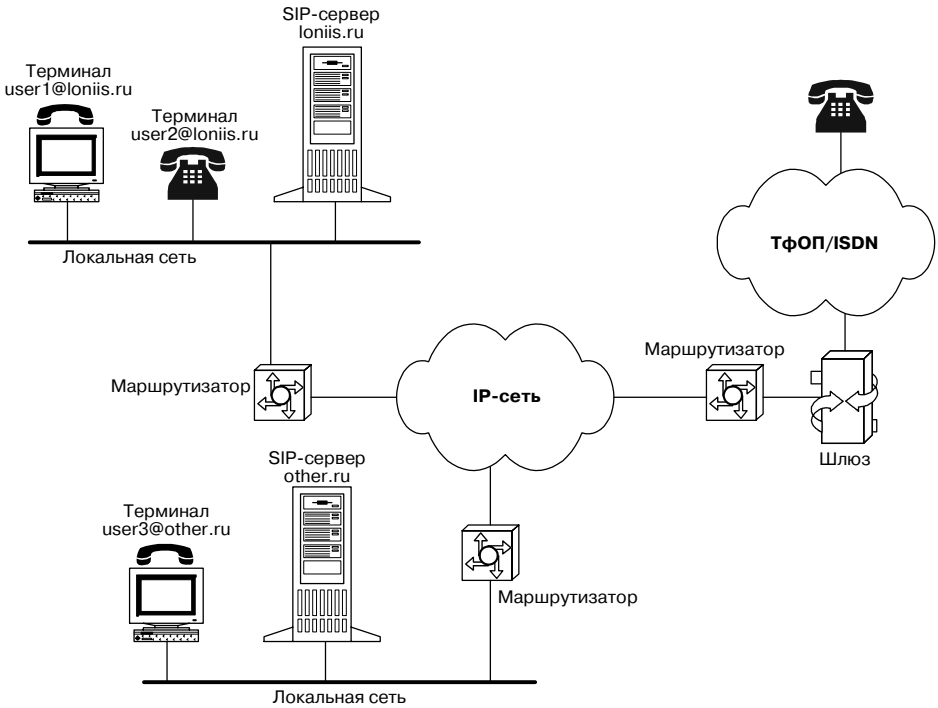

Рис. 7.3 Пример построения сети SIP

Стоит обратить внимание на то что, что SIP-серверы, представленные на рис. 7.3, являются отдельными функциональными сетевыми элементами. Физически они могут быть реализованы на базе серверов локальной сети, которые, помимо выполнения своих основных функций, будут также обрабатывать SIP-сообщения. Терминалы же могут быть двух типов: персональный компьютер со звуковой платой и программным обеспечением SIP-клиента (UA) или SIP-телефон, подключающийся непосредственно к ЛВС Ethernet (SIP-телефоны, производимые компанией Cisco Systems, недавно появились на российском рынке). Таким образом, пользователь локальной вычислительной сети передает все запросы к своему SIP-серверу, а тот обрабатывает их и обеспечивает установление соединений. Путем программирования сервер можно настроить на разные алгоритмы работы: он может обслуживать часть пользователей (например, руководство предприятия или особо важных лиц) по одним правилам, а другую часть – по иным. Возможно также, что сервер будет учитывать категорию и срочность вызовов, а также вести начисление платы за разговоры.

Структурная схема организации услуг SIP-сервера представлена на рисунке 7.4.

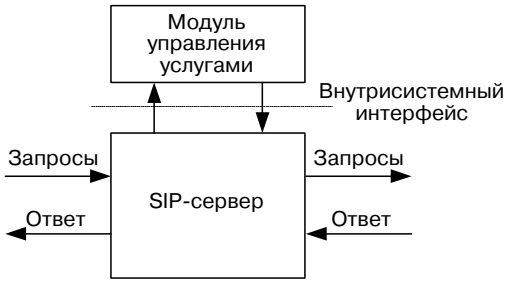

Рис. 7.4 Структурная схема организации услуг SIP-сервера

Модуль управления услугами отвечает за предоставление услуг и за общее управление сервером. Принятые сервером запросы и ответы поступают в модуль управления услугами и обрабатываются им, на основании чего определяется реакция на полученные сообщения. Интерфейс человек-машина позволяет гибко менять настройки сервера и вести мониторинг сети.

7.5 Сообщения протокола SIP

7.5.1 Структура сообщений

Согласно архитектуре «клиент-сервер» все сообщения делятся на запросы, передаваемые от клиента к серверу, и на ответы сервера клиенту.

Например, чтобы инициировать установление соединения, вызывающий пользователь должен сообщить серверу ряд параметров, в частности, адрес вызываемого пользователя, параметры информационных каналов и др. Эти параметры передаются в специальном SIP-запросе. От вызываемого пользователя к вызывающему передается ответ на запрос, также содержащий ряд параметров.

Все сообщения протокола SIP (запросы и ответы), представляют собой последовательности текстовых строк, закодированных в соответствии с документом RFC 2279. Структура и синтаксис сообщений SIP, как уже упоминалось ранее, идентичны используемым в протоколе HTTP. На рисунке 7.5 представлена структура сообщений протокола SIP.

Рис. 7.5 Структура сообщений протокола SIP

Стартовая строка представляет собой начальную строку любого SIP-сообщения. Если сообщение является запросом, в этой строке указываются тип запроса, адресат и номер версии протокола. Если сообщение является ответом на запрос, в стартовой строке указываются номер версии протокола, тип ответа и его короткая расшифровка, предназначенная только для пользователя.

Заголовки сообщений содержат сведения об отправителе, адресате, пути следования и др., в общем, переносят информацию, необходимую для обслуживания данного сообщения. О типе заголовка можно узнать по его имени. Оно не зависит от регистра (т.е. буквы могут быть прописные и строчные), но обычно имя пишут с большой буквы, за которой идут строчные.

Сообщения протокола SIP могут содержать так называемое тело сообщения. В запросах **ACK**, **INVITE** и **OPTIONS** тело сообщения содержит описание сеансов связи, например, в формате протокола SDP. Запрос **BYE** тела сообщения не содержит, а ситуация с запро-

сом **REGISTER** подлежит дальнейшему изучению. С ответами дело обстоит иначе: любые ответы могут содержать тело сообщения, но содержимое тела в них бывает разным.

7.5.2 Заголовки сообщений

В протоколе SIP определено четыре вида заголовков (Таблица 7.1):

- *Общие заголовки*, присутствующие в запросах и ответах;
- *Заголовки содержания,* переносят информацию о размере тела сообщения или об источнике запроса (начинаются со слова «**Content**»);
- *Заголовки запросов*, передающие дополнительную информацию о запросе;
- *Заголовки ответов*, передающие дополнительную информацию об ответе.

Заголовок содержит название, за которым, отделенное двоеточием, следует значение заголовка. В поле значения содержатся передаваемые данные. Следует отметить, что если сервер принимает сообщения, заголовки которых ему не известны, то эти заголовки игнорируются.

Ниже представлены наиболее часто используемые заголовки.

Заголовок **Call-ID** – уникальный идентификатор сеанса связи или всех регистраций отдельного клиента, он подобен метке соединения (call reference) в сигнализации DSS-1 [7]. Значение идентификатору присваивает сторона, которая инициирует 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@rts.loniis.ru** Возможна следующая ситуация: к одной мультимедийной конференции относятся несколько соединений, тогда все они будут иметь разные идентификаторы **Call-ID**.

Заголовок **To** – определяет адресата. Кроме SIP-адреса здесь может стоять параметр «**tag**» для идентификации конкретного терминала пользователя (например, домашнего, рабочего или сотового телефона) в том случае, когда все его терминалы зарегистрированы под одним адресом SIP URL. Запрос может множиться и достичь разных терминалов пользователя; чтобы их различать, необходимо иметь метку **tag**. Ее вставляет в заголовок терминальное оборудование вызванного пользователя при ответе на принятый запрос.

Если необходим визуальный вывод имени пользователя, например, на дисплей, то имя пользователя также размещается в поле **To**.

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

Таблица 7.1 Виды заголовков сообщений SIP

Общие заголовки	**Заголовки содержания**	**Заголовки запросов**	**Заголовки ответов**
Call-ID (идентификатор сеанса связи)	Content-Encoding (кодирование тела сообщения)	Accept (принимается)	Allow (разрешение)
Contact (контактировать)	Content-Length (размер тела сообщения)	Accept-Encoding (метод кодирования поддерживается)	Proxy-Authenticate (подтверждение подлинности прокси-сервера)
CSeq (последовательность)	Content-Type (тип содержимого)	Accept-Language (язык поддерживается)	Retry-After (повторить через некоторое время)
Date (Дата)		Authorization (авторизация)	Server (сервер)
Encryption (шифрование)			Unsupported (не поддерживается)
Expires (срабатывание таймера)		Hide (скрыть)	Warning (предупреждение)
From (источник запроса)		Max-Forwards (максимальное количество переадресаций)	WWW-Authenticate (подтверждение подлинности WWW-сервера)
Record-Route (запись маршрута)		Organization (организация)	
Timestamp (метка времени)		Priority (приоритет)	
To (Адресат)		Proxy-Authorization (авторизация прокси-сервера)	
Via (через)		Proxy-Require (требуется прокси-сервер)	
		Route (маршрут)	
		Require (требуется)	
		Response-Key (ключ кодирования ответа)	
		Subject (тема)	
		User-Agent (агент пользователя)	

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 из диапазона от 1 до 2^{32} и типа запроса. Сервер должен проверять значение **CSeq** в каждом принимаемом запросе и считать запрос новым, если значение **CSeq** больше предыдущего. Пример заголовка: **CSeq: 2 INVITE.**

Заголовок **Via** служит для того, чтобы избежать ситуации, в которых запрос пойдет по замкнутому пути, а также для тех случаяев, когда необходимо, чтобы запросы и ответы обязательно проходили по одному и тому же пути (например, в случае использования 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, и так до тех пор, пока запрос не достигнет адресата. Таким образом, в заголовке **Via** указывается весь путь, пройденный запросом: каждый прокси-сервер добавляет поле со своим адресом. При необходимости (например, чтобы обеспечить секретность) действительный адрес может скрываться.

Например, запрос на своем пути обрабатывался двумя прокси-серверами: сначала сервером loniis.ru, потом sip.telecom.com. Тогда в запросе появятся следующие поля:

Via: SIP/2.0/UDP sip.telecom.com:5060;branch=721e418c4.1
Via: SIP/2.0/UDP loniis.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 следующим образом: **721e418c4.1**.

Содержимое полей **Via** копируется из запросов в ответы на них, и каждый сервер, через который проходит ответ, удаляет поле **Via** со своим именем.

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

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

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

После того, как мы рассмотрели наиболее часто встречающиеся заголовки сообщений протокола SIP, следует обратить внимание на то, что запросы и ответы на них могут включать в себя лишь определенный набор заголовков (Таблица 7.2). Здесь опять буква «M» означает обязательное присутствие заголовка в сообщении, буква «O» – необязательное присутствие, буква «F» запрещает присутствие заголовка.

Таблица 7.2 Связь заголовков с запросами и ответами протокола SIPv2.0

Название заголовка	Место использования заголовка	ACK	BYE	CAN	INV	OPT	REG
Accept	Заголовок в запросах	F	F	F	O	O	O
Accept	Заголовок в ответе 415	F	F	F	O	O	O
Accept-Encoding	Заголовок в запросах	F	F	F	O	O	O
Accept-Encoding	Заголовок в ответе 415	F	F	F	O	O	O
Accept-Language	Заголовок в запросах	F	O	O	O	O	O
Accept-Language	Заголовок в ответе 415	F	O	O	O	O	O
Allow	Заголовок в ответе 200	F	F	F	F	M	F
Allow	Заголовок в ответе 405	O	O	O	O	O	O
Authorization	Заголовок в запросах	O	O	O	O	O	O
Call-ID	Общий заголовок - копируется из запросов в ответы	M	M	M	M	M	M
Contact	Заголовок в запросах	O	F	F	O	O	O
Contact	Заголовок в ответах 1xx	F	F	F	O	O	F
Contact	Заголовок в ответах 2xx	F	F	F	O	O	O
Contact	Заголовок в ответах 3xx	F	O	F	O	O	O
Contact	Заголовок в ответе 485	F	O	F	O	O	O
Content-Encoding	Заголовки содержания	O	F	F	O	O	O
Content-Length	Заголовки содержания	O	F	F	O	O	O
Content-Type	Заголовки содержания	*	F	F	*	*	*
Cseq	Общий заголовок - копируется из запросов в ответы	M	M	M	M	M	M
Date	Заголовок в ответах	O	O	O	O	O	O
Encryption	Заголовок в ответах	O	O	O	O	O	O
Expires	Заголовок в ответах	F	F	F	O	F	O
From	Общий заголовок - копируется из запросов в ответы	M	M	M	M	M	M
Hide	Заголовок в запросах	O	O	O	O	O	O
Max-Forwards	Заголовок в запросах	O	O	O	O	O	O
Organization	Общий заголовок	F	F	F	O	O	O
Proxy-Authenticate	Заголовок в ответе 407	O	O	O	O	O	O
Proxy-Authorization	Заголовок в запросах	O	O	O	O	O	O
Proxy-Require	Заголовок в запросах	O	O	O	O	O	O
Priority	Заголовок в запросах	F	F	F	O	F	F
Require	Заголовок в запросах	O	O	O	O	O	O
Retry-After	Заголовок в запросах	F	F	F	F	F	O
Retry-After	Заголовок в ответах 404, 480, 486, 503, 600 и 603	O	O	O	O	O	O
Response-Key	Заголовок в запросах	F	O	O	O	O	O
Record-Route	Заголовок в запросах	O	O	O	O	O	O
Record-Route	Заголовок в ответах 2xx	O	O	O	O	O	O
Route	Заголовок в запросах	O	O	O	O	O	O
Server	Заголовок в ответах	O	O	O	O	O	O
Subject	Заголовок в запросах	F	F	F	O	F	F
Timestamp	Общий заголовок	O	O	O	O	O	O
To	Общий заголовок - копируется из запросов в ответы	M	M	M	M	M	M
Unsupported	Заголовок в ответе 420	O	O	O	O	O	O
User-Agent	Общий заголовок	O	O	O	O	O	O
Via	Общий заголовок - копируется из запросов в ответы	M	M	M	M	M	M
Warning	Заголовок в ответах	O	O	O	O	O	O
WWW-Authenticate	Заголовок в ответе 401	O	O	O	O	O	O

* Примечание – поле необходимо только в случае, когда тело сообщения содержит какую-либо информацию, т.е. не является пустым.

7.5.3 Запросы

В настоящей версии протокола SIP определено шесть типов запросов. Каждый из них предназначен для выполнения довольно широкого круга задач, что является явным достоинством протокола SIP, так как благодаря этому число сообщений, которыми обмениваются терминалы и серверы, сведено к минимуму. С помощью запросов клиент сообщает о 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 той же строке в поле **Request-URI** указан SIP-адрес оборудования, которому этот запрос адресован. Содержание полей **To** и **Request-URI** может различаться, например, в поле **To** может быть указан публикуемый адрес абонента, а в поле **Request-URI** – текущий адрес пользователя.

Запрос **INVITE** приглашает пользователя принять участие в сеансе связи. Он обычно содержит описание сеанса связи, в котором указывается вид принимаемой информации и параметры (список возможных вариантов параметров), необходимые для приема информации, а также может указываться вид информации, которую вызываемый пользователь желает передавать. В ответе на запрос типа **INVITE** указывается вид информации, которая будет приниматься вызываемым пользователем, и, кроме того, может указываться вид информации, которую вызываемый пользователь собирается передавать (возможные параметры передачи информации).

В этом сообщении могут содержаться также данные, необходимые для аутентификации абонента, и, следовательно, доступа клиентов к SIP-серверу. При необходимости изменить характеристики уже организованных каналов передается запрос **INVITE** с новым описанием сеанса связи. Для приглашения нового участника к уже установленному соединению также используется сообщение **INVITE**.

Запрос **ACK** подтверждает прием ответа на запрос **INVITE.** Следует отметить, что запрос **ACK** используется только совместно с запросом **INVITE**, т.е. этим сообщением оборудование вызывающего пользователя показывает, что оно получило окончательный ответ на свой запрос **INVITE**. В сообщении **ACK** может содержаться окончательное описание сеанса связи, передаваемое вызывающим пользователем.

Запрос **CANCEL** отменяет обработку ранее переданных запросов с теми же, что и в запросе **CANCEL,** значениями полей **Call-ID, To, From** и **CSeq**, но не влияет на те запросы, обработка которых уже завершена. Например, запрос **CANCEL** применяется тогда, когда прокси-сервер размножает запросы для поиска пользователя по нескольким направлениям и в одном из них его находит. Обработку

запросов, разосланных во всех остальных направлениях, сервер отменяет при помощи сообщения **CANCEL**.

Запросом **BYE** оборудование вызываемого или вызывающего пользователя завершает соединение. Сторона, получившая запрос **BYE**, должна прекратить передачу речевой (мультимедийной) информации и подтвердить его выполнение ответом **200 OK**.

При помощи запроса типа **REGISTER** пользователь сообщает свое текущее местоположение. В этом сообщении содержатся следующие поля:

- Поле **To** содержит адресную информацию, которую надо сохранить или модифицировать на сервере;
- Поле **From** содержит адрес инициатора регистрации. Зарегистрировать пользователя может либо он сам, либо другое лицо, например, секретарь может зарегистрировать своего начальника;
- Поле **Contact** содержит новый адрес пользователя, по которому должны передаваться все дальнейшие запросы **INVITE**. Если в запросе **REGISTER** поле **Contact** отсутствует, то регистрация остается прежней. В случае отмены регистрации здесь помещается символ «*»;
- В поле **Expires** указывается время в секундах, в течение которого регистрация действительна. Если данное поле отсутствует, то по умолчанию назначается время – 1 час, после чего регистрация отменяется. Регистрацию можно также отменить, передав сообщение **REGISTER** с полем **Expires**, которому присвоено значение 0, и с соответствующим полем **Contact.**

Запросом **OPTIONS** вызываемый пользователь запрашивает информацию о функциональных возможностях терминального оборудования вызываемого пользователя. В ответ на этот запрос оборудование вызываемого пользователя сообщает требуемые сведения. Применение запроса **OPTIONS** ограничено теми случаями, когда необходимо узнать о функциональных возможностях оборудования до установления соединения. Для установления соединения запрос этого типа не используется.

После испытаний протокола SIP в реальных сетях оказалось, что для решения ряда задач вышеуказанных шести типов запросов недостаточно. Поэтому возможно, что в протокол будут введены новые сообщения. Так, в текущей версии протокола SIP не предусмотрен способ передачи информации управления соединением или другой информации во время сеанса связи. Для решения этой задачи был предложен новый тип запроса – **INFO**. Он может использоваться в следующих случаях:

- для переноса сигнальных сообщений ТфОП/ISDN/сотовых сетей между шлюзами в течение разговорной сессии;

- для переноса сигналов DTMF в течение разговорной сессии;
- для переноса биллинговой информации.

Завершив описание запросов протокола SIP, рассмотрим, в качестве примера, типичный запрос типа **INVITE** (рис. 7.6).

```
INVITE sip: watson@boston.bell-tel.com SIP/2.0
         Via: SIP/2.0/UDP kton.bell-tel.com
         From: A. Bell <sip: a.g.bell@bell-tel.com>
         To: T. Watson <sip: watson@bell-tel.com>
         Call-ID: 3298420296@kton.bell-tel.com
         Cseq: 1 INVITE
         Content-Type: application/sdp
         Content-Length: ...

         v=0
         o=bell 53655765 2353687637 IN IP4 128.3.4.5
         C=IN IP4 kton.bell-tel.com
         m=audio 3456 RTP/AVP 0 3 4 5
```

Рис. 7.6 Пример запроса INVITE

В этом примере пользователь Bell (a.g.bell@bell-tel.com) вызывает пользователя Watson (watson@bell-tel.com). Запрос передается к прокси-серверу (boston.bell-tel.com). В полях **To** и **From** перед адресом стоит запись, которую вызывающий пользователь желает вывести на дисплей вызываемого пользователя. В теле сообщения оборудование вызывающего пользователя указывает в формате протокола SDP, что оно может принимать в порту 3456 речевую информацию, упакованную в пакеты RTP и закодированную по одному из следующих алгоритмов кодирования: 0 – PCMU, 3 – GSM, 4 – G.723 и 5 – DVI4.

При передаче сообщений протокола SIP, упакованных в сигнальные сообщения протокола UDP, существует вероятность того, что размер запроса или ответа окажется больше максимально допустимого для данной сети, и произойдет фрагментация пакета. Чтобы избежать этого, используется сжатый формат имен основных заголовков, подобно тому, как это делается в протоколе SDP. Ниже приведен список таких заголовков (Таблица 7.3).

Таблица 7.3 Сжатые имена заголовков

Сжатая форма имени	Полная форма имени
c	Content-Type
e	Content-Encoding
f	From
i	Call-ID
m	Contact (от "moved")
l	Content-Length
s	Subject
t	To
v	Via

При написании имен заголовков в сжатом виде сообщение **INVITE**, показанное ранее на рисунке 6, будет выглядеть следующим образом (рис. 7.7):

```
INVITE sip: watson@boston.bell-tel.com SIP/2.0
         v: SIP/2.0/UDP kton.bell-tel.com
         f: A. Bell <sip: a.g.bell@bell-tel.com>
         t: T. Watson <sip: watson@bell-tel.com>
         i: 3298420296@kton.bell-tel.com
         Cseq: 1 INVITE
         c: application/sdp
         l: ...

         v=0
         o=bell 53655765 2353687637 IN IP4 128.3.4.5
         C=IN IP4 kton.bell-tel.com
         m=audio 3456 RTP/AVP 0 3 4 5
```

Рис. 7.7 Пример запроса INVITE с сокращенными заголовками

В заключение параграфа, как и в предыдущих главах, сведем все запросы, с их кратким описанием, в таблицу 7.4.

Таблица 7.4 Запросы SIP

Тип запроса	Описание запроса
INVITE	Приглашает пользователя к сеансу связи. Содержит SDP-описание сеанса
ACK	Подтверждает прием окончательного ответа на запрос **INVITE**
BYE	Завершает сеанс связи. Может быть передан любой из сторон, участвующих в сеансе
CANCEL	Отменяет обработку запросов с теми же заголовками **Call-ID**, **To**, **From** и **CSeq**, что и в самом запросе **CANCEL**
REGISTER	Переносит адресную информацию для регистрации пользователя на сервере определения местоположения
OPTION	Запрашивает информацию о функциональных возможностях терминала

7.5.4 Ответы на запросы

После приема и интерпретации запроса, адресат (прокси-сервер) передает ответ на этот запрос. Содержание ответов бывает разным: подтверждение установления соединения, передача запрошенной информации, сведения о неисправностях и т.д. Структуру ответов и их виды протокол SIP унаследовал от протокола HTTP.

Определено шесть типов ответов, несущих разную функциональную нагрузку. Тип ответа кодируется трехзначным числом. Самой важной является первая цифра, которая определяет класс ответа, остальные две цифры лишь дополняют первую. В некоторых случаях оборудование даже может не знать все коды ответов, но оно обязательно должно интерпретировать первую цифру ответа.

Все ответы делятся на две группы: информационные и финальные. Информационные ответы показывают, что запрос находится в стадии обработки. Они кодируются трехзначным числом, начинающимся с единицы, – **1xx**. Некоторые информационные ответы, например, **100 Trying**, предназначены для установки на нуль таймеров, которые запускаются в оборудовании, передавшем запрос. Если к моменту срабатывания таймера ответ на запрос не получен, то считается, что этот запрос потерян и может (по усмотрению производителя) быть передан повторно. Один из распространенных ответов – **180 Ringing**; по назначению он идентичен сигналу «Контроль посылки вызова» в ТфОП и означает, что вызываемый пользователь получает сигнал о входящем вызове.

Финальные ответы кодируются трехзначными числами, начинающимися с цифр 2, 3, 4, 5 и 6. Они означают завершение обработки запроса и содержат, когда это нужно, результат обработки запроса. Назначение финальных ответов каждого типа рассматривается ниже.

Ответы **2xx** означают, что запрос был успешно обработан. В настоящее время из всех ответов типа **2xx** определен лишь один – **200 OK**. Его значение зависит от того, на какой запрос он отвечает:

- ответ **200 OK** на запрос **INVITE** означает, что вызываемое оборудование согласно на участие в сеансе связи; в теле ответа указываются функциональные возможности этого оборудования;
- ответ **200 OK** на запрос **BYE** означает завершение сеанса связи, в теле ответа никакой информации не содержится;
- ответ **200 OK** на запрос **CANCEL** означает отмену поиска, в теле ответа никакой информации не содержится;
- ответ **200 OK** на запрос **REGISTER** означает, что регистрация прошла успешно;
- ответ **200 OK** на запрос **OPTION** служит для передачи сведений о функциональных возможностях оборудования, эти сведения содержатся в теле ответа.

Ответы **3xx** информируют оборудование вызывающего пользователя о новом местоположении вызываемого пользователя или переносят другую информацию, которая может быть использована для нового вызова:

- в ответе **300 Multiple Choices** указывается несколько SIP-адресов, по которым можно найти вызываемого пользователя, и 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 Temporary** означает, что пользователь временно (промежуток времени может быть указан в поле Expires) находится по другому адресу, который указывается в поле Contact.

Ответы **4xx** 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 наличия в нем синтаксических ошибок;
- 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 адреса не обслуживаются и т.д.;
- ответ **485 Ambiguous** означает, что адрес в запросе не определяет вызываемого пользователя однозначно;
- ответ **486 Busy Here** означает, что вызываемый пользователь в настоящий момент не может принять входящий вызов по данному адресу. Ответ не исключает возможности связаться с пользователем по другому адресу или, к примеру, оставить сообщение в речевом почтовом ящике.

Ответы **5xx** информируют о том, что запрос не может быть обработан из-за отказа 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 функции, необходимые для обслуживания этого запроса. Ответ передается, например в том случае, когда сервер не может распознать тип запроса;
- ответ **502 Bad Gateway** информирует о том, что сервер, функционирующий в качестве шлюза или прокси-сервера, принял некорректный ответ от сервера, к которому он направил запрос;
- ответ **503 Service Unavailable** говорит от том, что сервер не может в данный момент обслужить вызов вследствие перегрузки или проведения технического обслуживания.

Ответы **6xx** информируют о том, что соединение с вызываемым пользователем установить невозможно:

- ответ **600 Busy Everywhere** сообщает, что вызываемый пользователь занят и не может принять вызов в данный момент ни по одному из имеющихся у него адресов. Ответ может указывать время, подходящее для вызова пользователя;

- ответ **603 Decline** означает, что вызываемый пользователь не может или не желает принять входящий вызов. В ответе может быть указано подходящее для вызова время;
- ответ **604 Does Not Exist Anywhere** означает, что вызываемого пользователя не существует.

Напомним, что запросы и ответы на них образуют SIP-транзакцию. Она осуществляется между клиентом и сервером и включает в себя все сообщения, начиная с первого запроса и заканчивая финальным ответом. При использовании в качестве транспорта протокола TCP все запросы и ответы, относящиеся к одной транзакции, передаются по одному TCP-соединению.

На рисунке 7.8 представлен пример ответа на запрос **INVITE**.

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP kton.bell-tel.com
From: A. Bell <sip:a.g.bell@bell-tel.com>
To: <sip:watson@bell-tel.com>;
Call-ID: 3298420296@kton.bell-tel.com
Cseq: 1 INVITE
Content-Type: application/sdp
Content-Length: ...

v=0
o=watson 4858949 4858949 IN IP4 192.1.2.3
t=3149329600 0
c=IN IP4 boston.bell-tel.com
m=audio 5004 RTP/AVP 0 3
a=rtpmap:0 PCMU/8000
a=rtpmap:3 GSM/8000
```

Рис. 7.8 Пример SIP-ответа 200 OK

В этом примере приведен ответ пользователя Watson на приглашение принять участие в сеансе связи, полученное от пользователя Bell. Наиболее вероятный формат приглашения рассмотрен нами ранее (рис. 7.7). Вызываемая сторона информирует вызывающую о том, что она может принимать в порту 5004 речевую информацию, закодированную в соответствии с алгоритмами кодирования PCMU, GSM. Поля **From, To, Via, Call-ID** взяты из запроса, показанного на рисунке 7.7. Из примера видно, что это ответ на запрос **INVITE** с полем **CSeq:** 1.

После того, как мы рассмотрели запросы и ответы на них, можно отметить, что протокол SIP предусматривает разные алгоритмы установления соединения. При этом стоит обратить внимание, что одни и те же ответы можно интерпретировать по-разному в зависимости от конкретной ситуации. В таблицу 7.5 сведены все ответы на запросы, определенные протоколом SIP.

Таблица 7.5 Ответы SIP

Код ответа	Пояснение	Назначение
100	Trying	Запрос обрабатывается, например, сервер обращается к базам данных, но местоположение вызываемого пользователя в настоящий момент не определено
180	Ringing	Местоположение вызываемого пользователя определено. Ему дается сигнал о входящем вызове
181	Call Is Being Forwarded	Прокси-сервер переадресует вызов к другому пользователю
182	Queued	Вызываемый пользователь временно не доступен, но входящий вызов поставлен в очередь. Когда вызываемый пользователь станет доступным, он передаст финальный ответ
200	OK	Команда успешно выполнена
300	Multiple Choices	Вызываемый пользователь доступен по нескольким адресам. Вызывающий пользователь может выбрать любой из них
301	Moved Permanently	Пользователь изменил свое местоположение, его новый адрес указан в поле Contact
302	Moved Temporarily	Пользователь временно изменил свое местоположение, его новый адрес указан в поле Contact
305	Use Proxy	Вызываемая сторона может принять входящий вызов только в том случае, когда он проходит через прокси-сервер. Вызывающей стороне рекомендуется обратиться к прокси-серверу, адрес которого указан в поле Contact. Ответ передается только терминальным оборудованием (UAS)
380	Alternative Service	Вызов не достиг адресата, но существует альтернативный вариант обслуживания, который указан в теле ответа. Например, вызов может быть переадресован к речевому почтовому ящику
400	Bad Request	В запросе обнаружена синтаксическая ошибка
401	Unauthorised	Требуется проведение процедуры авторизации пользователя
402	Payment Required	Требуется предварительная оплата услуг
403	Forbidden	Запрос не будет обслуживаться сервером и не должен передаваться повторно
404	Not Found	Сервер не обнаружил вызываемого пользователя в домене, указанном в поле Request-URI
405	Method Not Allowed	Не разрешается передавать запрос этого типа на адрес, указанный в поле Request-URI. В поле Allow ответа указываются разрешенные типы запросов
406	Not Acceptable	Ответы, генерируемые вызываемой стороной, не будут поняты вызывающей стороной
407	Proxy Authentication Required	Клиент должен подтвердить свое право доступа к прокси-серверу
408	Request Timeout	Сервер не может передать ответ, например, указать местоположение вызываемого пользователя, в течение промежутка времени, специфицированного в поле Expires запроса. Вызывающий пользователь может повторно передать запрос через некоторое время
409	Conflict	Обработка запроса REGISTER не может быть завершена из-за конфликта между действием, определенным в параметре action запроса, и текущим состоянием ресурсов
410	Gone	Сервер больше не имеет доступа к запрашиваемому ресурсу и не знает, куда переадресовать запрос
411	Length Required	Требуется указать длину тела сообщения в поле Content-Length

413	Request Entity Too Large	Размер запроса слишком велик для обработки
414	Request-URI Too Large	Адрес, указанный в поле Request-URI, оказался слишком большим, поэтому его интерпретация невозможна
415	Unsupported Media Type	Запрос содержит не поддерживаемый формат тела сообщения
420	Bad Extension	Сервер не понял расширение протокола, специфицированное в поле Require
480	Temporarily not available	Вызываемый пользователь временно недоступен
481	Call Leg/Transaction Does Not Exist	Посылается в ответ на получение запроса BYE, не относящегося к текущим соединениям, или запроса CANCEL, не относящегося к текущим запросам
482	Loop Detected	Сервер обнаружил, что принятый им запрос передается по замкнутому маршруту (в поле Via уже имеется адрес этого сервера)
483	Too Many Hops	Сервер обнаружил в поле Via, что принятый им запрос прошел через большее количество прокси-серверов, чем разрешено в поле Max-Forwards
484	Address Incomplete	Сервер принял запрос с неполным адресом в поле To или Request-URI. Требуется дополнительная адресная информация
485	Ambiguous	Адрес вызываемого пользователя неоднозначен. В заголовке Contact ответа может содержаться список адресов, по которым этот запрос можно передать
486	Busy Here	В настоящий момент вызываемый пользователь не желает или не может принять вызов на этот адрес. Ответ не исключает возможности связаться с пользователем по другому адресу
500	Internal Server Error	Внутренняя ошибка сервера
501	Not Implemented	В сервере не реализованы функции, необходимые для обслуживания запроса. Ответ передается в том случае, когда сервер не может распознать тип полученного им запроса
502	Bad Gateway	Сервер, функционирующий в качестве шлюза или прокси-сервера, принимает некорректный ответ от сервера, к которому он направил запрос
503	Service Unavailable	Сервер не может в данный момент обслужить вызов вследствие перегрузки или проведения технического обслуживания
504	Gateway Time-out	Сервер, функционирующий в качестве шлюза или прокси-сервера, в течение установленного интервала времени не получил ответ от сервера (например, от сервера определения местоположения), к которому он обратился для завершения обработки запроса
505	SIP Version not supported	Сервер не поддерживает данную версию протокола SIP
600	Busy Everywhere	Вызываемый пользователь занят и не желает принимать вызов в данный момент. Ответ может указывать подходящее для вызова время
603	Decline	Вызываемый пользователь не может или не желает принимать входящие вызовы. В ответе может быть указано подходящее для вызова время
604	Does not exist anywhere	Вызываемого пользователя не существует
606	Not Acceptable	Вызываемый пользователь не может принять входящий вызов из-за того, что вид информации, указанный в описании сеанса связи в формате SDP, полоса пропускания и т.д. неприемлемы

7.6 Алгоритмы установления соединения

Протоколом SIP предусмотрены 3 основных сценария установления соединения: с участием прокси-сервера, с участием сервера переадресации и непосредственно между пользователями. Различие между перечисленными сценариями заключается в том, что по-разному осуществляется поиск и приглашение 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 переадресации лишь реализует преобразование постоянного адреса 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 простейшими. Ведь прежде чем вызов достигнет адресата, он может пройти через несколько прокси-серверов, или сначала направляется к серверу переадресации, а затем проходит через один или несколько прокси-серверов. Кроме того, прокси-серверы могут размножать запросы и передавать их по разным направлениям и т.д. Но, все же, как уже было уже отмечено в начале параграфа, эти три сценария являются основными. Здесь мы рассмотрим подробно два первых сценария; третий сценарий в данной главе рассматриваться не будет.

7.6.1 Установление соединения с участием сервера переадресации

В этом параграфе описан алгоритм установления соединения с участием сервера переадресации вызовов. Администратор сети сообщает пользователям адрес сервера переадресации. Вызывающий пользователь передает запрос **INVITE** (1) на известный ему адрес сервера переадресации и порт 5060, используемый по умолчанию (Рисунок 7.9). В запросе вызывающий пользователь указывает адрес вызываемого пользователя. Сервер переадресации запрашивает текущий адрес нужного пользователя у сервера определения местоположения (2), который сообщает ему этот адрес (3). Сервер переадресации в ответе **302 Moved temporarily** передает вызывающей стороне текущий адрес вызываемого пользователя (4), или он может сообщить список зарегистрированных адресов вызываемого пользователя и предложить вызывающему пользователю самому выбрать один из них. Вызывающая сторона подтверждает прием ответа **302** посылкой сообщения **ACK** (5).

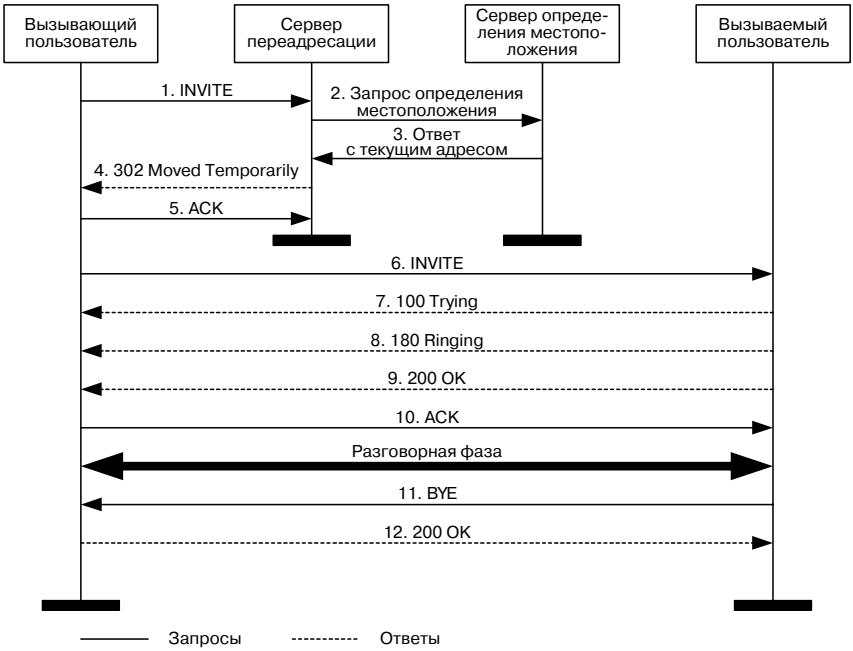

Рис. 7.9 Сценарий установления соединения через сервер переадресации

Теперь вызывающая сторона может связаться непосредственно с вызываемой стороной. Для этого она передает новый запрос **INVITE** (6) с тем же идентификатором **Call-ID**, но другим номером **CSeq**. В теле сообщения **INVITE** указываются данные о функциональных возможностях 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 перезапуска его таймеров. После завершения обработки поступившего запроса оборудование вызываемой стороны сообщает своему пользователю о входящем вызове, а встречной стороне передает ответ **180 Ringing** (8). После приема вызываемым пользователем входящего вызова удаленной стороне передается сообщение **200 OK** (9), в котором содержатся данные о функциональных возможностях 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 любой из сторон передается запрос **BYE** (11), который подтверждается ответом **200 OK** (12).

7.6.2. Установление соединения с участием прокси-сервера

В этом параграфе описан алгоритм установления соединения с участием прокси-сервера. Администратор сети сообщает адрес

этого сервера пользователям. Вызывающий пользователь передает запрос **INVITE** (1) на адрес прокси-сервера и порт 5060, используемый по умолчанию (Рисунок 7.10). В запросе пользователь указывает известный ему адрес вызываемого пользователя. Прокси-сервер запрашивает текущий адрес вызываемого пользователя у сервера определения местоположения (2), который и сообщает ему этот адрес (3). Далее прокси-сервер передает запрос **INVITE** непосредственно вызываемому оборудованию (4). Опять в запросе содержатся данные о функциональных возможностях вызывающего терминала, но при этом в запрос добавляется поле **Via** с адресом прокси-сервера для того, чтобы ответы на обратном пути шли через него. После приема и обработки запроса вызываемое оборудование сообщает своему пользователю о входящем вызове, а встречной стороне передает ответ **180 Ringing** (5), копируя в него из запроса поля **To, From, Call-ID, CSeq** и **Via**. После приема вызова пользователем встречной стороне передается сообщение **200 OK** (6), содержащее данные о функциональных возможностях вызываемого терминала в формате протокола SDP. Терминал вызывающего пользователя подтверждает прием ответа запросом **ACK** (7). На этом фаза установления соединения закончена и начинается разговорная фаза.

По завершении разговорной фазы одной из сторон передается запрос **BYE** (8), который подтверждается ответом **200 OK** (9).

Все сообщения проходят через прокси-сервер, который может модифицировать в них некоторые поля.

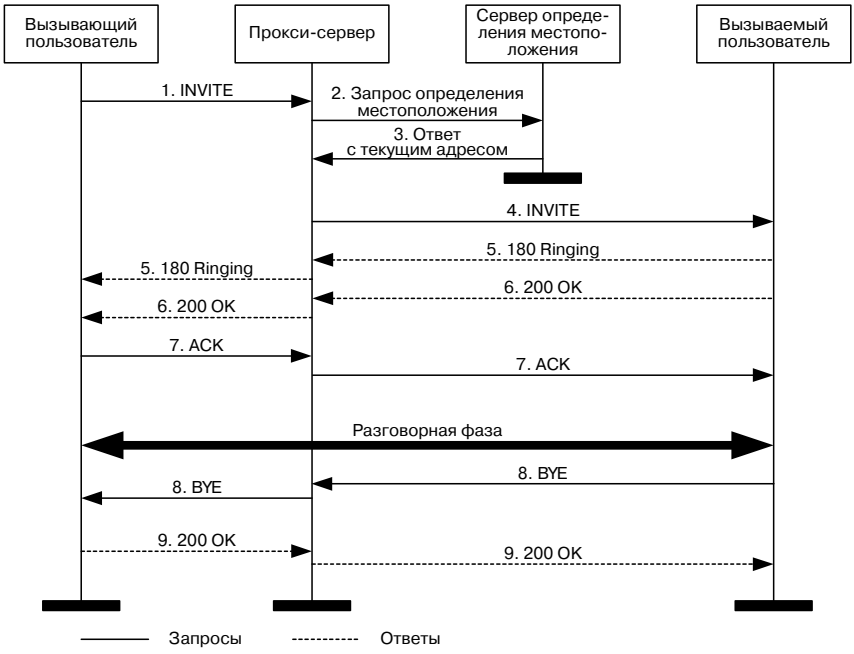

Рис. 7.10 Сценарий установления соединения через прокси-сервер

7.7 Реализация дополнительных услуг на базе протокола SIP

В этом параграфе рассматриваются примеры реализация дополнительных услуг на базе протокола SIP.

Дополнительная услуга «Переключение связи» позволяет пользователю переключить установленное соединение к третьей стороне. На рисунке 7.11 приведен пример реализации этой услуги. Пользователь B устанавливает связь с пользователем A, который, переговорив с B, переключает эту связь к пользователю C, а сам отключается.

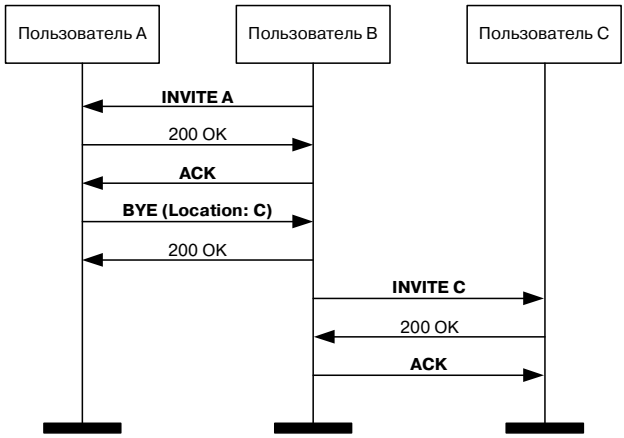

Рис. 7.11 Дополнительная услуга "Переключение связи"

Дополнительная услуга «Переадресация вызова» позволяет пользователю назначить адрес, на который, при определенных условиях, следует направлять входящие к нему вызовы. Такими условиями могут быть занятость пользователя, отсутствие его ответа в течение заданного времени или и то, и другое; возможна также безусловная переадресация. Оборудование пользователя, заказавшего эту услугу, получив сообщение **INVITE B**, проверяет условия, в которых оно получено, и если условия требуют переадресации, передает сообщение **INVITE** с заголовком **Also**, указывая в нем адрес пользователя, к которому следует направить вызов. Терминал вызывающего пользователя, получив сообщение **INVITE** с таким заголовком, инициирует новый вызов по адресу, указанному в поле **Also.** В нашем случае пользователь A вызывает пользователя B, а терминал последнего переадресует вызов к пользователю C (Рисунок 7.12).

Дополнительная услуга «Уведомление о вызове во время связи» позволяет пользователю, участвующему в телефонном разговоре, получить уведомление о том, что к нему поступил входящий вызов (Рисунок 7.13).

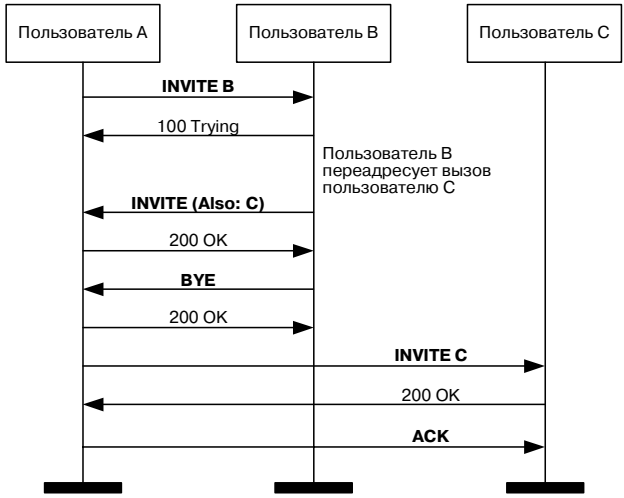

Рис. 7.12 Дополнительная услуга "Переадресация вызова"

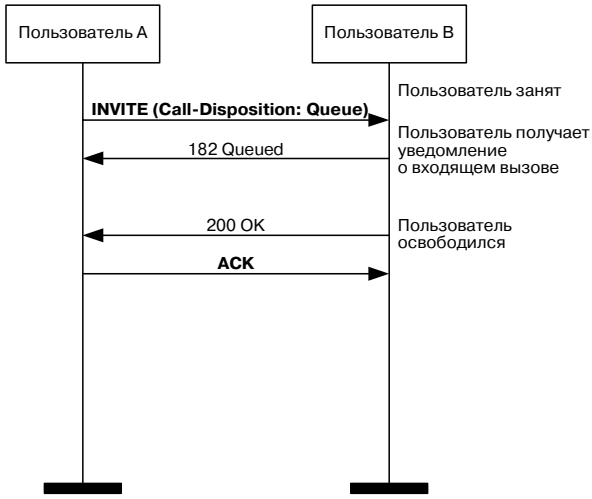

Рис. 7.13 Дополнительная услуга "Уведомление о вызове во время связи"

Услуга реализуется с помощью заголовка **Call-Disposition**, в котором содержится инструкция по обслуживанию вызова. 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. Вызываемая сторона подтверждает исполнение запроса 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 финальный ответ **200 OK**.

7.8 Сравнительный анализ протоколов H.323 и SIP

Прежде чем начать сравнение функциональных возможностей протоколов SIP и H.323, напомним, что протокол SIP значительно моложе своего соперника, и опыт его использования в сетях связи несопоставим с опытом использования протокола H.323. Существует еще один момент, на который следует обратить внимание. Интенсивное внедрение технологии передачи речевой информации по IP-сетям потребовало постоянного наращивания функциональных возможностей как протокола H.323 (к настоящему времени утверждена уже третья версия протокола), так и протокола SIP (утверждена вторая версия протокола). Этот процесс приводит к тому, что достоинства одного из протоколов перенимаются другим.

И последнее. Оба протокола являются результатом решения одних и тех же задач специалистами ITU-T и комитета IETF. Естественно, что решение ITU-T оказалось ближе к традиционным телефонным сетям, а решение комитета IETF базируется на принципах, составляющих основу сети Internet.

Перейдем непосредственно к сравнению протоколов, которое будем проводить по нескольким критериям.

Дополнительные услуги. Набор услуг, поддерживаемых обоими протоколами, примерно одинаков.

Дополнительные услуги, предоставляемые протоколом H.323, стандартизированы в серии рекомендаций ITU-T H.450.x. Протоколом SIP правила предоставления дополнительных услуг не определены, что является его серьезным недостатком, так как вызывает проблемы при организации взаимодействия оборудования разных фирм-производителей. Некоторые специалисты предлагают решения названных проблем, но эти решения пока не стандартизированы.

Примеры услуг, предоставляемых обоими протоколами:

- Перевод соединения в режим удержания (Call hold);
- Переключение связи (Call Transfer);
- Переадресация (Call Forwarding);
- Уведомление о новом вызове во время связи (Call Waiting);
- Конференция.

Рассмотрим последнюю услугу несколько более подробно. Протокол SIP предусматривает три способа организации конференции: с использованием устройства управления конференциями MCU, режима многоадресной рассылки и соединений участников друг с другом. В последних двух случаях функции управления конференциями могут быть распределены между терминалами, т.е. центральный контроллер конференций не нужен. Это позволяет организовывать конференции с практически неограниченным количеством участников.

Рекомендация H.323 предусматривает те же три способа, но управление конференцией во всех случаях производится централизованно контроллером конференций MC (Multipoint Controller), который обрабатывает все сигнальные сообщения. Поэтому для организации конференции, во-первых, необходимо наличие контроллера MC у одного из терминалов, во-вторых, участник с активным контроллером MC не может выйти из конференции. Кроме того, при большом числе участников конференции MC может стать «узким местом». Правда, в третьей версии рекомендации ITU-T H.323 принято положение о каскадном соединении контроллеров, однако производители эту версию в своем оборудовании пока не реализовали. Преимуществом протокола H.323 в части организации конференций являются более мощные средства контроля конференций.

Протокол SIP изначально ориентирован на использование в IP-сетях с поддержкой режима многоадресной рассылки информации (примером может служить сеть Mbone, имеющая тысячи постоянных пользователей). Этот механизм используется в протоколе SIP не только для доставки речевой информации (как в протоколе H.323), но и для переноса сигнальных сообщений. Например, в режиме многоадресной рассылки может передаваться сообщение **INVITE**, что облегчает определение местоположения пользователя и является очень удобным для центров обслуживания вызовов (Call-center) при организации групповых оповещений.

В то же время, протокол H.323 предоставляет больше возможностей управления услугами, как в части аутентификации и учета, так и в части контроля использования сетевых ресурсов. Возможности протокола SIP в этой части беднее, и выбор оператором этого протокола может служить признаком того, что для оператора важнее техническая интеграция услуг, чем возможности управления услугами.

Протокол SIP предусматривает возможность организации связи третьей стороной (third-party call control). Эта функция позволяет реализовать такие услуги, как набор номера секретарем для менеджера и сопровождение вызова оператором центра обслуживания вызовов. Подобные услуги предусмотрены и протоколом H.323, но реализация их несколько сложнее.

В протоколе SIP есть возможность указывать приоритеты в обслуживании вызовов, поскольку во многих странах существуют требования предоставлять преимущества некоторым пользователям. В протоколе H.323 такой возможности нет. Кроме того, пользователь SIP-сети может регистрировать несколько своих адресов и указывать приоритетность каждого из них.

Персональная мобильность пользователей. Протокол SIP имеет хороший набор средств поддержки персональной мобильности пользователей, в число которых входит переадресация вызова к новому местоположению пользователя, одновременный поиск по не-

скольким направлениям (с обнаружением зацикливания маршрутов) и т.д. В протоколе SIP это организуется путем регистрации на сервере определения местоположения, взаимодействие с которым может поддерживаться любым протоколом. Персональная мобильность поддерживается и протоколом H.323, но менее гибко. Так, например, одновременный поиск пользователя по нескольким направлениям ограничен тем, что привратник, получив запрос определения местоположения пользователя LRQ, не транслирует его к другим привратникам.

Расширяемость протокола. Необходимой и важной в условиях эволюционирующего рынка является возможность введения новых версий протоколов и обеспечение совместимости различных версий одного протокола. Расширяемость (extensibility) протокола обеспечивается:

– согласованием параметров;
– стандартизацией кодеков;
– модульностью архитектуры.

Протокол SIP достаточно просто обеспечивает совместимость разных версий. Поля, которые не понятны оборудованию, просто игнорируются. Это уменьшает сложность протокола, а также облегчает обработку сообщений и внедрение новых услуг. Клиент может запросить какую-либо услугу с помощью заголовка **Require**. Сервер, получивший запрос с таким заголовком, проверяет, поддерживает ли он эту услугу, и если не поддерживает, то сообщает об этом в своем ответе, содержащем список поддерживаемых услуг.

В случае необходимости, в организации IANA (Internet Assigned Numbers Authority) могут быть зарегистрированы новые заголовки. Для регистрации в IANA отправляется запрос с именем заголовка и его назначением. Название заголовка выбирается таким образом, чтобы оно говорило об его назначении. Указанным образом разработчик может внедрять новые услуги.

Для обеспечения совместимости версий протокола SIP определено шесть основных видов запросов и 6 классов ответов на запросы. Так как определяющей в кодах ответов является первая цифра, то оборудование может указывать и интерпретировать только ее, а остальные цифры кода только дополняют смысл и их анализ не является обязательным.

Более поздние версии протокола H.323 должны поддерживать более ранние версии. Но возможна ситуация, когда производители поддерживают только одну версию, чтобы уменьшить размер сообщений и облегчить их декодирование.

Новые функциональные возможности вводятся в протокол H.323 с помощью поля **NonStandardParameter**. Оно содержит код произ-

водителя и, следом за ним, код услуги, который действителен только для этого производителя. Это позволяет производителю расширять услуги, но сопряжено с некоторыми ограничениями. Во-первых, невозможно запросить у вызываемой стороны информацию о поддерживаемых ею услугах, во-вторых, невозможно добавить новое значение уже существующего параметра. Существуют также проблемы, связанные с обеспечением взаимодействия оборудования разных производителей.

На расширение возможностей протокола, как и на совместимость оборудования, его реализующего, оказывает влияние и набор кодеков, поддерживаемый протоколом. В протоколе SIP для передачи информации о функциональных возможностях терминала используется протокол SDP. Если производитель поддерживает какой-то особенный алгоритм кодирования, то этот алгоритм просто регистрируется в организации IANA, неоднократно упоминавшейся в этой главе.

В протоколе H.323 все кодеки должны быть стандартизированы. Поэтому приложения с нестандартными алгоритмами кодирования могут столкнуться с проблемами при реализации их на базе протокола H.323.

Протокол SIP состоит из набора законченных компонентов (модулей), которые могут заменяться в зависимости от требований и могут работать независимо друг от друга. Этот набор включает в себя модули поддержки сигнализации для базового соединения, для регистрации и для определения местоположения пользователя, которые не зависят от модулей поддержки качества обслуживания (QoS), работы с директориями, описания сеансов связи, развертывания услуг (service discovery) и управления конфигурацией.

Архитектура протокола H.323 монолитна и представляет собой интегрированный набор протоколов для одного применения. Протокол состоит из трех основных составляющих, и для создания новой услуги может потребоваться модификация каждой из этих составляющих.

Масштабируемость сети (scalability). Сервер SIP, по умолчанию, не хранит сведений о текущих сеансах связи и поэтому может обработать больше вызовов, чем привратник H.323, который хранит эти сведения (statefull). Вместе с тем, отсутствие таких сведений, по мнению некоторых специалистов, может вызвать трудности при организации взаимодействия сети IP-телефонии с ТФОП.

Необходимо также иметь в виду зоновую архитектуру сети H.323, позволяющую обеспечить расширяемость сети путем увеличения количества зон.

Время установления соединения. Следующей существенной характеристикой протоколов является время, которое требуется, чтобы установить соединение. В запросе **INVITE** протокола SIP содержится вся необходимая для установления соединения информация, включая описание функциональных возможностей терминала. Таким образом, в протоколе SIP для установления соединения требуется одна транзакция, а в протоколе H.323 необходимо производить обмен сообщениями несколько раз. По этим причинам затраты времени на установление соединения в протоколе SIP значительно меньше затрат времени в протоколе H.323. Правда, при использовании инкапсуляции сообщений H.245 в сообщения H.225 или процедуры Fast Connect время установления соединения значительно уменьшается.

Кроме того, на время установления соединения влияет также и нижележащий транспортный протокол, переносящий сигнальную информацию. Ранние версии протокола H.323 предусматривали использование для переноса сигнальных сообщений H.225 и H.245 только протокол TCP, и лишь третья версия протокола предусматривает возможность использования протокола UDP. Протоколом SIP использование протоколов TCP и UDP предусматривалось с самого начала.

Оценка времени установления соединения производится в условных единицах – RTT (round trip time) – и составляет для протокола SIP 1,5 ÷ 2,5 RTT, а для протокола H.323 6 – 7 RTT.

Адресация. К числу системных характеристик, несомненно, относится и предусматриваемая протоколами адресация. Использование URL является сильной стороной протокола SIP и позволяет легко интегрировать его в существующую систему DNS-серверов и внедрять в оборудование, работающее в IP-сетях. Пользователь получает возможность переправлять вызовы на Web-страницы или использовать электронную почту. Адресом в SIP может также служить телефонный номер с адресом используемого шлюза.

В протоколе H.323 используются транспортные адреса и alias-адреса. В качестве последнего может использоваться телефонный номер, имя пользователя или адрес электронной почты. Для преобразования alias-адреса в транспортный адрес обязательно участие привратника.

Сложность протокола. Протокол H.323, несомненно, сложнее протокола SIP. Общий объем спецификаций протокола H.323 составляет примерно 700 страниц. Объем спецификаций протокола SIP составляет 150 страниц. Протокол H.323 использует большое количество информационных полей в сообщениях (до 100), при нескольких десятках таких же полей в протоколе SIP. При этом для организации базового соединения в протоколе SIP достаточно использовать всего три типа запросов (**INVITE**, **BYE** и **ACK**) и несколько полей (**To**, **From**, **Call-ID**, **CSeq**).

Протокол SIP использует текстовый формат сообщений, подобно протоколу HTTP. Это облегчает синтаксический анализ и генерацию кода, позволяет реализовать протокол на базе любого языка программирования, облегчает эксплуатационное управление, дает возможность ручного ввода некоторых полей, облегчает анализ сообщений. Название заголовков SIP–сообщений ясно указывает их назначение.

Протокол H.323 использует двоичное представление своих сообщений на базе языка ASN.1, поэтому их непосредственное чтение затруднительно. Для кодирования и декодирования сообщений необходимо использовать компилятор ASN.1. Но, в то же время, обработка сообщений, представленных в двоичном виде, производится быстрее.

Довольно сложным представляется взаимодействие протокола H.323 с межсетевым экраном (firewall). Кроме того, в протоколе H.323 существует дублирование функций. Так, например, оба протокола H.245 и RTCP имеют средства управления конференцией и осуществления обратной связи.

Выводы. На основе проведенного выше сравнения можно сделать вывод о том, что протокол SIP больше подходит для использования Internet-поставщиками, поскольку они рассматривают услуги IP-телефонии лишь как часть набора своих услуг.

Операторы телефонной связи, для которых услуги Internet не являются первостепенными, скорее всего, будут ориентироваться на протокол H.323, поскольку сеть, построенная на базе рекомендации H.323, представляется им хорошо знакомой сетью ISDN, наложенной на IP-сеть.

Не стоит также забывать, что к настоящему времени многие фирмы-производители и поставщики услуг уже вложили значительные средства в оборудование H.323, которое успешно функционирует в сетях.

Таким образом, ответ на вопрос, какой из протоколов предпочтительнее использовать, будет зависеть от целей бизнеса и требуемых функциональных возможностей. Скорее всего, эти варианты не следует рассматривать как конкурирующие, а как предназначенные для разных областей рынка услуг, поскольку они могут работать параллельно и взаимодействовать через специальный шлюз. Проиллюстрируем это утверждение следующим примером. В настоящее время рынок услуг все больше нацеливается на услуги с доплатой за дополнительные возможности (value added), и простота их предоставления дает реальные преимущества. Так, использование SIP в какомлибо частном домене дает возможность более гибкого предоставления услуг, а наличие средств, обеспечивающих переход от прото-

кола SIP к протоколу H.323, гарантирует взаимодействие с областями, использующими другие решения. В таблице 7.6 приведен вариант возможного обмена сообщениями.

Таблица 7.6 Алгоритм установления соединения с участием шлюза H.323/SIP

Шаг	H.323-сторона шлюза	SIP-сторона шлюза	Комментарии
1	→ Setup (с процедурой FastStart)		Содержит описание возможностей приема информации
2	← Call proceeding		Подтверждение прокси-сервером приема сообщения SETUP
3		INVITE →	Содержит описание возможностей приема информации в формате SDP
4		180 Ringing ←	Уведомление вызывающего пользователя о том, что вызываемому пользователю передается сигнал о входящем вызове
5	← Alerting		
6		200 OK ←	Вызываемый пользователь принял входящий вызов, сообщение содержит описание возможностей приема информации
7	← Connect		
8		ACK →	
•			
•	Телефонный разговор		
•			
N		BYE ←	Разговор завершен
N+1	← Release complete		
N+2		200 OK →	

Если в течение разговорной фазы оборудованию H.323 необходимо открыть новые логические каналы, шлюз передает новое сообщение **INVITE** терминалу SIP, как это показано в таблице 7.7.

Таблица 7.7 Открытие новых логических каналов

Шаг	H.323-сторона шлюза	SIP-сторона шлюза	Комментарии
	→ OpenLogicalChannel		
		INVITE →	Тот же идентификатор соединения, что и в предыдущем сообщении INVITE (но номер Cseq -увеличен) Описание нового канала в формате SDP
		200 OK ←	Содержит описание нового канала в формате SDP
	← OpenLogicalChannelAck		