

Министерство образования и науки Российской Федерации
Федеральное государственное автономное образовательное
учреждение высшего образования
«Южно-Уральский государственный университет
(национальный исследовательский университет)»
Высшая школа электроники и компьютерных наук
Кафедра «Инфокоммуникационные технологии»

ДОПУСТИТЬ К ЗАЩИТЕ
Заведующий кафедрой ИКТ
С.Н. Даровских _____
«__» _____ 2019 г.

«Сравнительный анализ протоколов функционирования IP-телефонии»

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
К ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ
ЮУрГУ-Д.11.03.02.2019.240.00 ПЗ ВКР

Руководитель работы:
доцент кафедры ИКТ
В.В. Новиков _____
«__» _____ 2019 г.

Автор работы:
студент группы КЭ-459
В.С. Стуков _____
«__» _____ 2019 г.

Нормконтролер:
В.Д. Спицына _____
«__» _____ 2019 г.

Челябинск
2019

РЕФЕРАТ

Стуков В.С. Сравнительный анализ протоколов функционирования IP-телефонии. – Челябинск: ЮУрГУ, ВШ ЭКН; 2019, 41 с., 1 табл., 9 ил., библиогр. список – 20 наим.

В данной выпускной квалификационной работе были рассмотрены два основных протокола функционирования IP-телефонии SIP и H.323. Были рассмотрены характеристики, области применения и достоинства каждого.

Цель работы заключается в анализе этих протоколов на основе рассмотренных критериев и выявление лучшего из них в настоящее время.

					11.03.02.2019.240.00 ПЗ			
<i>Изм.</i>	<i>Лист</i>	<i>№ докум.</i>	<i>Подпись</i>	<i>Дата</i>				
Разраб.	Стуков				Сравнительный анализ протоколов функционирования IP- телефонии	<i>Лит.</i>	<i>Лист</i>	<i>Листов</i>
Провер.	Новиков					Д	3	41
Реценз.						ЮУрГУ Кафедра ИКТ		
Н. Контр.	Спицына							
Утверд.								

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ.....	6
1 ТРЕБОВАНИЯ К СОДЕРЖАНИЮ	8
1.1 Технические характеристики протокола SIP	8
1.1.1 Типы запросов.....	9
1.1.2 Ответы на запросы.....	10
1.2 Технические характеристики протокола H.323	13
1.2.1 Протокол RAS	13
1.2.2 Протокол H.225.....	14
1.2.3 Протокол H.245.....	14
1.2.4 Сообщения RAS.....	15
1.3 Сценарии обмена сообщениями протокола SIP	17
1.3.1 Установление соединения с участием сервера переадресации.....	17
1.3.2 Установление соединения с участием прокси-сервера.....	19
1.3.3 Реализация дополнительных услуг на базе протокола SIP	20
1.4 Сценарий обмена сообщениями протокола H.323	22
1.4.1 Базовое соединение с участием привратника.....	23
1.4.2 Базовое соединение без участия привратника.....	27
1.4.3 Туннелирование управляющих сообщений.....	30
1.4.4 Процедура быстрого установления соединения.....	30
1.5 Достоинства и недостатки протокола SIP	33
1.6 Достоинства и недостатки протокола H.323	34
1.7 Области практического применения протокола SIP	35
1.8 Области практического применения протокола H.323	36
1.9 Сравнительный анализ протоколов H.323 и SIP	36
1.9.1 Дополнительные услуги	36
1.9.2 Персональная мобильность пользователей	38
1.9.3 Расширяемость протокола.....	38

1.9.4 Масштабируемость сети	39
1.9.5 Время установления соединения	39
1.9.6 Сложность протокола.....	40
ЗАКЛЮЧЕНИЕ	42
БИБЛИОГРАФИЧЕСКИЙ СПИСОК	43

ВВЕДЕНИЕ

IP-телефония — это телефонная связь по протоколу IP. Под этим понятием подразумевается набор протоколов функционирования, технологий, методов, обеспечивающих обычные для телефонии, дозвон, набор номера, голосовое общение двух абонентов, и видео общение по сети интернет и иным IP-сетям.

Протоколы обеспечивают регистрацию клиентского устройства (шлюз, терминал или IP-телефон) на сервере, или, как он еще называется, привратнике провайдера, вызов и переадресацию вызова, установление видео и голосового соединений, а так же передачу номера абонента и его имени.

В данной работе будут рассматриваться два основных протокола функционирования – SIP и H.323.

SIP (Session Initiation Protocol) – Протокол инициирования сеансов. Это протокол прикладного уровня, предназначенный для модификации, организации и завершения сеансов связи: телефонных соединений, мультимедийных конференций и распределения мультимедийной информации. Пользователям предоставляется возможность принимать участие в существующих сеансах связи, приглашать других пользователей и быть приглашенными ими к новому сеансу связи. Приглашения могут быть адресованы как одному пользователю, так и группе пользователей или всем пользователям.

Протокол SIP был разработан и специфицирован в комитете IETF (Internet Engineering Task Force) группой MMUSIC (Multiparty Multimedia Session Control) в 1999 году.

Протокол H.323 один из старейших стандартов, разработанный в 1996 году и представляет собой стек различных протоколов. В него входят три основных протокола: протокол взаимодействия оконечного оборудования с привратником – RAS, протокол управления соединениями – H.225 и протокол управления логическими каналами – H.245.

Три этих протокола, наряду с Интернет-протоколами TCP/IP (Transmission Control Protocol, протокол управления передачей), UDP (User Datagram Protocol, протокол пользовательских датаграмм), RTP (Real-time Transport Protocol, протокол передачи в реальном времени), RTCP (Real-Time Transport Control Protocol, протокол управления передачей в реальном времени) и Q.931 (сигнальный протокол) представлены на рисунке 1.

Гарантированная доставка информации по протоколу TCP		Негарантированная доставка информации по протоколу UDP		
H.245	H.225		Потоки речи и видеoinформации	
	Управление соединением (Q.931)	RAS	RTCP	RTP
TCP		UDP		
IP				
Канальный уровень				
Физический уровень				

Рисунок 1 – Стек протоколов H.323

На этом рисунке суть изображенной иерархии заключается в следующем. Чтобы перенести сигнальные сообщения H.225 и управляющие сообщения H.245 используется протокол TCP – это протокол установления соединения и гарантированной доставки информации. А сигнальные сообщения протокола RAS переносятся протоколом с негарантированной доставкой информации – UDP. Для переноса речевой и видеoinформации используется протокол передачи информации в реальном времени – RTP. Протоколом RTCP осуществляется контроль переноса пользовательской информации.

1 Требования к содержанию

В работе приводятся сведения о протоколах SIP и H.323. Рассмотрены их технические характеристики, достоинства, недостатки и области применения. Представлены сценарии обмена сообщениями. А так же проведен их сравнительный анализ.

1.1 Технические характеристики протокола SIP

Протокол инициирования сеансов – Session Initiation Protocol (SIP) является протоколом прикладного уровня и предназначается для организации, модификации и завершения сеансов связи.

Имеется архитектура «клиент-сервер», согласно которой, все сообщения делятся либо на запросы от клиента к серверу, либо на ответы сервера клиенту.

Например, чтобы установить соединение, вызывающему абоненту необходимо сообщить серверу некоторые параметры, в том числе адрес вызываемого абонента, параметры информационных каналов и др. Все эти параметры передаются SIP-запросе. От вызываемого абонента к вызывающему будет передан ответ на запрос, который также имеет ряд параметров.

Запросы и ответы протокола SIP, являются последовательностью текстовых строк, которые закодированы в соответствии с документом RFC 2279. На рисунке 2 представлена структура сообщений протокола SIP.

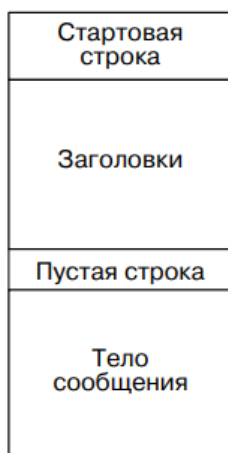


Рисунок 2 – Структура сообщений протокола SIP

Стартовая строка является начальной строкой любого SIP-сообщения. Если это запрос, то в этой строке будет указан тип запроса, адресат и версия протокола. Если это ответ на запрос, тогда в данной строке укажется версия протокола, тип ответа и его расшифровка, которая предназначена только для пользователя.

В заголовках содержатся данные об отправителе, адресате, пути следования и др., т.е. несут информацию, которая нужна чтобы обслужить данное сообщение. Тип заголовка узнается по его имени. Имя не зависит от регистра (буквы могут быть прописные и строчные), но как правило его пишут с большой буквы, за которой следуют строчные.

В протоколе SIP выделяется всего четыре вида заголовков:

- общие заголовки, содержащиеся в запросах и ответах;
- заголовки содержания, которые отвечают за перенос информации о размере тела сообщения и источнике запроса;
- заголовки запросов, которые передают дополнительную информацию о запросе;
- заголовки ответов, которые передают дополнительную информацию об ответе.

Так же протокол включает в себя так называемое тело сообщения. Оно содержится в некоторых запросах и включает в себя описание сеансов связи. В ответах немного иначе: тело сообщения содержится в любом ответе, но его содержание всегда будет разным.

1.1.1 Типы запросов

В последней версии протокола разделяется шесть типов запросов. Каждый из которых выполняет обширный круг задач, что несомненно является одним из достоинств протокола SIP. Благодаря этому, количество сообщений сводится к минимуму, которыми обмениваются серверы и терминалы. Запросы предоставляют клиенту ряд услуг, таких как приглашение абонентов принять

участие в сеансах связи, улучшать уже установленные сеансы, завершать их, сообщение о текущем местоположении и т.д. Тип принятого запроса определяется сервером по названию, которое указано в стартовой строке.

Типы запросов:

- INVITE – приглашение пользователя к сеансу связи. Содержит SDP, описание сеанса;
- ACK – подтверждение приема окончательного ответа на запрос INVITE;
- BYE – завершение сеанса связи;
- CANCEL – отмена обработки запросов;
- REGISTER – перенос адресной информации, чтобы зарегистрировать пользователя на сервере определения местоположения;
- OPTION – запрос информации о функционале данного терминала.

1.1.2 Ответы на запросы

После того как запрос принят, прокси-сервер (адресат) передает ответ на данный запрос. Содержание ответов всегда разное, будь то подтверждение установления соединения, передача запрошенной информации или сведения о неисправностях и т.д. Данную структуру ответов и их типы протокол SIP перенял от протокола HTTP (HyperText Transfer Protocol, протокол передачи гипертекста).

Типы ответов на запросы:

- Trying – запрос в обработке;
- Ringing – местоположение вызываемого абонента определено, ему подается сигнал о входящем вызове;
- Call Is Being Forwarded – переадресация к другому пользователю;
- Queued – вызываемый абонент временно не доступен, но входящий вызов будет поставлен в очередь;
- OK – команда успешно выполнена;

- Multiple Choices – вызываемый абонент доступен на нескольких адресах;
- Moved Permanently – абонент изменил свое местоположение, его новый адрес будет указан в поле Contact;
- Moved Temporarily – абонент временно изменил свое местоположение, его новый адрес указан в поле Contact;
- Use Proxy – вызываемый абонент может принять входящий вызов только тогда, когда он проходит через прокси-сервер;
- Alternative Service – вызов не достиг вызываемого абонента, но есть альтернативный вариант, к примеру голосовая почта;
- Bad Request – в запросе обнаружена синтаксическая ошибка;
- Unauthorised – от пользователя требуется авторизация;
- Payment Required – от пользователя требуется предварительная оплата услуг;
- Forbidden – сервер не будет обслуживать запрос;
- Not Found – сервер не обнаружил вызываемого пользователя в домене;
- Method Not Allowed – не разрешается передавать запрос этого типа на адрес;
- Not Acceptable – ответы от вызываемого абонента, не будут поняты вызывающим абонентом;
- Proxy Authentication Required – от клиента требуется подтверждение права доступа;
- Request Timeout – сервер не может передать ответ;
- Conflict – обработка запроса REGISTER не может быть завершена из-за конфликта между действием, определенным в параметре action запроса, и текущим состоянием ресурсов;
- Gone – сервер больше не имеет доступа к запрашиваемому ресурсу;

- Length Required – требуется указать длину тела сообщения в поле Content-Length;
- Request Entity Too Large – размер запроса слишком велик для обработки;
- Request-URI Too Large – указанный адрес оказался слишком большим;
- Unsupported Media Type – запрос содержит не поддерживаемый формат тела сообщения;
- Bad Extension – сервер не опознал расширение протокола;
- Temporarily not available – вызываемый абонент временно недоступен;
- 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;
- Loop Detected – сервер обнаружил, что принятый им запрос передается по замкнутому маршруту;
- Too Many Hops – сервер обнаружил, что принятый им запрос прошел через большее количество прокси-серверов, чем это разрешено;
- Address Incomplete – сервер принял запрос с неполным адресом и требуется дополнительная адресная информация;
- Ambiguous – адрес вызываемого пользователя неоднозначен;
- Busy Here – в настоящее время вызываемый абонент не желает или не может принять вызов по этому адресу;
- Internal Server Error – внутренняя ошибка сервера;
- Not Implemented – нет функций, необходимых для обслуживания запроса;
- Bad Gateway – сервер, функционирующий в качестве шлюза, принимает некорректный ответ от сервера, к которому он направил запрос;

- Service Unavailable – обслуживание сервера в данный момент недоступно;
- Gateway Time-out – сервер, функционирующий в качестве шлюза, в течение времени не получил ответ от сервера, к которому он обратился для завершения обработки запроса;
- SIP Version not supported – данная версия протокола SIP не поддерживается сервером;
- Busy Everywhere – вызываемый абонент не желает принимать вызов в настоящее время;
- Decline – вызываемый абонент не может или не желает принимать входящие вызовы;
- Does not exist anywhere – вызываемый абонент не существует;
- Not Acceptable – вызываемый абонент не может принять входящий вызов потому, что информация, указанная в описании сеанса связи неприемлема.

1.2 Технические характеристики протокола H.323

В семейство протокола H.323 входят три основных протокола: RAS, H.245 и H.225, которые будут описаны ниже.

1.2.1 Протокол RAS

Благодаря протоколу RAS (Registration Admission Status) обеспечивается взаимодействие оконечных и других устройств с привратником.

К основным функциям протокола относятся:

- регистрация устройств в сети H.323;
- контролирование доступа к ресурсам в сети;
- возможность изменять полосы пропускания во время связи;

- запрашивание и фиксация состояния устройств на данный момент времени.

UDP в данном случае используется как транспортный протокол.

1.2.2 Протокол H.225

Благодаря протоколу H.225 (Q.931) происходит установление, поддержание и завершение речевого соединения.

TCP выступает в качестве транспортного протокола.

К сообщениям Q.931 относятся:

- SETUP – установить;
- CALL PROCEEDING – обработка вызова;
- ALERTING – готовность;
- CONNECT – соединить;
- DISCONNECT – разъединить;
- RELEASE – освободить;
- RELEASE COMPLETE – освобождение закончено.

1.2.3 Протокол H.245

Благодаря протоколу H.245 происходит обмен информацией между участниками соединения, которая необходима для создания логических каналов. Именно по этим каналам совершается передача речевой информации, которая упакована в пакеты RTP/UDP/IP. В таблице 1 представлены управляющие сообщения протокола H.245.

Таблица 1 – Управляющие сообщения протокола H.245

Процедуры	Сообщения
Определение ведущего и ведомого	masterSlaveDetermination masterSlaveDeterminationAck (ведомое) masterSlaveDeterminationAck (ведущее)
Обмен данными о функциональных возможностях	TerminalCapabilitySet TerminalCapabiltySetAck TerminalCapabilitySetReject TerminalCapabilitySetRelease
Открытие и закрытие логических каналов	TerminalCapabilitySet TerminalCapabiltySetAck TerminalCapabilitySetReject TerminalCapabilitySetRelease
Выбор режима обработки информации	RequestMode FunctlonNotSupported RequestModeAck

Начальная фаза в установлении соединения с использованием сигнализации H.323 заключается в выполнении процедур, которые предусмотрены протоколом RAS. После чего следуют фаза сигнализации H.225.0 (Q.931). Далее происходит обмен управляющими сообщениями H.245. К слову, завершение соединения происходит в обратной последовательности.

1.2.4 Сообщения RAS

К сообщениям протокола RAS относятся:

- GRQ – Gatekeeper Request (Запрос привратника);
- GCF – Gatekeeper Confirm (Подтверждение привратника);

- GRJ – Gatekeeper Reject (Отказ привратника);
- RRQ – Registration Request (Запрос регистрации);
- RCF – Registration Confirm (Подтверждение регистрации);
- RRJ – Registration Reject (Отказ в регистрации);
- URQ – Unregistratton Request (Запрос отмены регистрации);
- UCF – Unregistration Confirm (Регистрация отменена);
- URJ – Unregistration Reject (Отказ в отмене регистрации);
- ARQ – Admission Request (Запрос доступа);
- ACF – Admission Confirm (Подтверждение доступа);
- ARJ – Admission Reject (Отказ в доступе);
- BRQ – Bandwidth Request (Запрос изменения полосы пропускания);
- BCF – Bandwidth Confirm (Подтверждение изменения полосы пропускания);
- BRJ – Bandwidth Reject (Отказ в предоставлении полосы);
- IRQ – Information Request (Запрос информации);
- IRR – Information Response (Ответ на запрос информации);
- DRQ – Disengage Request (Запрос разъединения);
- DCF – Disengage Confirm (Подтверждение получения сообщения DRQ);
- DRJ – Disengage Reject (Отклонение DRQ);
- LRQ – Location Request (Запрос местоположения);
- LCF – Location Confirm (Сообщение о местоположении оборудования);
- LRJ – Location Reject (Отказ дать сведения о местоположении оборудования).

1.3 Сценарии обмена сообщениями протокола SIP

Протоколом SIP предусмотрены три 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, эти три сценария являются основными.

1.3.1 Установление соединения с участием сервера переадресации

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. 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). На рисунке 3 представлен сценарий установления соединения.

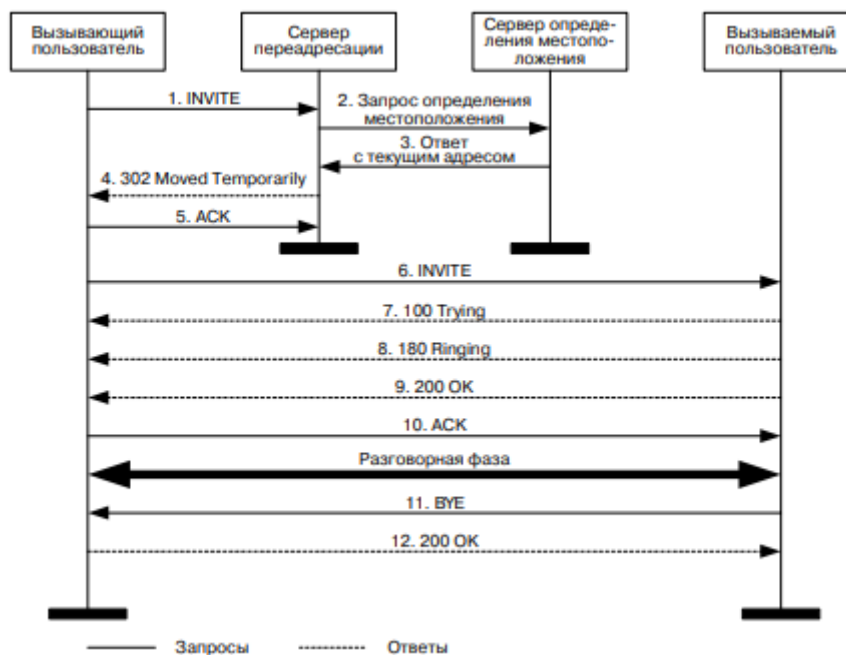


Рисунок 3 – Сценарий установления соединения через сервер переадресации

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 АСК (10). На этом фаза установления соединения закончена и начинается разговорная фаза.

По завершении разговорной фазы любой из сторон передается запрос ВУЕ (11), который подтверждается ответом 200 ОК (12).

1.3.2 Установление соединения с участием прокси-сервера

На рисунке 4 представлен сценарий установления соединения.

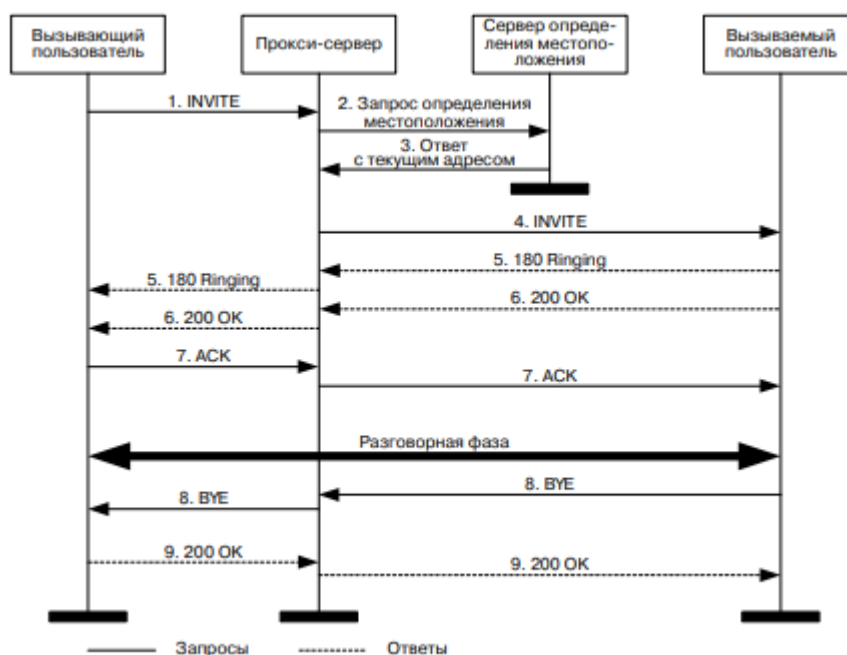


Рисунок 4 – Сценарий установления соединения через прокси-сервер

Администратор сети сообщает адрес этого сервера пользователям. Вызывающий пользователь передает запрос INVITE (1) на адрес прокси-сервера и порт 5060, используемый по умолчанию. 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 ОК (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 ОК (9).

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

1.3.3 Реализация дополнительных услуг на базе протокола SIP

Дополнительная услуга «Переключение связи» позволяет пользователю переключить установленное соединение к третьей стороне. На рисунке 5 приведен пример реализации этой услуги. Пользователь В устанавливает связь с пользователем А, который, переговорив с пользователем В, переключает эту связь к пользователю С, а сам отключается.

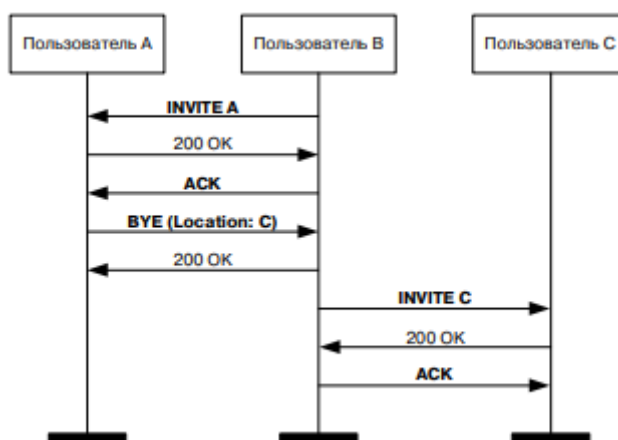


Рисунок 5 – Дополнительная услуга "Переключение связи"

Дополнительная услуга «Переадресация вызова» представлена на рисунке 6.

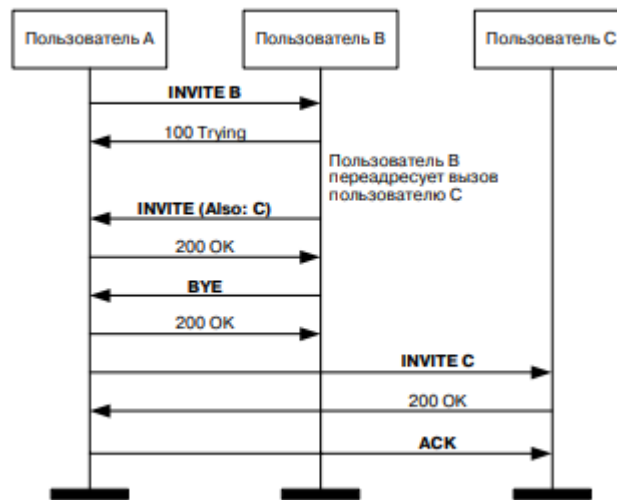


Рисунок 6 – Дополнительная услуга "Переадресация вызова"

Эта услуга 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 В, 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 А вызывает пользователя В, а терминал последнего переадресует вызов к пользователю С (5).

Дополнительная услуга «Уведомление о вызове во время связи» позволяет пользователю, участвующему в телефонном разговоре, получить уведомление о том, что к нему поступил входящий вызов и представлена на рисунке 7.

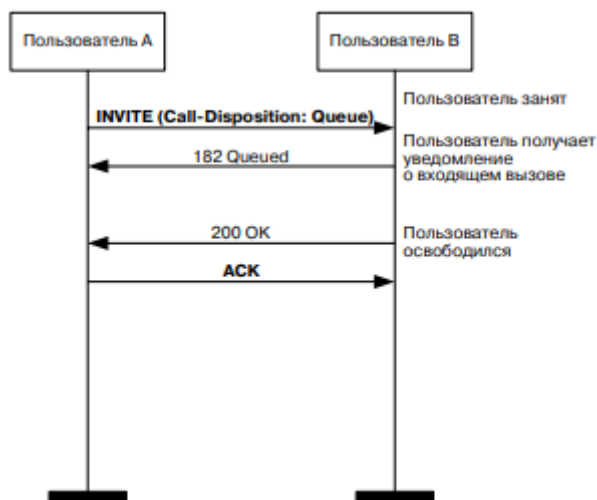


Рисунок 7 – Дополнительная услуга "Уведомление о вызове во время связи"

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 ОК.

1.4 Сценарий обмена сообщениями протокола H.323

В качестве примеров взяты случаи:

- вызываемый и вызывающий пользователи зарегистрированы в одном и том же привратнике, который маршрутизирует сигнальную и управляющую информацию;
- вызываемый и вызывающий пользователи соединяются непосредственно друг с другом, привратник в сети отсутствует.

Прежде чем рассматривать эти два сценария, отметим, что в общем случае алгоритмы установления, поддержания и разрушения соединений по H.323 включают в себя следующие фазы:

- фаза А. Установление соединения;
- фаза Б. Определение ведущего/ведомого оборудования и обмен данными о функциональных возможностях;
- фаза В. Установление аудиовизуальной связи между вызывающим и вызываемым оборудованием;
- фаза Г. Изменение полосы пропускания, запрос текущего состояния оборудования, создание конференций и обращение к дополнительным услугам;
- фаза Д. Завершение соединения.

1.4.1 Базовое соединение с участием привратника

Вызывающее оборудование передает сообщение ARQ с alias-адресом вызываемого абонента, в ответ на которое привратник передает сообщение ACF с уведомлением, что именно он будет маршрутизировать сигнальные сообщения (Gatekeeper routed call signaling), и с указанием транспортного адреса своего сигнального канала. Далее вызывающее оборудование передает на этот транспортный адрес запрос соединения Setup. Привратник пересылает сообщение Setup вызываемому оборудованию и передает вызывающему оборудованию сообщение Call Proceeding, означающее, что полученной информации достаточно для обслуживания поступившего вызова. Вызываемое оборудование также отвечает на Setup сообщением Call Proceeding. Если оборудование имеет возможность принять вызов, оно передает запрос допуска к ресурсам сети ARQ, на который привратник может ответить подтверждением ACF или отказом в допуске к ресурсам сети ARJ. Сценарий этого случая приведен на рисунке 8.

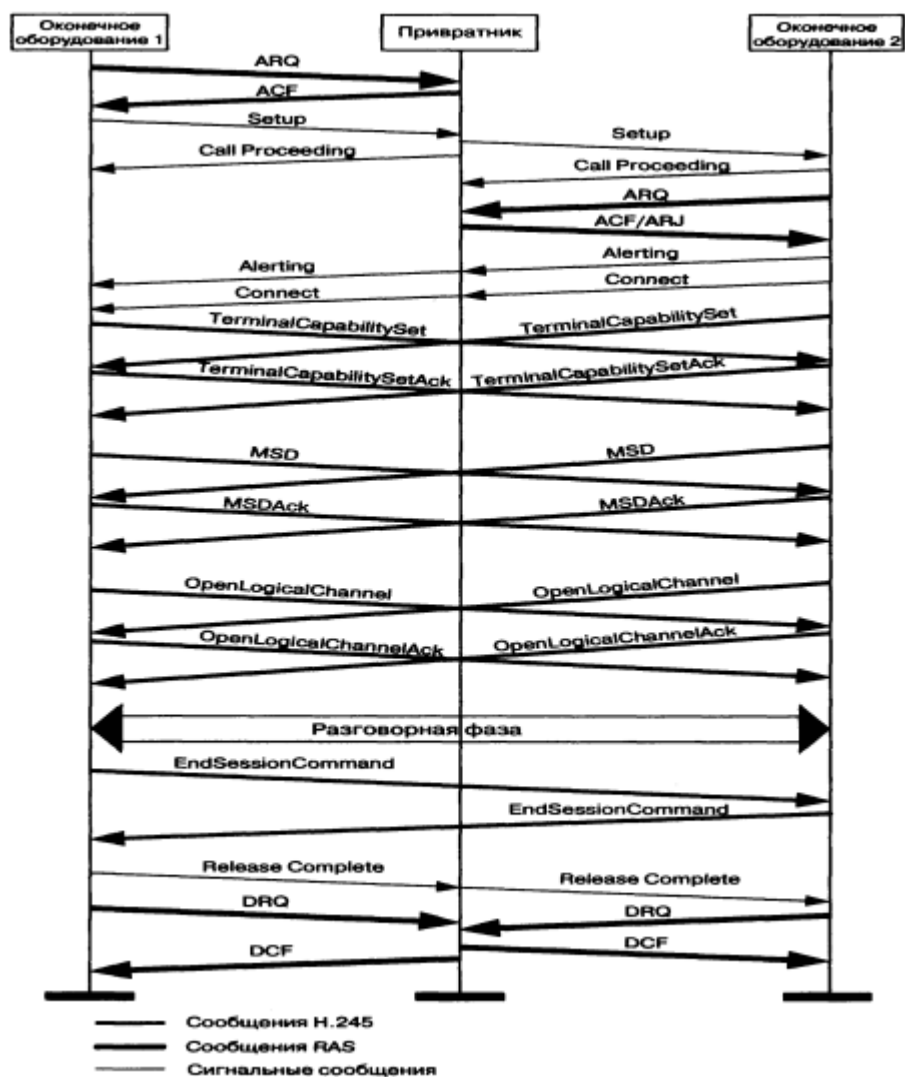


Рисунок 8 – Пример соединения с участием привратника

В первом случае вызываемое оборудование передает сообщение Alerting, и привратник маршрутизирует его к вызывающему оборудованию. Вызываемому пользователю подается визуальный или акустический сигнал о входящем вызове, а вызывающему дается индикация того, что вызываемый пользователь не занят и ему подается вызывной сигнал. При отказе в допуске к ресурсам сети вызываемое оборудование закрывает сигнальный канал путем передачи привратнику сообщения Release Complete.

После того как вызываемый пользователь примет входящий вызов, привратнику передается сообщение Connect с транспортным адресом управляющего канала N.245 вызываемого оборудования. Привратник заменяет

этот адрес транспортным адресом своего управляющего канала H.245 и пересылает Connect вызывающему оборудованию, после чего открывается управляющий канал H.245.

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

После открытия управляющего канала H.245 начинается обмен данными о функциональных возможностях оборудования. В рассматриваемом нами случае все управляющие сообщения, передаваемые от одного оконечного оборудования к другому, маршрутизируются привратником. Терминалы обмениваются сообщениями Terminal Capabilty Set, в которых указываются возможные алгоритмы декодирования принимаемой информации. Следует отметить, что сообщение Terminal Capablilty Set должно быть первым сообщением, передаваемым по управляющему каналу. Оборудование, принявшее сообщение Terminal Capablilty Set от другого оборудования, подтверждает его получение передачей сообщения Terminal Capablilty Set Ack.

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

В ответ на полученные сообщения master Slave Determination оба устройства передают сообщения master Slave Determination Ack, в которых

указывается, какое из этих устройств является для данного соединения ведущим, а какое - ведомым.

Так же возможен сценарий процедуры Master Slave Determination, предусматривающий сокращение количества передаваемых сообщений: оборудование, передавшее сообщение master Slave Determination и получившее в ответ сообщение master Slave Determination Ack, передает сообщение master Slave Determination Ack.

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

Далее открывается разговорная сессия. Оборудование вызывающего пользователя передает речевую информацию, упакованную в пакеты RTP/UDP/IP, на транспортный адрес RTP-канала оборудования вызванного пользователя, а вызванный пользователь передает пакетированную речевую информацию на транспортный адрес RTP-канала оборудования вызывающего пользователя. При помощи канала RTCP ведется контроль передачи информации по RTP каналам.

После окончания разговорной фазы начинается фаза разрушения соединения. Оборудование пользователя, инициирующего разъединение, должно прекратить передачу речевой информации, закрыть логические каналы и передать

по управляющему каналу сообщение H.245 end Session Command, означающее, что пользователь хочет завершить соединение. Далее от встречного оборудования ожидается сообщение end Session Command, после приема которого управляющий канал H.245 закрывается. Следующим шагом, если сигнальный канал еще открыт, передается сообщение Release Complete.

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

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

1.4.2 Базовое соединение без участия привратника

Теперь рассмотрим случай, когда вызываемое и вызывающее оборудование взаимодействуют непосредственно друг с другом, привратник в сети отсутствует. Пример установления соединения без участия привратника представлен на рисунке 9.

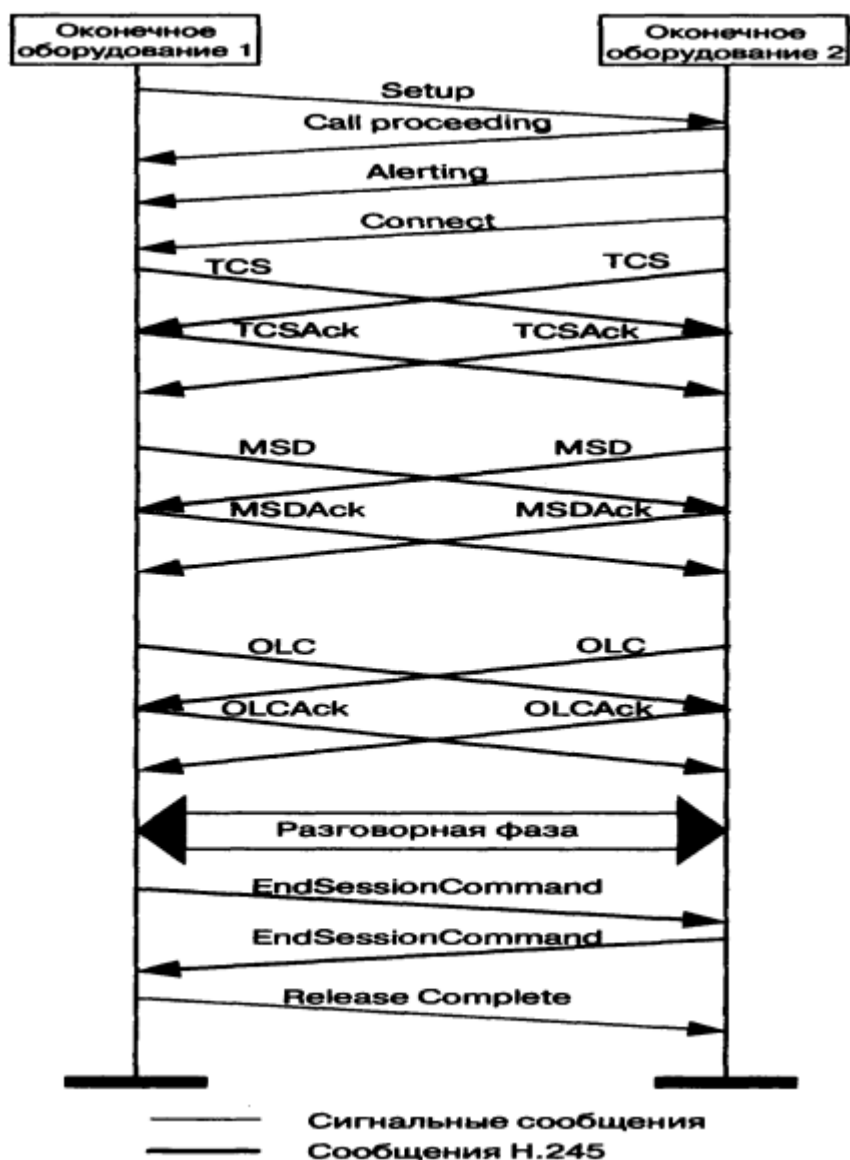


Рисунок 9 – Пример соединения без участия привратника

Вызывающее оборудование посылает запрос соединения Setup на известный транспортный адрес сигнального канала вызываемого оборудования. Вызываемое оборудование отвечает на Setup сообщением Call Proceeding, а затем - Alerting. Вызываемому пользователю дается визуальный или акустический сигнал о входящем вызове, а вызывающему - индикация того, что вызываемый пользователь не занят и получает вызывной сигнал.

Как только вызываемый пользователь примет входящий вызов, передается сообщение Connect с указанием транспортного адреса управляющего канала H.245 вызываемого оборудования, после чего этот канал открывается.

И здесь, чтобы ускорить открытие разговорной сессии, управляющий канал тоже может быть открыт вызываемым оборудованием после получения сообщения Setup с транспортным адресом управляющего канала H.245 вызывающего оборудования, или вызывающим пользователем после получения сообщения Call Proceeding или Alerting, в котором содержится транспортный адрес управляющего канала H.245 вызываемого оборудования.

После открытия управляющего канала выполняются все процедуры, описанные в первом случае: обмен данными о функциональных возможностях, определение ведущего/ведомого оборудования, открытие однонаправленных логических каналов.

Далее открывается разговорная сессия. Оборудование вызывающего пользователя передает речевую информацию, упакованную в пакеты RTP/UDP/IP, на транспортный адрес RTP-канала оборудования вызываемого пользователя, а оно, в свою очередь, передает пакетированную речевую информацию на транспортный адрес RTP-канала оборудования вызывающего пользователя.

После окончания разговорной фазы начинается фаза разрушения соединения. Оборудование пользователя, инициирующего разъединение, прекращает передачу речевой информации, закрывает логические каналы и передает по управляющему каналу сообщение H.245 end Session Command, означающее, что пользователь хочет завершить соединение. Ожидается сообщение end Session Command от встречного оборудования, после чего управляющий канал H.245 закрывается. Следующим шагом передается сообщение Release Complete, и сигнальный канал закрывается.

Пользователь, получивший команду end Session Command от пользователя, инициировавшего разъединение, должен прекратить передачу речевой информации, закрыть логические каналы и передать сообщение end Session Command. Далее, если сигнальный канал остался открытым, передается сообщение Release Complete, сигнальный канал закрывается, и обслуживание вызова считается завершенным.

1.4.3 Туннелирование управляющих сообщений

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

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

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

1.4.4 Процедура быстрого установления соединения

Самый быстрый способ установления соединения в сети, базирующейся на рекомендации H.323, - это использование процедуры Fast Connect. Чтобы инициировать процедуру Fast Connect, вызывающее оборудование передает сообщение Setup с элементом fast Start. Этот элемент может включать в себя одну или несколько структур Open Logical Channel. Одна из структур Open Logical Channel обязательно должна содержать элемент forward Logical Channel Parameters и может содержать элемент reverse Logical Channel Parameters, но, в то

же время, структура Open Logical Channel описывает точно один однонаправленный логический канал. Это означает, что когда описывается прямой логический канал, то в структуре присутствует только элемент forward Logical Channel Parameters. Элемент содержит информацию об алгоритме, который используется вызывающим оборудованием для кодирования передаваемой информации, и адрес канала RTCR. При описании канала обратного направления в элементе forward Logical Channel Parameters не содержится никакой информации, хотя сам он обязательно присутствует, а в элементе reverse Logical Channel Parameters содержатся сведения об алгоритме декодирования принимаемой информации, транспортный адрес RTP, на который следует передавать информацию, и адрес канала RTCR.

В элементе fast Start может присутствовать несколько альтернативных структур Open Logical Channel, различающихся алгоритмами кодирования передаваемой информации или декодирования принимаемой информации, причем наиболее предпочтительные алгоритмы указываются в первую очередь.

Вызываемое оборудование может отклонить процедуру Fast Connect, либо если оно ее не поддерживает, либо если существует потребность в использовании процедур H.245 с открытием отдельного канала H.245 или с Туннелированием управляющих сообщений. В этом случае элемент fast Start не включается ни в одно из сообщений, передаваемых после приема Setup, до сообщения Connect включительно. Открытие логических каналов для передачи речевой информации производится с использованием процедур H.245.

Вызываемое оборудование, получившее сообщение Setup с элементом fast Start и могущее поддержать процедуру Fast Connect, должно включить элемент fast Start в любое из сообщений Q.931, передаваемых после приема Setup, до сообщения Connect включительно. Элемент fast Start содержит структуры Open Logical Channel, которые выбраны вызываемым оборудованием из структур, предложенных вызывающим оборудованием. И снова одна из структур Open Logical Channel содержит элемент forward Logical Channel Parameters со

сведениями об алгоритме кодирования информации, с транспортными адресами каналов RTP и RTCP вызываемого оборудования. Вторая структура Open Logical Channel включает в себя элемент forward Logical Channel Parameters, не содержащий никакой информации, и элемент reverse Logical Channel Parameters со сведениями об алгоритме кодирования информации и с транспортным адресом канала RTCP вызываемого оборудования.

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

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

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

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

1.5 Достоинства и недостатки протокола SIP

Из достоинств можно отметить:

- наличие дополнительных услуг связи – к ним относятся переадресация, удержание вызовов, поддержка нескольких линий, передача видео и т. д.;
- отсутствие привязки абонента к какому-либо месту – мы можем уехать на другой конец города, на дачу, в санаторий, на Дальний Восток или вообще другую страну, совершенно бесплатно оставаясь на связи там, где есть доступ в интернет. Вместе с абонентом мигрирует и его телефонный номер;
- нет нужды в покупке дорогого оборудования – зачастую необходим всего лишь самый обычный компьютер, подключенный к интернету;
- моментальное предоставление добавочных номеров – возможность в один момент передать свой номер людям, дабы они могли тут же с вами связаться без каких либо проблем посредством традиционной телефонии;
- быстрая скорость подключения к поставщику услуг – зачастую, аккаунт который вы создаете, после регистрации будет сразу активен. Т.е. вам сразу будут доступны внутрисетевые звонки другим SIP-абонентам, притом совершенно бесплатно;
- применение SIP-протокола позволяет с лёгкостью расширять сети на тысячи и десятки тысяч абонентов;
- лёгкость в освоении – описание спецификаций занимает 150 листов против 700 листов у протокола H.323;
- лёгкость в расширении – при необходимости сюда можно внедрить новые сервисы.

Недостатков со стороны протокола наблюдается немного:

- нельзя дозвониться до абонента, если он отключился от сети (не везде можно обойтись без традиционной телефонии или мобильной связи). Решить проблему потери контакта можно воспользовавшись функциями автоответчика;
- перебои в качестве связи. Отмечается, что некоторые абоненты жалуются на ухудшение качества связи. Как правило, ухудшение качества связи связано с проблемами со стороны провайдера, либо со стороны абонента, а так же могут повлиять сторонние каналы передачи данных.

1.6 Достоинства и недостатки протокола H.323

Протокол H.323 всеобъемлющ. Он может использоваться в полных сетях конференц-связи для передачи аудио и видео данных. Выгоды от реализации конференц-связи со стандартом H.323 не мало:

- стандарт H.323 обеспечит очень качественную конференц-связь на базе мультимедиа. Такая конференц-связь поддерживает: совместную работу по передаче данных или видео, а так же коллективное редактирование растровых изображений;
- благодаря стандарту H.323 есть возможность взаимодействия оборудования от различных производителей на базе H.320 и H.323;
- технология H.323 позволит с выгодой использовать имеющиеся капиталовложения в инфраструктуру корпоративной сети;
- технологию H.323 можно использовать для междугородных и международных телефонных соединений, чтобы снизить их стоимость;

- с помощью технологии H.323 можно эффективнее использовать технологию ISDN(Integrated Services Digital Network, цифровая сеть с интеграцией служб) применяя шлюзы H.320 и уменьшая число линий ISDN;
- в корпоративной интрасети благодаря технологии H.323 обеспечиваются надежные соединения и уменьшаются проблемы с поддержкой;
- технология H.323 открывает доступ к более сложному управлению конференц-связи в сети;
- технология H.323 не зависит от обеспечения аппаратуры и ее операционной системы.

В сравнении с SIP у H.323 имеются недостатки:

- технология H.323 на установку соединения расходует больше времени;
- технологии H.323 для установки соединения требуется примерно 12 пакетов, в то время как для SIP необходимо примерно четыре пакета;
- чтобы установить соединение, технология H.323 нуждается в TCP и UDP;
- в отличие от SIP, реализация технологии H.323 гораздо сложнее;
- с помощью технологии H.323 управление вызовом третьей стороны невозможно.

1.7 Области практического применения протокола SIP

SIP-протокол отвечает за установление соединения между абонентами. Чтобы совершать звонки с его помощью, необходимо специальное оборудование: SIP-телефон, телефон с SIP-шлюзом, мобильное или десктопное устройство и программы для разговора — софтфоны.

Данный протокол активно используется в IP-телефонии, в том числе для работы виртуальных АТС (услуга, заменяющая физическую офисную телефонную станцию). Пользователи могут вызывать друг друга, обмениваться файлами и мультимедийной информацией, привлекать к установленному сеансу других участников, управлять переводом звонков. Также он используется при проведении сеансов видеосвязи и видеоконференций. Нельзя не отметить и его применение в онлайн-играх, где нужно соединить двух и более игроков.

1.8 Области практического применения протокола H.323

Стандарт H.323 протокола постепенно выходит из оборота, в частности, для телефонов. Несколько лет назад многие производители телефонов отказались от тенденций создания устройств, которые могли бы использовать оба протокола IP-телефонии. Сегодня в основном применяется SIP. Однако на данный момент у многих пользователей есть устройство стандарта H.323.

H.323 использует телекоммуникационный подход к передаче голоса и видео по IP, в то время как SIP - использует интернет-подход.

1.9 Сравнительный анализ протоколов H.323 и SIP

Изначально протокол H.323 разрабатывали опираясь на традиционную телефонию, а протокол SIP на сети Internet. Однако их задачи заключались в одном и том же. Со временем протокол SIP и H.323 постоянно улучшали свои возможности и сравнительный анализ проведен из нижеперечисленных критериев.

1.9.1 Дополнительные услуги

Стоит отметить, что набор услуг обоих протоколов примерно одинаков. Единственная проблема протокола SIP, что его дополнительные услуги не стандартизированы, что может иногда вызывать конфликт оборудования разных

фирм. В то время как у протокола H.323 они стандартизированы. В данный момент эта проблема решается специалистами.

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.

Обратим внимание на услугу конференция. Протокол SIP предусматривает три способа организации этой услуги. В двух случаях нет необходимости в центральном контроллере, Это значит что функциями управления конференцией обладают все терминалы, что позволяет вести конференции с неограниченным количеством участников. В третьем случае используется MCU (Multipoint Control Unit, устройство управления конференциями), в режиме многоадресной рассылки и соединения участников друг с другом.

В стандарте H.323 так же три способа организации этой услуги. Все эти способы построены на управлении контролером MC (Multipoint Controller, обработка сигнальных сообщений). У одного терминала необходимо наличие MC, вдобавок данный терминал не может покинуть конференцию. В то же время данный стандарт обеспечивает качественную конференц-связь.

Достоинством протокола SIP является то, что при многоадресной рассылке можно передавать не только речевой информации, но и сигнальных сообщений.

Так же у протокола SIP есть функция, с помощью которой можно организовать связь третьей стороне. Здесь предусмотрены набор номера секретарем, или сопровождение вызова оператором из call-center (центр обслуживания звонков). Важно, все это есть и в стандарте H.323, но техническая реализация данных услуг сложнее, как любых других.

Если раньше у протокола SIP было меньше возможностей управлениями услугами, чем у стандарта H.323, то сейчас эта проблема решена.

Вдобавок ко всему, у стандарта H.323 есть еще один минус. При обслуживании вызова, у него отсутствует возможность указать приоритет.

1.9.2 Персональная мобильность пользователей

В отличие от протокола H.323, протокол SIP более гибкий в этом вопросе. Он предоставляет объемный набор средств поддержки. Персональная мобильность пользователей организуется путем регистрации местоположения на сервере. С данным сервером может взаимодействовать любой протокол.

Как уже было сказано выше, протокол SIP более гибкий чем H.323. В частности протокол SIP ищет пользователя по нескольким направлениям одновременно, а H.323 в одном.

1.9.3 Расширяемость протокола

С эволюцией технологий, очень важно чтобы протоколы обзаводились улучшенной версией и обеспечивалась совместимость версий. Т.е. расширяемость протокола отвечает за стандартизацию протоколов и согласование параметров.

Несовместимость версий не так страшна для протокола SIP. Если оборудованию какие то запросы будут не понятны, то они просто игнорируются.

Если необходимо, организация IANA (Internet Assigned Numbers Authority) может зарегистрировать новые запросы.

В протоколе H.323 так же поддерживаются старые версии новыми. Однако бывает, что производители поддерживают лишь одну версию, чтобы облегчить процесс работы.

Регистрация новых возможностей в протоколе H.323 происходит при помощи поля NonStandardParameter. Здесь производитель указывает свои услуги, которые действительны только для него. Это увеличивает спектр услуг, но есть и недостатки. Невозможно запросить информацию о поддерживаемых функциях и изменить уже существующую. Отсюда проблемы с поддержкой оборудования от разных производителей.

Набор кодеков тоже оказывает влияние на расширяемость протокола. Производитель иногда необходим иной набор кодеков и тогда он просто регистрирует его в IANA.

В протоколе H.323 все кодеки стандартизируются, и если использовать приложения с нестандартными наборами кодека, то будут возникать проблемы.

Протокол SIP представляет собой набор модулей. Эти модули работают независимо друг от друга и их можно заменять.

Протокол H.323 представляет собой единый набор протоколов и для новой услуги необходима модификация всех его составляющих.

1.9.4 Масштабируемость сети

Во время сеанса связи привратник H.323 содержит в себе информацию о нем. В то время как сервер-SIP эту информацию не содержит. Поэтому он может обработать больше сеансов связи, чем H.323. Однако отсутствие такой информации может вызвать некоторые проблемы.

Не стоит забывать про зонную архитектуру H.323. Она увеличивает количество зон. Это приводит к расширению сети.

1.9.5 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.

1.9.6 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 не, обходимо 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.

Заключение

По проделанной работе можно заключить, что протокол SIP в наше время используется все чаще и чаще. В силу своей простоты и удобства его предпочтет большинство поставщиков услуг. Данный протокол активно используется в виртуальных АТС (услуга, заменяющая физическую офисную телефонную станцию). Пользователи могут вызывать друг друга, обмениваться файлами и мультимедийной информацией, привлекать к установленному сеансу других участников, управлять переводом звонков. Используется при проведении сеансов видеосвязи и видеоконференций, а так же в онлайн играх, где необходимо соединение двух и более участников.

Можно с уверенностью заявить, что в наше время, предпочтительным является протокол SIP.

Здесь стоит отметить, что ранее в оборудование H.323 поставщиками услуг уже были вложены значительные деньги. Оно так же успешно функционирует, и потому до сих пор используется. Вдобавок у многих пользователей пока остаются устройства стандарта H.323. Однако то время, когда для операторов телефонной связи были не так важны услуги Internet, уже уходит в прошлое. Большинство производителей телефонов несколько лет назад уже отказались от тенденции создавать устройства, поддерживающие оба протокола, в основном применяя только SIP.

Так же в настоящее время операторы телефонной связи все чаще нацелены на дополнительные услуги с доплатой. Преимуществ тем больше, чем проще реализация дополнительных услуг. И здесь протокол SIP в сравнении с H.323 является явным фаворитом.

Библиографический список

- 1 Протокол SIP: пятый справочник / Б. С. Гольдштейн, А. А. Зарубин, В. В. Саморезов. – СПб.: БХВ – Петербург, 2005. – 456 с.
- 2 Протоколы сети доступа: Том 2 (3-е издание) / Б. С. Гольдштейн. – СПб.: БХВ – Петербург, 2005. – 288 с.
- 3 Сигнализация в сетях связи: Том 1 (4-е издание) / Б. С. Гольдштейн. – СПб.: БХВ – Петербург, 2005. – 448 с.
- 4 IP–телефония: 3-е издание / Б. С. Гольдштейн, А. В. Пинчук, А. Л. Суховицкий. – М.: Радио и связь, 2006. – 336 с.
- 5 Сети связи: учеб. Пособие / Б. С. Гольдштейн, Н. А. Соколов, Г. Г. Яновский. – СПб.: БХВ – Петербург, 2014. – 400 с. ил.: – (Учебная литература для вузов)
- 6 Call-центры и компьютерная телефония: учеб. Пособие / Б. С. Гольдштейн, В. А. Фрейнкман. – СПб.: БХВ – Петербург, 2006. – 368 с.
- 7 Телекоммуникационные сети: Монография в 4-х главах. Глава 4 / Н. А. Соколов. – М., Альварес Пабблишинг, 2004. – 191 с.
- 8 Исследование протокола SIP [электронный ресурс]. Режим доступа: https://studwood.ru/1651059/tehnika/issledovanie_protokola, свободный.
- 9 Сигнализация H.323 [электронный ресурс]. Режим доступа: <http://tnu.podelise.ru/docs/index-289191.html?page=28>, свободный.
- 10 Основы IP-телефонии, базовые принципы [электронный ресурс]. Режим доступа: <https://habr.com/ru/post/183152/>, свободный.
- 11 Протоколы IP-телефонии [электронный ресурс]. Режим доступа: <http://voiplab.by/wiki/new-voip-technology/100-protokoly-ip-telefonii>, свободный.
- 12 Назначение протокола SIP [электронный ресурс]. Режим доступа: <http://zaysev.me/index.php/myblog/entry/2016/01/24/protokol-sip>, свободный.

- 13 Стандарт H.323 [электронный ресурс]. Режим доступа: <https://trueconf.ru/h323.html>, свободный.
- 14 Технология H.323 [электронный ресурс]. Режим доступа: http://aek-54.ru/ip_tlf/lektion/L5_H323.pdf, свободный.
- 15 Протокол H.323 [электронный ресурс]. Режим доступа: <https://www.intuit.ru/studies/courses/8/8/lecture/245?page=3>, свободный.
- 16 H.323, протокол, шлюзы, порты, настройка и применение [электронный ресурс]. Режим доступа: <http://fb.ru/article/470801/h-protokol-shlyuzyi-portyi-nastroyka-i-primenenie>, свободный.
- 17 VoIP-протоколы применяемые в IP-телефонии [электронный ресурс]. Режим доступа: <https://telcom.pro/voip-protokoly-v-ip-telefoniy/>, свободный.
- 18 Протокол H.323 и SIP [электронный ресурс]. Режим доступа: <http://iptop.net/sip/09.php>, свободный.
- 19 Что такое SIP протокол [электронный ресурс]. Режим доступа: <https://blog.zebratelecom.ru/how/chto-takoe-sip-protokol.html>, свободный.
- 20 Взаимодействие клиентов SIP [электронный ресурс]. Режим доступа: <https://habr.com/ru/post/188352/>, свободный.