**Internet-телефония как двигатель SIP**

Христиан Штредике

Шумиха вокруг недорогих или вовсе бесплатных телефонных разговоров по internet помогла окончательно утвердиться S1P как протоколу для передачи голоса по IP. Наибольший интерес к нему проявляется в сегменте конечных пользователей и малых/домашних офисов (SOHO), т. е. в случае телефонных звонков по соединениям DSL. Однако и производители телекоммуникационных систем с поддержкой IP не могут более игнорировать SIP. В статье подробно рассказывается о техническом развитии и изменении стандарта SIP.

Изначально считалось, что протокол SIP для передачи голоса по IP разработчикам будет реализовать проще, чем устоявшийся, но сравнительно сложный конкурирующий протокол Н.323. Эти времена давно прошли. Сегодня стандарты, относящиеся к SIP, уже насчитывают более 2 тыс. страниц, a IETF все еще усердно утверждает новые запросы на комментарии (Requests for Comments, RFC). Речь идет не столько об основополагающих темах, сколько об эзотерических: о транспортном уровне, «политике сеансов» или просто-напросто о том, каким образом медиа-сервер должен перехватывать нажатия клавиш и транслировать их на сервер приложений (см. Рисунок 1).

Для конечного пользователя такие нюансы едва ли имеют значение, поскольку используемый в повседневной жизни набор функций должен оставаться стабильным. Производители из области SIP уже настолько хорошо освоились с существующими стандартами, что продукты разных компаний в основном совместимы друг с другом. В областях, где IETF пока еще не установила окончательного стандарта, часто производители сами находят прагматические решения. К примеру, Broadsoft определила, каким образом должно осуществляться управление светодиодными индикаторами телефонов и как на телефоне можно принять звонок с компьютера.

Однако стандарт SIP не бесспорен, «конкуренция» поджимает со всех сторон: так, поставщику Skype удалось чуть ли не за ночь занять рынок бесплатной Internet-телефонии, да и вообще создать его. Вместо того чтобы ввязываться в дискуссии о стандартизации, инженеры Skype предпочли сами творить историю, предложив собственный подход. То обстоятельство, что при использовании этого метода трафик частично проходит через компьютеры, которые не имеют никакого отношения к участвующим в разговоре пользователям, вследствие чего приходится мириться с неустранимым риском вторжения в частную сферу, по всей видимости, никому не мешает. Для дальнейшего успеха очень важно, примут ли эту технологию в качестве стандарта такие игроки, как Cisco и Microsoft, — вопрос пока открыт. Еще один протокол VoIP, IAX, наделал очень много шума в связи с перспективой появления нового стандарта. В спецификации IAX меньше 50 страниц, и привлекает она своей простотой. Воодушевленное этим фактом сообщество открытых исходных кодов, организовавшееся вокруг проекта Asterisk, рассчитывает в связи с этим на появление недорогого оборудования для передачи голоса по IP. Однако речь в случае IAX идет о полностью самостоятельном протоколе. Стань он разработкой более крупного игрока, возмущению не было бы предела. А теперь, как и в случае со Skypc, IAX остается ждать, согласятся ли его принять лидеры рынка.

**NAT: решение проблемы**

Преобразование сетевых адресов (Network Address Translation, NAT), как и прежде — одна из важнейших проблем при передаче голоса по IP. В последние годы производители маршрутизаторов DSL и брандмауэров занимались в первую очередь HTTP и SMTP. Типичным для этих протоколов является то, что действия всегда инициируются клиентом: электронная почта ему никогда не доставляется — каждые несколько минут он сам вынужден проверять, нет ли на почтовом сервере непрочитанных сообщений.

В случае телефонии этот подход больше не работает. Сервер (в Internet) должен быть в состоянии доставить клиенту (в локальной сети) сообщение, что достигается благодаря ограничению срока действия регистрации клиента, когда тому приходится регистрироваться снова и снова. При этом заносится «отметка» в таблицу NAT, через которую сервер отправляет входящие сообщения. Возникающий при таком методе «дежурный» трафик не стоит недооценивать — на каждого пользователя за месяц приходится до 100 Мбайт. Многие операторы скорее смирятся с большим количеством трафика, чем станут объяснять своим клиентам, как им следует конфигурировать маршрутизаторы.

Проблема NAT решается путем простого прохождения UDP через NAT (Simple Traversal UDP over NAT, STUN). Этот стандарт (RFC 3489) позволяет конечным устройствам в сети «взглянуть на себя в зеркало» при помощи внешнего сервера и таким образом обеспечить правильное соответствие общедоступных и локальных IP-адресов. Однако STUN функционирует не во всех случаях: если брандмауэр использует так называемую симметричное преобразование NAT, то конечное устройство становится достижимым через Internet только с сервера STUN, а пакеты иного происхождения, к примеру от IP-телефонов, не пропускаются. STUN работает во многих средах, однако успешное применение этого протокола, к сожалению, остается делом случая.

Новый инфраструктурный компонент для операторских сетей, который решает проблему симметричной трансляции NAT, называется пограничным контроллером сеансов (Session Border Controller, SBC). Вначале он был оценен IETF как «неудачный», однако позже стало ясно, что без пего, к сожалению, не обойтись. Благодаря SBC подавляющее большинство абонентов Internet-телефонии могут пользоваться своим IP-телефоном без необходимости внесения каких-либо изменений в маршрутизатор или конечное устройство (см. Рисунок 2). Наряду с решением проблемы NAT контроллер SBC позволяет, к примеру, операторам прерывать разговор, когда средства на счету клиента истекли. Кроме того, с его введением решается и проблема фрагментации UDP, когда маршрутизатор не может корректно переправлять очень большие пакеты. Поскольку SBC не дает полной информации о маршрутизации, пакеты обычно столь малы, что трудностей не возникает. Для оператора такая технология привносит интересный побочный эффект: когда клиенты не видят информации о маршрутизации, они не могут напрямую связаться с собеседником и обойти при этом оператора и связанный с этим биллинг.

**QOS: берега пока не видно**

Когда речь идет о передаче голоса по IP в пределах корпоративных сетей, должное качество услуг (Quality of Service, QoS) подразумевается само собой. Это утверждение справедливо также применительно к различным предложениям операторов и провайдеров для соответствующих соединений через глобальную сеть. Иначе выглядит ситуация в области SOHO, где у пользователей также есть желание приобщиться к Inlernet-телефонии по недорогим соединениям DSL. Локальный маршрутизатор DSL в состоянии сортировать покидающие локальную сеть пакеты по исходящим очередям в соответствии с QoS, однако обратное направление контролирует провайдер.

По опыту Германии можно сказать, что ситуация в этой области оставляет желать лучшего, поскольку соответствующе биты QoS, как правило, игнорируются. Гораздо чаще оператор предоставляет пакетам TCP более высокий приоритет, чем UDP. К сожалению, загрузка в большинстве случаев происходит по TCP, и поэтому она может заметно мешать параллельным телефонным разговорам по IP. На данный момент существуют два решения этой проблемы. Первое заключается в выборе провайдера, предлагающего QoS. При использовании SBC он способен обеспечит правильную сортировку пакетов, даже если входящие пакеты VoIP не маркированы битами QoS. Второе, скорее прагматическое, решение состоит в том, чтобы арендовать второй канал DSL и физически разделить голос и данные. Этот вариант функционирует очень хорошо, и при коммерческом использовании часто оправдывает себя экономически.

**Безопасность: старая тема на новый лад**

С растущей привлекательностью телефонии на базе Internet возникают схожие проблемы, связанные с безопасностью, как и в других областях коммуникаций по IP: речь идет о спаме, хакерских атаках и попытках прослушивания. По аналогии с «сорной» почтой наблюдается настоящая волна «сорных» звонков: снам по Internet-телефонии (Spam via Internet-Telephony, SPIT). Поисковая машина Google выдает уже более 130 тыс. совпадений но теме «снам и SPIT». Принцип прост: когда телефонные звонки бесплатны, «спитеры» могут запустить из какой-либо части Internet миллионы звонков, и те, кто их принимает, слышат, что выиграли, например, путешествие на юг Тихого океана. Целевые адреса получить достаточно просто, испробовав все номера, предоставляемые провайдером его клиентам.

Меры противодействия известны по борьбе с традиционным спамом. Во-первых, операторы начинают вести так называемые «белые списки». Как правило, они охватывают адресный потенциал партнеров-операторов. В случае звонка из Internet от третьей стороны он отклоняется. Во-вторых, составляются и «черные списки», содержащие данные о клиентах, рассылающих SPIT, что может происходить и автоматически, когда клиент инициирует больше звонков, чем в состоянии это сделать.

По всей видимости, дело дошло до первых вирусных звонков, содержащих манипулируемый пакет данных: хотя он и не приводит к отказу всей системы, но посредством соответствующего программного кода преобразуется в послушного робота, который по команде превращается, к примеру, в подслушивающий жучок. В таких случаях рекомендуется проинформировать как производителя оконечного устройства, так и провайдера. Для предотвращения подобных атак в будущем существует достаточное количество технических возможностей.

Наряду с так называемыми атаками DoS (к ним относится и SPIT) важную роль играет защита частной сферы, для чего используются методы, аналогичные тем, что специфицированы в HTTP. Анало-гвм HTTPS является SIPS, «защищенный» стандарт SIP. Как и в случае HTTPS, для идентификации участников служат сертификаты, они представляют базис для согласования необходимого ключа. Соответствующим образом SRTP является дополнением протокола передачи данных в реальном времени (Real Time Transport Protocol, RTP), причем используется шифрование AES с длиной ключа 128 бит. Обмен ключами происходит посредством SIPS. На данный момент дискуссия о корректной формулировке стандарта еще не окончена, однако все вопросы должны быть разрешены в ближайшие месяцы, и при помощи SIPS и SRTP будет возможным полноценное шифрование переговоров.

Заметим, что упомянутые пограничные контроллеры сеансов в случае SIPS и SRTP могут расшифровывать переговоры. С точки зрения провайдеров, это очень удобно, поскольку по решению судов иногда они вынуждены прослушивать некоторые соединения, а вот конечному пользователю это вряд ли понравится. Поэтому по аналогии с электронной почтой в области SIP были определены S/MIME для сквозного шифрования, в результате чего оператор не сможет прослушивать разговоры. Правда, возникает вопрос, согласятся ли законодательные органы терпеть сквозное шифрование перед лицом террористических угроз, ведь владельца proxy-сервера (да еще и расположенного за границей) прослушать практически невозможно.

**SIP в офисе**

SIP получил распространение прежде всего в области конечных пользователей и при подключении небольших и домашних офисов. Однако решения VoIP для корпоративной области, где до сих пор часто встречаются нестандартные технологии, дают основания полагать, что SIP и здесь будет играть более важную роль. В области телекоммуникационных систем на базе SIP сообщения о прогрессе связаны не столько с появлением новинок в стандартизации, сколько с внедрением существующих стандартов. Выбор пригодных для использования решений заметно расширился, равно как и спектр предложений совместимых устройств. Все явственнее прослеживается тенденция, когда пользователю телекоммуникационной системы не приходится приобретать все компоненты у одного производителя. Наряду со специализированными компаниями крупные игроки исходят из того, что они не должны больше выпускать систему целиком. Если не случится непредвиденного, вскоре вариантов будет так же много, как и в компьютерной отрасли.

Несколько менее радует основополагающая коммуникационная архитектура. В принципе, технологический подход SIP заключался как раз в том, чтобы устройства по большей части взаимодействовали непосредственно друг с другом. По сравнению с централизованной концепцией ее преимущество состоит в том, что такие системы гораздо лучше масштабируются, и при передаче мультимедийных данных задержка заметно короче. К сожалению, по причине высокой сложности этот подход, по всей видимости, потерпел неудачу: большинство систем VoIP использует традиционную топологию телекоммуникационной телефонной станции и поддерживает только прямые соединения с конечными устройствами. Аналоговый кабель телекоммуникационной системы заменяется, если можно так сказать, на SIP. И пользователям не стоит об этом беспокоиться, пока их проблемы решаются . LAN

**Список литературы**

Журнал LAN №8 2005