Інформаційні технології

УДК 004.852

Ситник Артем Вадимович
бакалавр комп'ютерних наук
Національного технічного університету України
«Київський політехнічний інститут імені Ігоря Сікорського»
Сытник Артем Вадимович
бакалавр компьютерных наук
Национального технического университета Украины
«Киевский политехнический институт имени Игоря Сикорского»
Sytnyk Artem
Bachelor of computer science
The National Technical University of Ukraine
«Igor Sikorsky Kyiv Polytechnic Institute»

ПРОТОКОЛ SIP ЯК ОСНОВА IP ТЕЛЕФОНІЇ
ПРОТОКОЛ SIP КАК ОСНОВА IP ТЕЛЕФОНИИ
SIP PROTOCOL AS THE BASIS OF IP TELEPHONY

Анотація. У статті описані принципи роботи IP-телефонії та застосування протоколу SIP.

Ключові слова: SIP, IP-телефонія, NAT, QoS, DSL.

Аннотация. В статье описаны принципы работы IP-телефонии и применение протокола SIP.

Ключевые слова: SIP, IP-телефония, NAT, QoS, DSL.

Summary. the article describes the principles of IP telephony and the application of the SIP protocol.

Key words: SIP, IP-telephony, NAT, QoS, DSL.

Галас навколо недорогих або зовсім безкоштовних телефонних розмов по мережі Інтернет допоміг остаточно утвердитися SIP як протоколу для передачі голосу по IP. Найбільший інтерес до нього проявляється в сегменті кінцевих користувачів у офісах чи вдома, тобто в разі телефонних дзвінків по з'єднаннях DSL. Однак і виробники телекомунікаційних систем з підтримкою IP не можуть більше ігнорувати SIP. У статті докладно розповідається про технічний розвиток і зміни стандарту SIP.

Спочатку вважалося, що протокол SIP для передачі голосу по IP розробникам буде реалізувати простіше, ніж усталений, але порівняно складний конкуруючий протокол H.323. Ці часи давно пройшли. Сьогодні стандарти, які стосуються SIP, вже налічують понад 2 тисячі сторінок.

Для кінцевого користувача такі нюанси навряд чи мають значення, оскільки набір функцій, що використовується в повсякденному житті, повинен залишатися стабільним. Виробники в області SIP вже настільки добре освоїлися з існуючими стандартами, що продукти різних компаній, в основному, сумісні один з одним.

Однак стандарт SIP не беззаперечний, «конкуренція» підтискає з усіх боків: так, постачальнику Skype вдалося мало не за ніч зайняти ринок безкоштовної IP-телефонії, та й взагалі створити його. Замість того, щоб вплутуватися в дискусії про стандартизацію, інженери Skype віддали перевагу самостійно творити історію, запропонувавши власний підхід.

NAT: вирішення проблеми

Перетворення мережних адрес (Network Address Translation, NAT), як і раніше – одна з найважливіших проблем при передачі голосу по IP. В останні роки виробники маршрутизаторів DSL і брандмауерів займалися в першу чергу HTTP і SMTP. Типовим для цих протоколів є те, що дії завжди ініціюються клієнтом: електронна пошта йому ніколи не

доставляється - кожні кілька хвилин він сам змушений перевіряти, чи немає на поштовому сервері непрочитаних повідомлень.

У разі телефонії цей підхід більше не працює. Сервер (у Internet) повинен бути в змозі доставити клієнтові повідомлення, що досягається завдяки обмеженню терміну дії реєстрації клієнта, коли тому доводиться реєструватися знову і знову. При цьому заноситься «відмітка» в таблицю NAT, через яку сервер відправляє вхідні повідомлення. «Черговий» трафік, який виникає при такому методі, не варто недооцінювати - на кожного користувача за місяць припадає до 100 Мбайт. Багато операторів швидше змиряться з великою кількістю трафіку, ніж стануть пояснювати своїм клієнтам, як їм слід конфігурувати маршрутизатори.

Проблема NAT вирішується шляхом простого проходження UDP через NAT (Simple Traversal UDP over NAT, STUN). Цей стандарт (RFC 3489) дозволяє кінцевим пристроям в мережі «поглянути на себе в дзеркало» за допомогою зовнішнього сервера, і, таким чином, забезпечити правильну відповідність загальнодоступних і локальних IP-адрес. Однак STUN функціонує не у всіх випадках: якщо брандмауер використовує так зване симетричне перетворення NAT, то кінцевий пристрій стає досяжним через Internet тільки з сервера STUN, а пакети іншого походження, наприклад від IP-телефонів, не пропускаються. STUN працює в багатьох середовищах, проте успішне застосування цього протоколу, на жаль, залишається справою випадку.

Новий інфраструктурний компонент для операторських мереж, який вирішує проблему симетричної трансляції NAT, називається прикордонним контролером сеансів (Session Border Controller, SBC). Спочатку він був оцінений IETF як «невдалий», проте пізніше стало зрозуміло, що без нього, на жаль, не обійтися. Завдяки SBC переважна більшість абонентів IP-телефонії можуть користуватися своїм IP-телефоном без необхідності внесення будь-яких змін до маршрутизатора

або кінцевого пристрою. Крім того, з його введенням вирішується і проблема фрагментації UDP, коли маршрутизатор не може коректно переправляти дуже великі пакети. Оскільки SBC не дає повної інформації про маршрутизації, пакети звичайно настільки малі, що труднощів не виникає. Для оператора така технологія привносить цікавий побічний ефект: коли клієнти не бачать інформації про маршрутизацію, вони не можуть напряму зв'язатися зі співрозмовником і обійти при цьому оператора і пов'язаний з цим біллінг.

Якість надання послуг

Коли мова йде про передачу голосу по IP в межах корпоративних мереж, належна якість послуг (Quality of Service, QoS) мається на увазі сама собою. Це твердження справедливо також стосовно різних пропозицій операторів і провайдерів для відповідних з'єднань через глобальну мережу. Інакше виглядає ситуація у випадку з офісами, де у користувачів також є бажання долучитися до IP-телефонії по недорогих з'єднаннях DSL. Локальний маршрутизатор DSL в стані сортувати вихідні пакети відповідно до QoS, однак зворотний напрямок контролює провайдер.

З досвіду Німеччини можна сказати, що ситуація в цій області залишає бажати кращого. Набагато частіше оператор надає пакетам TCP більш високий пріоритет, ніж UDP. На жаль, завантаження в більшості випадків відбувається по TCP, і тому вона може помітно заважати паралельним телефонним розмовам по IP. На даний момент існують два рішення цієї проблеми. Перше полягає у виборі провайдера, що пропонує QoS. При використанні SBC він здатний забезпечити правильне сортування пакетів, навіть якщо вхідні пакети VoIP не марковані бітами QoS. Друге, швидше прагматичне, рішення полягає в тому, щоб орендувати другий канал DSL і фізично розділити голос і дані. Цей варіант

функціонує дуже вдало і при комерційному використанні часто виправдовує себе економічно.

Безпека

Зі зростаючою привабливістю телефонії на базі IP виникають схожі проблеми, пов'язані з безпекою, як і в інших областях комунікацій по IP: мова йде про спам, хакерські атаки і спроби прослуховування. За аналогією зі «сміттєвою» поштою спостерігається справжня хвиля «бур'янистих» дзвінків: спам по IP-телефонії (Spam via Internet-Telephony, SPIT). Принцип простий, коли телефонні дзвінки безкоштовні, зловмисники можуть запустити з будь-якої частини Internet мільйони дзвінків, і ті, хто їх приймає, чують, що виграли, наприклад, подорож на південь Тихого океану. Цільові адреси отримати досить просто, випробувавши всі номери, що надаються провайдером його клієнтам.

Заходи протидії відомі по боротьбі з традиційним спамом. По-перше, оператори починають вести так звані «білі списки». Як правило, вони охоплюють адресний потенціал партнерів-операторів. У разі дзвінка з Internet від третьої сторони він відхиляється. По-друге, складаються і «чорні списки», які містять дані про клієнтів, що розсилають спам, що може відбуватися і автоматично, коли клієнт ініціює більше дзвінків, ніж в змозі це зробити.

Поряд з так званими атаками DoS (до них відноситься і SPIT) важливу роль відіграє захист приватної сфери, для чого використовуються методи, аналогічні тим, що специфіковані в HTTP. Аналогом HTTPS є SIPS, «захищений» стандарт SIP. Як і у випадку HTTPS, для ідентифікації учасників служать сертифікати, вони представляють базис для узгодження необхідного ключа. Відповідним чином SRTP є доповненням протоколу передачі даних в реальному часі (Real Time Transport Protocol, RTP), причому використовується шифрування AES з довжиною ключа 128 біт.

Обмін ключами відбувається за допомогою SIPS. На даний момент дискусія про коректне формулювання стандарту ще не закінчена, проте всі питання повинні бути вирішені у найближчі місяці, і за допомогою SIPS і SRTP буде можливим повноцінне шифрування переговорів.

SIP в офісі

SIP набув поширення насамперед у галузі кінцевих користувачів і при підключенні невеликих і домашніх офісів. Однак рішення VoIP для корпоративної області, де досі часто зустрічаються нестандартні технології, дають підстави вважати, що SIP і тут буде грати більш важливу роль. В області телекомунікаційних систем на базі SIP повідомлення про прогрес пов'язані не стільки з появою новинок в стандартизації, скільки з впровадженням існуючих стандартів. Вибір придатних для використання рішень помітно розширився, так само як і спектр пропозицій сумісних пристроїв. Все виразніше простежується тенденція, коли користувачеві телекомунікаційної системи не доводиться купувати всі компоненти в одного виробника. Поряд зі спеціалізованими компаніями великі гравці виходять з того, що вони не повинні більше випускати систему цілком. Якщо не трапиться непередбаченого, незабаром варіантів буде так само багато, як і в комп'ютерній галузі.

Література

1. Internet-телефония как двигатель SIP [Електронний ресурс] – Режим доступу до ресурсу: https://www.osp.ru/lan/2005/08/377136/
2. SIP-телефонія - це сучасна цифрова телефонія. [Електронний ресурс] – Режим доступу до ресурсу: https://pautina.ua/ua/telefon/sip-voip/
3. IP-телефония [Електронний ресурс] – Режим доступу до ресурсу: https://ru.wikipedia.org/wiki/IP-телефония