SIP 기반 VoIP 의 NAT Traversal 해결을 위한 ICE 의 적용

문병천, 김강석, 홍만표
아주대학교 대학원 지식정보공학과
e-mail : { munbc8308, kangskim, mphong }@ajou.ac.kr

Applying ICE to Solving NAT Traversal of SIP based VoIP

Byeongcheon Mun, Kangseok Kim, Manpyo Hong
Dept. of Knowledge Information Engineering, Graduate School of Ajou University

요 약

VoIP 서비스는 패킷 데이터 망을 기존의 전화망처럼 이용하기 위한 서비스이다. VoIP 에서 디바이스간 통화를 위해 SIP 프로토콜을 사용 한다. 현재 패킷 데이터 망을 이용하는 디바이스들이 많아지면서 IP 주소 부족 현상이 나타났다. 이 현상을 해결하기 위해 NAT 기술이 고안 되었고 NAT 는 패킷 헤더의 IP 주소를 변환하는 동작을 한다. 이러한 동작은 SIP 를 이용한 VoIP 서비스에서 NAT Traversal 을 일으키게 된다. NAT Traversal 은 NAT 가 패킷 헤더의 IP 주소만을 변경하기 때문에 SIP 처럼 어플리케이션 헤더의 IP 주소를 참고하는 프로토콜에서 목적지를 찾아가지 못하는 경우를 말한다. 이러한 문제를 해결하기 위한 기술들의 종류와 장단점을 살펴보고 NAT Traversal 에 효과적인 기술인 ICE 를 VoIP 서비스에 적용 하고 중복된 과정을 최소화한 개선된 호 설정 과정을 제안한다.

1. 서론

VoIP(Voice over Internet Protocol)은 회선교환 기술을 이용해 음성 데이터를 전송하는 방식과 다르게 음성 데이터를 데이터 망을 이용해 패킷 형태로 변환하여 패킷교환 방식으로 전달하는 IP 전화 기술을 말한다[1]. 기존의 전화망에 비해 넓은 확장성과 낮은 이용 요금을 강점으로 활발히 서비스 되고 있다. 이런 VoIP 기술을 사용해 디바이스끼리 통신하기 위해 호를 맺는 과정이 필요하다. 호를 맺기 위한 프로토콜은 SIP 가 있다. SIP 는 텍스트 기반의 프로토콜로서 넓은 확장성과 해석의 쉬움으로 멀티미디어 화상회의, 이동성 지원 서비스, 인스턴트 메시지 서비스, 전자 상거래, P2P 등 많은 분야에서 응용되고 있다.

현재의 패킷 데이터 망에 NAT(Network Address Translation) 기술은 필수 불가결한 존재이다. NAT 는 기존의 IPv4 주소지정 방법으로는 점점 수요가 많아지는 디바이스 들의 IP 주소를 충분히 제공할 수 없어서 개발된 기술이다[2]. 이런 주소 부족을 해결하기 위해 IPv6 역시 개발되었으나 현재 패킷 데이터 망에는 보편적으로 보급되지 않고 있다. 이런 NAT 기술은 사설 네트워크의 주소를 감춰주는 역할도 하고 있어 보안상의 이유로 사용되기도 한다. NAT 가 고안되었을 당시의 네트워크의 가장 기본적인 모델은 서버-클라이언트 모델이지만 VoIP 서비스는 디바이스간의 통신이 목적인 P2P 모델에 더 가깝다.

VoIP 서비스에서 디바이스간에 SIP 프로토콜을 사용하여 호를 맺게 되는데 이런 SIP 처럼 텍스트 기반의 어플리캐이션 헤더를 사용하는 프로토콜은 NAT 장비로 인해 통신이 불가능한 경우가 있다. NAT 는 들어온 패킷 헤더의 IP 주소를 변하게 하는데 SIP 처럼 목적지 주소의 지정방식이 IP 패킷 헤더 부분과 메시지 내부의 Contact 필드 즉 어플리캐이션 헤더에서 이루어지게 되면 쌍방 간 메시지 교환에 문제가 발생하게 되어 통화를 위한 호 연결이 되지 않게 된다. 이러한 현상을 NAT Traversal 이라 한다[3].

NAT Traversal 의 해결을 위해서는 고도화된 NAT 장비를 사용하는 방법과 기존의 서버-클라이언트 모델을 적용한 STUN[4], TURN[5], ICE[6] 라는 해결방법이 고안되어 있다. 고도화된 NAT 장비를 사용한 해결 방법은 기존의 NAT 장비 전체를 교체해야 하는 부담이 있다. 그래서 서버-클라이언트 모델을 이용한 해결 방법이 주로 사용되고 있다. STUN 방식은 서버를 이용해 주소를 바인딩하고 TURN 방식은 서버에서 릴레이 주소를 할당하는 방법이다. ICE 는 이 두 방식을 NAT 의 종류에 따라 선택해서 적용하는 프레임워크이다. 본 논문에서는 NAT Traversal 과 이러한 현상을 해결하는 방법인 STUN, TURN, ICE 의 장단점을 2 장에서 알아 본다. 3 장에서는 VoIP 서비스에 ICE 를 적용하고 VoIP 와 ICE 의 호 설정 과정과 이 과정을 간소화하는 방법을 제안 한다. 결론 및 향후 연구 과제에 대해서는 4 장에서 기술 한다.

본 연구는 미래창조과학부 및 한국인터넷진흥원의 "고용계약형 지식정보보안 석사과정 지원사업"의 연구결과로 수행되었음 (과제번호 H2101-13-1001)

2. 관련 연구

2.1 SIP (Session Initiation Protocol)

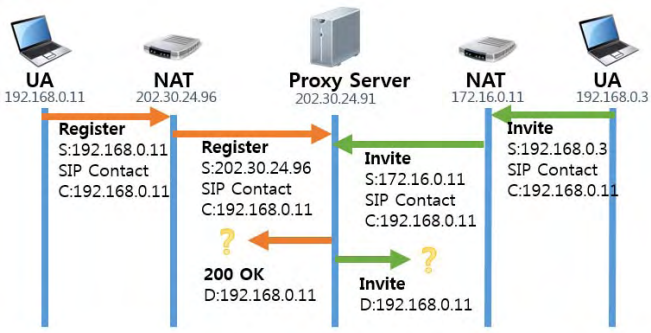
SIP 는 음성과 영상 등 멀티미디어 통신 세션을 생성, 삭제 변경 할 수 있는 시그널링 프로토콜로 IETF 에 의해 개발되었다. SIP 의 역할은 메시지 교환을 원하는 주체들 간에 메시지 세션을 제어하기 위한 정보를 교환 하는 것이다. SIP 는 통신을 위한 제어신호의 교환 역할 만을 한다[3].

2.2 NAT (Network Address Translator)

NAT 는 하나의 공인 IP 에 여러 사설 IP 를 할당 시켜주어 주소부족 문제를 해결하고 사설 IP 주소를 숨겨 보안목적으로도 사용 된다. NAT 는 Cone 과 Symmetric 두 가지 종류가 있다. Cone 과 Symmetric 의 차이는 도착지의 IP 주소가 주요한지 아닌지에 있다. 도착지에 상관없이 하나의 IP 주소에 매핑되면 Cone 방식이고 도착지 IP 주소가 다르면 다른 IP 주소로 매핑되는 것이 Symmetric 방식이다[2].

2.3 NAT Traversal

NAT Traversal 이란 SIP 처럼 어플리케이션 헤더를 사용하는 프로토콜이 NAT 를 거쳐 가면서 패킷 헤더의 IP 주소의 변화로 인해 정확한 목적지에 전달이 되지 않는 문제를 말한다. NAT 장비는 네트워크 3 계층과 4 계층의 패킷 헤더만을 인식 함으로 SIP 처럼 어플리케이션 헤더를 사용하는 프로토콜을 처리하는데 다음과 같은 문제가 발생한다. SIP 는 UA(User Agent) 간에 호를 맺기 위해 Invite Message 를 보낸다. 이때 응답 Message 를 수신할 목적지의 IP 주소를 SIP 내부의 Contact 필드와 IP 헤더에 기입하고 Proxy Server 는 이 IP 주소로 응답 한다. NAT 를 통과 하면서 패킷 헤더의 사설 IP 주소는 공인 IP 주소로 변한다. SIP 메시지가 NAT 를 통과 하면 Message 의 패킷 헤더에 있는 IP Source Address 는 변하지만 응답을 받기 위한 SIP 내부의 Contact 필드는 변하지 않는다.



(그림 1) NAT Traversal

사설 IP 주소를 가지고 있는 UA 는 Source Address 를 SIP 내부의 Contact 필드에 있는 주소로 전송 하므로 NAT 에 의해 바뀐 공인 IP 주소와 Source Address 가 달라지기 때문에 외부에서 들어오는 응답 Message 가 목적지를 찾아가지 못해 메시지를 수신할 수 없는 문제가 발생 한다(그림 1). 이러한 NAT Traversal 은 NAT 의 종류에 따라 다른 해결 방법을 가지게 된다[7][8].

2.4 STUN (Simple Traversal of UDP through NAT)

NAT Traversal 문제를 해결하기 위한 방법으로 STUN[4]이라는 기술이 고안되었다. 이 기술은 STUN 서버가 공인 IP 를 가지고 SIP 메시지를 중계 하는 방법으로 NAT Traversal 문제를 해결 한다[6]. 그러나 STUN 방식 만으로는 NAT 의 종류 중 하나인 Symmetric NAT 를 통과하지 못하는 단점을 가지고 있다[9].

2.5 TURN (Traversal Using Relay Nat)

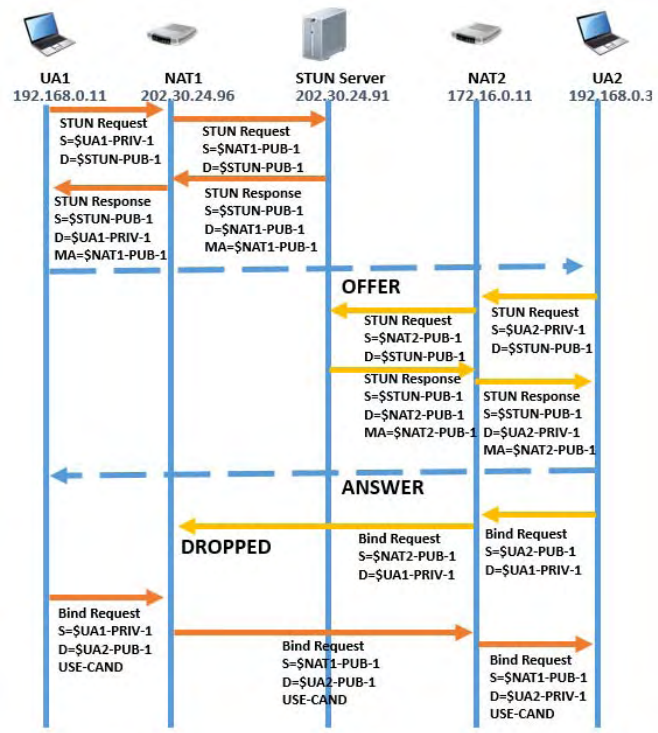
TURN[5]는 STUN 이 Symmetric NAT 를 통과 하지 못하는 문제를 해결하기 위해 고안되었다. 이 방식은 TURN Server 가 UA 와 Proxy Server 간의 주고 받는 모든 패킷들의 IP 주소 헤더 및 본문의 주소를 변경해 Relay 해 줌으로 NAT Traversal 을 해결 한다[7]. SIP 와 RTP 를 포함한 모든 패킷들이 TURN Server 를 거쳐 가기 때문에 통화 하는 UA 들이 많아질수록 TURN Server 의 부하가 커지게 된다[9].

2.6 ICE (Interactive Connectivity Establishment)

ICE[6]는 두 UA 가 서로 상대방과 통신하기 위한 최적의 경로를 찾을 수 있게 도와주는 프레임워크이며 STUN 과 TURN 의 조합으로 이루어진 기술이다. ICE 는 SIP 메시지 안에 다수의 IP 주소를 포함하도록 하여 UA 간 연결성을 확인한 후에 미디어를 전송하도록 한다.

UA 간 호를 맺을 시에 ICE 에서 NAT Traversal 을 어떻게 해결하는지는 (그림 2)의 과정과 같다. ICE 는 먼저 Network Topology 를 알기 위해 NAT 의 존재와 종류를 탐색하는데 이는 서버가 패킷을 릴레이 하기 위해 할당하는 IP 주소, NAT 의 공인 IP 주소, UA 의 사설 IP 주소를 비교하여 이루어 진다. 만약 UA 가 NAT 를 통과 한다면 위 3 개의 주소는 모두 다르겠지만, NAT 가 존재 하지 않는 다면 서버의 IP 주소와 UA 의 IP 주소는 동일할 것이다. 이렇게 NAT 의 존재를 확인한 후에 ICE 는 NAT 의 동작 방식에 따라 Cone 방식이라면 STUN 을 Symmetric 방식이라면 TURN 방식을 사용 하도록 결정한다. ICE 의 동작 방식이 결정 된 후 UA 는 서버에 자신의 주소를 알려주고 서버는 UA 의 사설 IP 와 NAT 에서 보여주는 공인 IP 주소를 알게 된다. UA 에서 호 설정을 요청하면 요청 받은 UA 에서 서버에 자신의 위치를 등록한다. 이렇게 각 UA 들의 주소와 NAT 의 유무 및 NAT 의 공인 IP 주소를 서버는 알고 있어 메시지를 정확하게 전송할 수 있게 된다. 이 과정을 통해 호를 맺은 후 RTP 를 이용한 멀티미디어 데이터를 주고 받는다[8].

ICE 는 각 NAT 의 종류 별로 전송 방법을 제공하기 때문에 처리 과정이 복잡하여 호 설정 시간이 길어지며 구현하기 어렵고 STUN 과 TURN 방식에 종속적인 단점을 가지고 있다[10].

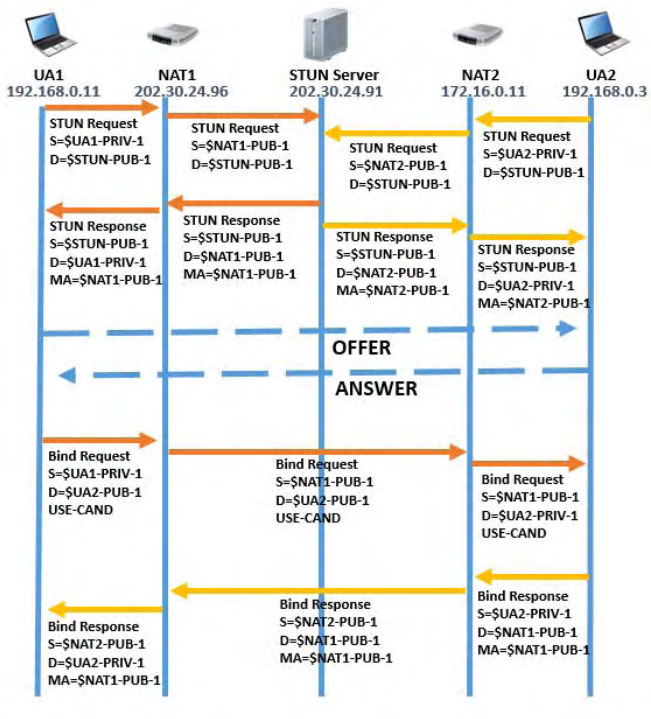


(그림 2) ICE(RFC5245)의 호 설정 단계

3. 제안 방식

현재 IPv4 주소 지정 방식에서 요구되는 IP 주소를 제공하기 위해 단기 정책으로 고안된 NAT 기술이 지만 현재 통신사에서 제공하는 패킷 데이터 망을 구성하기 위한 중요한 기술 이다. 하지만 SIP 프로토콜 기반의 VoIP 서비스 에서는 NAT Traversal 문제가 일어 날수 있음을 알아보았다. 본 논문에 제시된 STUN, TURN, ICE 이외에도 ALG[11], UPnP[12], SBC[13] 등등 NAT Traversal 문제를 해결하기 위한 많은 방법들이 제시되었지만 ALG 나 UPnP, PGP 같은 경우 현존하는 NAT 장비를 교체해야 하는 비용 부담이 존재 하며 SBC 역시 NAT 장비 마다 Controller 가 필요 함으로 추가적인 비용부담이 크다. 서버를 도입해 주소를 바인딩 하는 STUN 의 경우는 Symmetric NAT 에서 동작하지 못하는 문제가 있다. TURN 방식은 패킷을 재전송 처리해서 NAT Traversal 을 해결하지만 모든 패킷들의 IP 헤더와 어플리케이션 헤더를 서버에서 일일이 수정해야 함으로 호가 많아 질수록 서버의 부하가 많아진다.

STUN 과 TURN 모두 NAT Traversal 을 해결하기 위한 방법이지만 이 둘을 조합한 ICE 방식이 가장 효율적이며 확실한 해결 방법 이다. ICE 방식을 사용하게 되면 패킷의 Relay 가 필요하지 않은 구간에서는 STUN 방식을 사용하고 Relay 가 필요한 특수한 NAT 환경에서는 TURN 방식을 사용하여 좀 더 효율적으로 서버의 자원을 이용할 수 있게 된다. NAT 를 사용하는 현재 패킷 데이타 망에서 VoIP 서비스를 NAT Traversal 없이 사용하기 위해서는 ICE 의 도입을 제안한다. 하지만 ICE 방식은 Network Topology 를 알아내기 위해 걸리는 시간, 우선순위를 정하는 처리방식과 호 설정 과정이 복잡하기 때문에 VoIP 서비스만 사용 할 때 보다 통화의 대기 시간이 길어지게 된다 [9].



(그림 3) 제안한 호 설정 단계

현재 ICE 의 호 설정 단계는 UA A 가 STUN Server 에 STUN 요청 메시지를 보낸 후에 STUN Server 에서 응답을 받고 UA B 에 OFFER 를 보내면 UA B 는 STUN Server 에 자신을 할당하는 과정을 거친 후 UA A 에게 ANSWER 메시지를 보내게 된다. 그 후 UA B 는 A 에게 Bind 메시지를 보내지만 NAT 에 B 의 주소가 매핑 되어 있지 않음으로 버려지게 된다. 이때 UA A 에서도 B 로 Bind 메시지를 보내 B 가 Bind 응답메시지를 A 에게 보내게 되며 A 가 메시지를 받게 되면 호의 연결이 성립 되어 UA 간의 통신이 시작 된다(그림 2).

이런 ICE 의 호 설정 방식을 VoIP 서비스에 적용하게 되면 각 UA 는 총 두 번의 할당 과정을 거치게 된다. UA 가 VoIP 서버에 등록을 하면서 한번 할당 과정을 거치게 되고 UA 간에 호를 맺으면서 ICE 방식을 사용 하면서 한 번 더 할당 과정을 거치게 된다. 이런 중복된 할당 과정은 ICE 를 적용한 VoIP 서비스를 이용하면서 통화 대기 시간을 늘어 나게 하는 요소가 될 수 있다. 이를 해결 하기 위해 다음과 같은 방법을 제안 한다.

기존의 ICE 표준에서 제시한 호 설정 과정에서 UA 들의 할당 과정은 UA 의 요청이 있을 시에 시작하게 되어 있다. 할당의 목적은 서버에 UA 의 주소를 알려주어 정확한 주소로 메시지들을 주고 받기 위해서 이다. 하지만 이런 할당 과정은 VoIP 서비스에서는 Registrar 서버에 등록을 하며 진행 된다. 제안 하는

방법은 VoIP 의 과정 중 등록 과정에서 할당 과정을 한번만 거치게 하고 ICE 가 적용된 VoIP 에서는 해당 과정을 생략 시킨다. 서비스를 이용 하면서 할당 과정은 등록과정 중에 한번만 진행하고 그 후 과정은 ICE 표준에 따른다. 또한 ICE 표준에서는 ANSWER 메시지를 보낸 UA 에서 바로 Bind 메시지를 보내지만 이 메시지는 NAT 에 의해 버려질 가능성이 있다. 이 부분은 ANSWER 를 보낸 UA 가 요청을 보내지 않고 ANSWER 를 받은 UA 가 요청을 보내 NAT 로 인해 버려지는 메시지를 줄일 수 있다. 하지만 서버는 각각의 UA 에서 요청한 STUN Request 메시지를 동시에 처리하기 때문에 Response 를 보내기 까지 처리시간이 기존의 방법보다 조금 더 걸리게 됨을 예상 할 수 있다 (그림 3).

제안한 방법을 증명하기 위해 구성된 테스트 환경은 공인 IP 를 가진 서버와 NAT 내부의 UA 2 개로 구성된다. Proxy Server 및 ICE 는 오픈 소스인 Opensips[14]로 구현 하였고 UA 는 역시 오픈 소스인 Linphone[15]을 사용하였다. 기존의 방법으로 호 설정 단계를 진행 한다면 테스트 환경에서 UA 간에 보내는 SIP 메시지 하나당 평균 5ms 걸리게 된다. 전체 호 설정 과정에 SIP 메시지를 주고 받는 시간이 110ms 가 걸리게 되지만 제안된 방식은 그보다 적은 80ms 정도 소모된다고 할 수 있다<표 1>. STUN Request 와 Response 사이의 처리시간은 1ms 이하로 매우 작기 때문에 고려의 대상이 되지 않는다. 개선된 호 설정 과정을 사용하면 기존의 ICE 장비를 바꿀 필요가 없고 프로세스가 간소화됨으로 기존의 방식보다 빠른 처리를 할 수 있어 호 설정 시간을 줄일 수 있게 된다.

<표 1> RFC5245 와 제안 방식의 소모시간

	소모시간
RFC5245	22(SIP message) * 5ms = 110ms
제안 방식	16(SIP message) * 5ms = 80ms

4. 결론

본 논문은 NAT Traversal 과 NAT Traversal 을 해결하기 위한 방법으로 STUN, TURN, ICE 방식에 대하여 알아보았다. VoIP 서비스에서 사용하는 프로토콜의 특성과 네트워크의 NAT 환경으로 인한 NAT Traversal 이 나타남으로 ICE 의 적용을 제안하였다. 또한 ICE 표준에서 제시한 호 설정의 단계를 VoIP 서비스에 맞게 간소화해 보았다. 하나의 호에 대한 결과는 미비하지만 호가 많아질수록 과정의 복잡성에 의한 차이는 더 커질 것이다.

NAT 는 IP 부족 현상을 해결하기 단기 정책 이지만 보안성의 이유로 IPv6 가 보편화 되더라도 계속 쓰여질 기술이라고 본다. 이미 IPv6 를 위한 NAT 기술이 나와 있다. 또한 P2P 형태의 다양한 서비스들과 SIP 처럼 텍스트 기반의 확 장성이 좋은 프로토콜들이 늘어 나고 있어 NAT Traversal 에 관한 이슈들은 계속 생겨날 것이다.

향후 제안한 호 설정 과정을 구현하여 ICE 를 적용한 VoIP 서비스가 얼마나 효과적인지의 비교 분석과 NAT Traversal 해결에 관한 연구가 계속 필요 할 것이다.

참고문헌

[1] 이종화, 강신각, “인터넷 텔레포니(VoIP) 서비스의 설계 및 구현”, 한국통신학회, 2002

[2] K.Egevang, P. Francis, “The IP Network Address Translator(NAT)” RFC 1631, 1994

[3] J.Rosenberg, H. Schulzrinne, G. Camarillo, “SIP: session Initiation Protocol”, RFC3261, 2002

[4] J.Rosenberg, J.Weinberger, C. Huitema, “STUN – Simple Traversal of User Datagram Protocol Through Network Address Translator”, RFC 3489, 2003

[5] R. Mahy, “TURN – Traversal Using Relay around NAT”, RFC 5766, 2010

[6] J.Rosenberg, “Interactive Connectivity Establishment (ICE) : A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols”, RFC 5245, 2010

[7] 최경호, “VoIP Firewall/NAT Traversal 문제 해결을 위한 구조”, 한국정보과학회, 2007

[8] Yevgeniy Yeryomin, “Solving the Firewall and NAT Traversal Issues for SIP-based VoIP”, Telecommunications ICT, 2008

[9] 배기문, “NAT 환경에서 SIP 를 사용 할 때의 문제와 S-P Server 를 사용한 개선된 해결책”, 성균관대학교, 2012

[10] 한석준, “IMS 에서 효율적인 NAT Traversal 해결 시나리오” 한국산학기술학회, 2013

[11] P. Srisuresh, “DNS extensions to Network Address Translators (DNS_ALG), RFC 2694, 1999

[12] “UPnP Device Architecture”, ISO/IEC 29341-1:2011

[13] G. Camarillo, “Functionality of Existing Session Border Controller (SBC)”, IETF Draft, 2005

[14] OPENSIPS, “http://www.opensips.org”

[15] LINPHONE, “http://www.linphone.org”