SIP 사용자 에이전트의 NAT 통과

한재천* · 강신각

한국전자통신연구원

NAT Traversal of SIP User Agent

Jae-Cheon Han* · Shin-Gak Kang

Electronics and Telecommunications Research Institute

E-mail : { jupiter* , sgkang } @etri.re.kr

요 약

최근 들어 인터넷 사용자가 급증함에 따라 IPv4 주소의 고갈 문제가 대두되었고, 이를 해결하기 위하여 네트워크 주소 변환 기술이 주로 사용되고 있다. 네트워크 주소 변환 기술은 IP 계층에서 주소 변환을 통하여 제한된 IP 주소 자원을 공유해 사용할 수 있는 기술이지만 응용 계층에서 IP 주소를 직접 사용할 경우 문제가 발생하게 된다.

SIP 프로토콜은 다른 프로토콜들에 비하여 구현이 용이하고, 다양한 애플리케이션을 쉽게 개발할 수 있는 장점들을 가지고 있어 차세대 네트워크에서 호 연결을 위한 사실상의 표준으로 자리 잡아 가고 있다. SIP 프로토콜을 메시지 라우팅을 위하여 IP 주소를 직접 사용하기 때문에 IP 주소를 응용계층에서 사용할 경우 발생하는 문제를 그대로 안고 있다. 본 논문에서는 SIP 사용자 에이전트가 NAT 환경에서 동작할 때 발생하는 문제점에 대하여 알아보고, NAT 통과를 위해 제시된 표준 기술들에 대하여 알아보고자 한다.

키워드

RFC3261, SIP, VoIP, NAT Traversal,UPnP,IGD,STUN,TURN,ICE

I. 서 론

초기 인터넷은 단순히 텍스트 문서 또는 이메일을 전송하기 위하여 구축되었으며, 일부의 사람들만이 인터넷을 사용하였다. 최근 들어 인터넷 사용자가 급증함에 따라 IPv4 주소의 고갈 문제가 대두되었고, 이를 해결하기 위하여 네트워크 주소 변환 기술이 주로 사용되고 있다. 네트워크 주소 변환 기술은 IP 계층에서 주소 변환을 통하여 제한된 IP 주소 자원을 공유해 사용할 수 있는 기술이지만 응용 계층에서 IP 주소를 직접 사용할 경우 문제가 발생하게 된다.

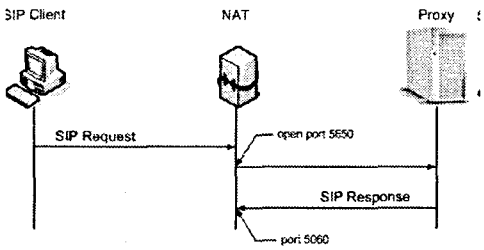
최근 들어 인터넷을 활용하는 다양한 서비스들이 개발되고 있다. 이러한 서비스 중 인터넷 전화 서비스는 가장 주목받는 서비스 중의 하나일 것이다. 인터넷 전화서비스를 위한 프로토콜로서 H.323, MGCP, SIP 등 다양한 프로토콜이 있다. SIP 프로토콜은 다른 프로토콜에 비하여 구현이 용이하고, 다양한 애플리케이션을 쉽게 개발할 수 있는 장점들을 가지고 있어 차세대 네트워크에서 호 연결을 위한 사실상의 표준으로 자리 잡아 가고 있다. SIP 프로토콜을 메시지 라우팅을 위하여 IP 주소를 직접 사용하기 때문에 IP 주소를 응용계층에서 사용할 경우 발생하는 문제를 그대로 안고 있다[2]. 본 논문에서는 SIP 사용자 에이전트가 NAT 환경에서 동작할 때 발생하는 문제점과 이를 해결할 수 있는 방법에 대하여 알아보고자 한다. 2장에서는 SIP 사용자 에이전트가 NAT 환경에서 갖는 문제점에 대하여 설명하고, 3장에서는 이러한 문제점을 극복하기 위하여 제시되고 있는 표준 기술에 대하여 설명한다. 결론 및 향후 연구 과제에 대해서는 4장에서 기술한다.

II. NAT 환경에서의 문제점

SIP 응답 메시지 통과 문제

기본적으로 SIP 클라이언트는 SIP 요청 메시지를 전송할 때 SIP 응답 메시지를 수신할 수 있는 주소를 Via 헤더에 기입하고, SIP 서버는 이 주소를 사용하여 SIP 응답 메시지를 전송해야 한다. 그러나 NAT가 SIP 메시지 전송을 위해 생성하는 핀홀은 SIP 요청 메시지의 Via 헤더에 기술되어 있는 주소와는 다를 수밖에 없기 때문에 SIP 응답 메시지가 NAT를 통과하는데 문제가 발생하게

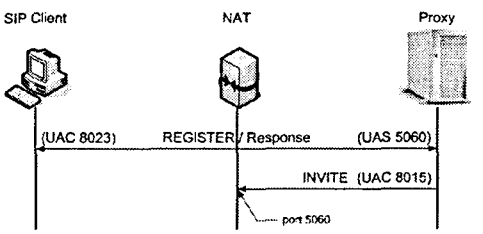
된다. <그림 1>은 NAT 환경에서 SIP 클라이언트가 동작할 때 발생하는 SIP 응답 메시지 통과 문제를 보여준다.



<그림 1> SIP 응답 메시지 통과 문제

SIP 요청 메시지 통과 문제

NAT 환경에서 동작하는 SIP 사용자 에이전트가 자신의 사설 IP 주소와 메시지 수신을 위한 포트 번호를 사용하여 접촉 주소(Contact Addresss)를 등록할 경우, 외부에서 전송하는 요청 메시지를 수신할 수 없는 문제가 발생한다. 이는 프락시 서버가 사설 IP를 이용하여 요청 메시지를 경로 배정할 수 없기 때문이다.



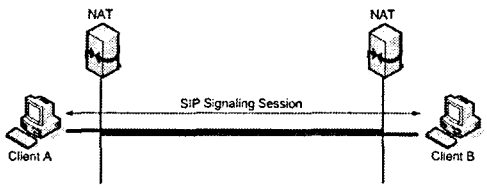
<그림 2> SIP 요청 메시지 통과 문제

프락시 서버가 maddr 옵션을 사용하여 IP 패킷에서 IP 주소를 추출해 저장할 경우에는 NAT로의 라우팅이 가능하지만 IP 응답 메시지 통과 문제에서와 마찬가지로 NAT가 생성하는 핀홀의 포트 번호가 SIP 사용자 에이전트가 메시지를 수신하는 포트와 다르기 때문에 메시지의 경로 배정이 정상적으로 이루어지지 않는다. <그림 2>는 SIP 요청 메시지 통과 문제에 대한 예를 보여준다.

미디어 통과 문제

일반적인 NAT는 NAT 외부에서 데이터 전송을 시작하게 될 경우, 데이터 전달에 필요한 핀홀 정보가 없기 때문에 데이터 전송 자체가 불가능하다.

인터넷 전화와 같이 RTP 프로토콜을 사용하여 미디어를 송수신해야 하는 어플리케이션에서는 일반적으로 미디어 송신을 위한 포트와 미디어 수신을 위한 포트를 별도로 사용하게 된다. 따라서 NAT 외부에서 NAT 안쪽으로 미디어를 전송해야만 하는데, 위에서 설명한 바와 같이 NAT가 갖는 문제점 때문에 미디어 전송이 불가능하다. 미디어 수신을 위한 포트와 미디어 송신을 위한 포트를 동일하게 사용할 경우에는 NAT의 구현 방식에 따라 미디어 송수신이 모두 가능한 경우도 있다.

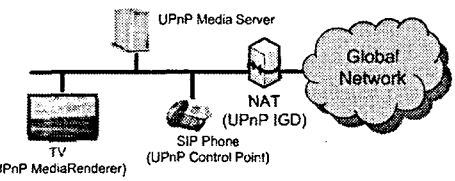


<그림 3> 미디어 통과 문제

III. NAT 통과 표준 기술

UPnP IGD 기술

UPnP(Universal Plug and Play) 기술은 피씨의 하드웨어 장치를 손쉽게 확장하기 위해 개발된 PnP(Plug and Play) 기술을 네트워크로 확장한 기술로서 가정 내에서 PC와 지능형 장치 또는 기기를 피어-투-피어 방식의 네트워크로 연결하기 위해 Microsoft, Intel, Sony 등의 회사가 주도로 개발한 아키텍처이다.

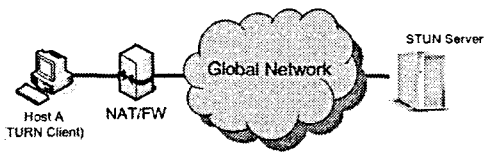


<그림 4> UPnP IGD를 이용한 NAT 통과

UPnP IGD(Internet Gateway Device)는 UPnP 장치 중의 하나로서 공용 IP 주소제공, 포트 예약 등 SIP 사용자 에이전트에서 NAT를 능동적으로 통과하기 위해 필요한 기능을 제공한다. UPnP IGD의 기능을 활용한 NAT 통과 방법은 실제 SIP 메시지를 수신 할 수 있는IP 정보를 SIP 메시지 구성에 사용하기 때문에 STUN이나 TURN 등과 같은 방식에 비하여 NAT 타입에 따라 NAT를 통과하지 못하는 경우는 존재하지 않으며, 보안을 위하여 S/MIME 등의 기술을 적용하여도 문제가 없다는 장점이 있다. 그러나 NAT가 UPnP IGD를 지원하는 경우에만 사용할 수 있다는 단점이 있다.

S T U N

STUN(Simple Traversal of UDP Through NATs) 프로토콜은 IP 어플리케이션이 자신과 공인망(Public Internet) 사이에 NAT 또는 방화벽이 존재하는지 검사할 수 있는 절차를 정의한 프로토콜이다[2]. 또한, 검사 과정에서 NAT 또는 방화벽에 생성한 핀홀 정보를 알아내는 것이 가능하다. SIP 사용자 에이전트는 검사를 통해 알아낸 핀홀 정보를 사용하여 NAT를 통과하여 통신하는 것이 가능하다.

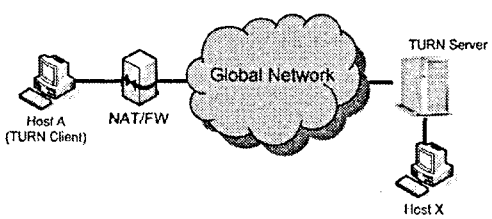


<그림 5> STUN

STUN 프로토콜에서는 NAT의 동작 특성에 따라 NAT를 *Full Cone, Restricted Cone, Port* Restricted Cone, Symmetric Cone 방식으로 구분하고 있으며, 이 NAT 분류 방법은 매우 폭넓게 사용되고 있다.

T U R N

Full Cone 방식의 NAT의 경우에는 STUN을 이용하여 NAT 통과가 매우 수월하게 이루어지며, Restricted Cone 방식의 경우에는 IP 어플리케이션의 구현 방법에 따라 NAT 통과가 불가능할 수도 있다. 그러나 Port Restricted Cone 방식의 경우에는 STUN 만으로는 NAT 통과가 불가능하다. 이러한 문제점을 해결하기 위해 제안된 방법이 TURN(Traversal Using Relay NAT) 프로토콜이다. TURN 프로토콜은 공인망에 데이터를 릴레이해 주는 서버를 두고, 항상 이 서버를 경유하여 통신하게 된다[3]. 이 방식은 어떠한 NAT 환경에서라도 통신이 가능하다는 장점이 있으나 TURN 서버에 걸리는 부하가 크며, 네트워크 대역폭을 많이 소비하는 단점이 있다.



<그림 6> TURN

I C E

STUN 프로토콜은 모든 종류의 NAT를 통과할 수 없다는 문제점이 있으며, TURN 프로토콜은 과도한 오버헤드가 발생하는 문제점을 안고 있다. 이러한 문제점을 해결하기 위하여 제시된 방법이 ICE(Interactive Connectivity Establishment) 기술이다[4].

ICE 프로토콜은 STUN, TURN 등과 같이 이미 개발되었거나 개발되고 있는 프로토콜을 사용하며, 여러 NAT 통과 방법 중에서 NAT의 특성에 따라 최적의 NAT 통과 방법을 찾는 프로토콜이다.

IV. 결 론

지금까지 SIP 사용자 에이전트가 NAT 환경에서 동작할 때 발생하는 문제점들에 대하여 살펴보았으며, NAT 통과 문제를 해결하기 위하여 제시된 대표적인 표준 기술들에 대하여 알아보았다. 이 밖에도 NAT를 통과하기 위한 방법으로 Symmectric Response 기술, Connection 재사용 기술 등 다양한 방법들이 제안되고 있다. NAT의 완벽한 통과를 위해서는 특정 기술 하나만으로는 불가능하며, 어플리케이션의 특성에 따라 다수의 NAT 통과 기술을 접목해야 함을 마지막으로 본 논문을 마치고자 한다.

참고문헌

[1] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler. "SIP: session initiation protocol" IETF RFC 3261, June 2002

[2] Rosenberg, J., Huitema, C., Mahy, R. and J. Weinberger, "STUN - Simple Traversal of UDP Through Network Address Translators", RFC 3489, March 2003.

[3] Rosenberg, J., R. Mahy, and C. Huitema, "Traversal Using Relay NAT (TURN)", draft-rosenberg-midcom-turn-07 (work in progress), February 21, 2005.

[4] Rosenberg, J., "Interactive Connectivity Establishment (ICE): A Methodology for Network Address Translator (NAT) Traversal for the Session Initiation Protocol (SIP)", draft-ietf-mmusic-ice-04 (work in progress), February 16, 2004.