

IMS에서 효율적인 NAT Traversal 해결 시나리오

한석준^{1*}, 이재오¹, 강승찬¹
¹한국기술교육대학교 전기전자통신공학과

The Efficient Scenario of Solving NAT Traversal in the IMS

Seok-Jun Han^{1*}, Jae-Oh Lee¹ and Seung-Chan Kang¹

¹Department of Electrical, Electronic and Communication Engineering,
Korea University of Technology and Education

요 약 IP 주소 공간의 부족 문제를 해결하기 위해 NAT(Network Address Translation) 기술을 활용할 수 있다. NAT의 주소 변환 테이블에 없는 바인딩과 관련된 패킷을 제거하는 필터링 특성 때문에 NAT Traversal 문제가 발생한다. 이러한 문제를 해결하기 위해 추가적인 장비를 활용한 여러 가지 방법들이 제시되었다. 최근의 네트워크 시장은 유선과 무선이 통합되는 형태로 발전하고 있으며, 이를 효과적으로 제어하기 위하여 IMS(IP Multimedia Subsystem)라는 유무선 통합 제어 망이 등장하였다. IMS에서 IBCF(Interconnection Border Control Function)와 IBGF(Interconnection Border Gateway Function)라는 추가적인 장비를 이용하여 NAT Traversal 문제를 해결하고 있다. 본 논문에서는 P-CSCF(Proxy-Call Session Control Function)를 활용하여 추가적인 장비를 사용하지 않고 NAT Traversal 문제를 해결하는 방안을 제안한다.

Abstract We can use NAT(Network Address Translation) technology to solve the lack of IP address. The problem of NAT traversal is happened when the filtering characteristics of NAT remove the packet that has no binding in the address translation table of NAT. There were many kinds of way to solve these problems by using additional device. Lately, network market is changed into integrating wired and wireless network by the IMS(IP Multimedia Subsystem). The IMS integrates to control network of wired and wireless network, has emerged to control convergence network effectively. Lately, the additional devices like IBCF(Interconnection Border Control Function) and IBGF(Interconnection Border Gateway Function) are used to solve the NAT traversal problem in the IMS. In this paper, we propose the solution of NAT traversal using P-CSCF without any additional equipment in the IMS.

Key Words : NAT, NAT Traversal, IMS, P-CSCF

1. 서론

IP 기반에서 사용되는 장비들이 급속도로 증가함에 따라 IP 주소 공간의 부족현상이 발생한다. 이를 해결하기 위한 방안으로 NAT를 활용하는 방법이 제시되고 있다. All-IP 기반의 IMS 망에서 모든 장비들이 IP를 사용하기 때문에 IP 주소의 부족 문제는 더욱 큰 문제가 될 수 있어 NAT 장비의 도입이 더욱 필요하다.

IMS는 IP 프로토콜을 기반으로 멀티미디어 서비스를

제공하기 위한 프레임워크로, 범용의 인터넷 기반 기술을 사용하여 신속한 서비스 개발 및 변경이 용이하다는 장점을 가지며, SIP(Session Initiation Protocol)를 이용한 효율적인 세션 관리 기능을 기반으로 다양한 3rd Party 애플리케이션과 쉽게 연동을 할 수 있다[1].

SIP를 이용한 RTP(Real-time Transport Protocol) 패킷 전송 시 SDP(Session Description Protocol)의 연결 정보인 "c" 파라미터의 사용자 IP 주소와 NAT장비를 통과한 패킷의 Source IP의 차이로 RTP 패킷이 전송될 수 없는

*Corresponding Author : Seok-Jun Han(Korea University of Technology and Education)

Tel: +82-10-3076-6393 email: sjhan@koreatech.ac.kr

Received September 25, 2012

Revised (1st October 31, 2012, 2nd November 06, 2012)

Accepted April 11, 2013

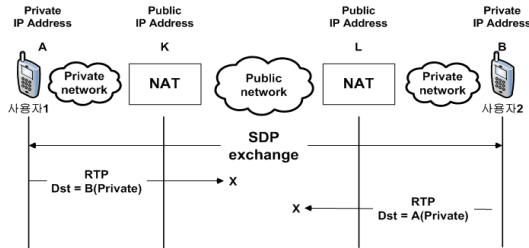
NAT Traversal 문제가 발생한다[2,3].

대부분 NAT Traversal 문제의 해결을 위해 추가적인 서버 등의 장비를 사용하여 상황에 따라 문제를 해결하는 한계를 가지고 있어, 본 논문에서는 IMS망에 별도의 추가적인 서버 등의 장비를 사용하지 않고 P-CSCF의 기능을 보강하여 NAT Traversal 문제를 해결하는 방안에 대한 알고리즘 및 시나리오를 제안한다.

2장에서 관련연구인 기존의 해결방안에 대해 고찰하고, 3장에서 P-CSCF를 이용한 문제해결 알고리즘 및 시나리오를 제안하고, 4장에서 기존 시스템과 비교를 한 후, 5장에서 결론과 향후과제를 제시한다.

2. 관련 연구

NAT Traversal 문제란, NAT내의 사실 주소가 외부의 공인 망에서는 보이지 않아 응답패킷이 사설망 내의 사용자로 도달하지 못하는 문제이다. 아래의 Fig. 1은 미디어 전송에 있어서의 NAT Traversal 문제 발생 시나리오이다.



[Fig. 1] NAT Traversal occurrence scenario

Fig. 1에서 사용자1은 세션 과정을 거쳐 RTP 전송을 위한 미디어 세션을 설립한다. RTP는 SDP의 IP 정보를 기반으로 세션을 열기 때문에 사용자1의 IP 주소인 A를 가리키고 있지만, 사용자1의 실제주소는 NAT 내부의 사설 주소이므로 외부에서 사용자1에게 패킷을 전송할 수 없는 NAT Traversal 문제가 발생한다.

NAT Traversal 문제의 해결방안으로 STUN, TURN, ICE, Media Relay 방식 등이 있다.

2.1 STUN(Session Traversal Utilities for NAT)

STUN은 대화형 IP 통신을 위한 NAT Traversal의 문제 해결을 위해 별도의 서버를 사용하는 방식이다. 사설망 내부의 사용자는 세션 설정을 위해 공중망의 STUN 서버에게 query 메시지를 보내고, STUN 서버는 NAT의

공인 IP 주소와 포트 정보를 사용자에게 알려준다. STUN 서버가 제공한 공인 IP 주소와 포트는 세션 성립단계에서 사용된다.

STUN 서버는 시그널링과 실제 미디어 스트림의 전송 경로에 존재하지 않아, Symmetric NAT 환경에서는 동작하지 못하는 문제점이 있다[4].

2.2 TURN(Traversal Using Relay NAT)

TURN은 종단간 미디어 전송을 위해 미디어 중계 서버를 사용하여 NAT 통과기술을 제공하는 방식으로 STUN과 마찬가지로 미디어 릴레이 서버 역할을 하는 별도의 서버를 이용한다. TURN 서버는 시그널링과 미디어 스트림 전송되는 경로에 존재하여 사설망으로 전해지는 모든 메시지는 TURN 서버를 경유하게 된다. 모든 메시지의 Source IP는 TURN 서버의 IP가 되고 미리 생성되어 있던 Symmetric NAT의 Pinhole을 통과할 수 있게 된다.

사용자가 증가하면 TURN 서버에 무리한 트래픽이 집중되어 지연이 발생하는 단점이 존재한다[5].

2.3 ICE(Interactive Connectivity Establishment)

ICE는 NAT Traversal 문제해결을 위해 P2P, STUN, TURN 중 가장 좋은 방법을 선택하여 미디어를 전송하는 방식으로, 각 방식을 적용하여 미디어 전송을 시도한 후 가장 효율적인 방법을 이용해서 패킷을 전송한다.

ICE 방식은 대부분의 상황에서 NAT Traversal 문제를 해결할 수 있는 방법이지만, 시스템의 구성과 구현이 복잡하고 STUN 방식이나 TURN 방식에 종속적인 단점을 가진다[6].

2.4 Media Relay

Media Relay 방식은 SIP 세션 경로에 Proxy 서버를 통해 SDP 메시지를 수정 또는 변경하여 사용자가 Proxy 서버를 통해 목적지에 미디어 스트림을 전송함으로써 NAT Traversal 문제를 해결한다.

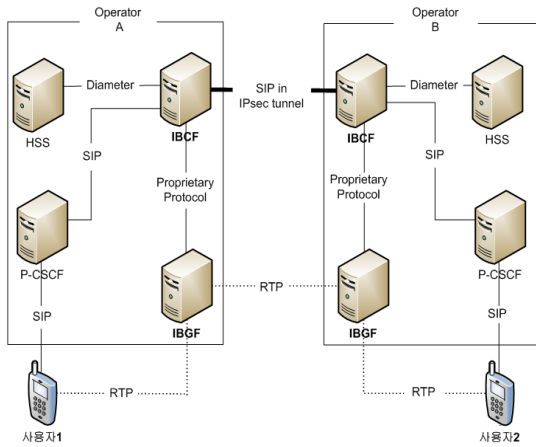
IMS에서는 IBCF와 IBGF를 통해 NAT Traversal 문제를 해결한다. IBCF는 세션의 설립과정에서 SDP 내의 IP 정보를 IBGF에게 알려주어, IBGF가 미디어 릴레이 서버로 동작하여 상대방에게 패킷을 전송하도록 한다.

Media Relay 방식은 NAT Traversal 문제를 해결하기 위해 기존의 문제 해결방식과 마찬가지로 별도의 서버를 사용해야 한다는 단점을 가지고 있다[7].

2.5 IMS 구조

All-IP 기반의 IMS 네트워크의 NAT Traversal 관련 기

본 구조를 Fig. 2에 나타내었다[8]. P-CSCF는 단말이 IMS 망에 접속하기 위한 최초 접속점 역할을 수행하며, IP할당, 권한 인증 등의 기능을 수행한다. HSS(Home Subscriber Server)는 사용자의 정보를 관리하는 역할을 수행하며, HSS는 보안기능이 뛰어난 Diameter 프로토콜을 사용하여 정보교환을 한다. IBCF는 Border Controller로서 IMS 망 사이의 연동을 위한 기능을 수행하고, IBGF는 IBCF로부터 수신한 SDP의 IP 정보를 이용해 미디어 중계 서버의 역할을 수행한다[9,10].

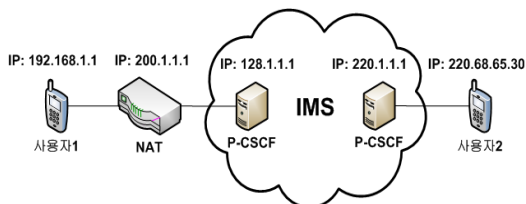


[Fig. 2] NAT Traversal solution using IBCF

3. NAT Traversal 해결방안

IMS 망에서 NAT Traversal 문제를 해결하기 위한 방법으로 별도의 서버를 사용하지 않고 P-CSCF의 기능을 보강하여 해당 문제를 해결하는 알고리즘과 시나리오를 제안한다.

3.1 문제 해결 알고리즘 및 시나리오



[Fig. 3] The structure of troubleshooting scenario

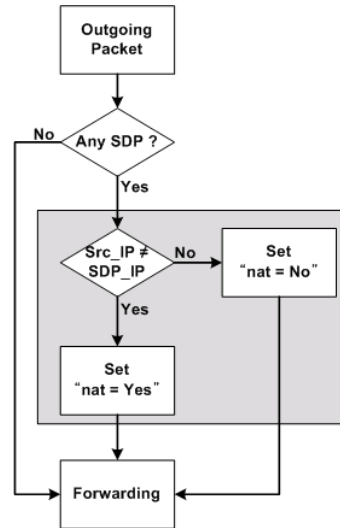
Fig. 3은 NAT Traversal이 발생하는 간단한 시나리오를 구체적으로 표현한 그림이다. 사용자1은 NAT 사설망

내의 사용자이고 사용자2는 공인 IP 주소 사용자라고 가정한다. 사용자들은 자신의 P-CSCF의 IP 주소를 알고, 사용자1은 사설 IP 주소 192.168.1.1를 갖고, 사용자2의 IP 주소는 공인 IP인 220.68.65.30이다. 이 외 NAT 장비의 IP 주소 100.1.1.1과 IMS 코어들의 주소들은 모두 공인 IP 주소이다. Fig. 3의 시나리오를 기반으로 NAT Traversal 문제 해결을 위한 P-CSCF의 패킷 처리 알고리즘과 시나리오를 제안한다.

3.1.1 P-CSCF 패킷 처리 알고리즘

NAT Traversal 문제를 해결하기 위한 P-CSCF의 패킷 처리 알고리즘은 Outgoing과 Incoming Packet 인 경우로 구분될 수 있다.

3.1.1.1 Outgoing Packet

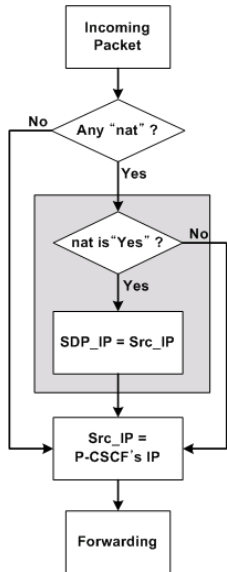


[Fig. 4] P-CSCF algorithm for outgoing packet

Fig. 4는 P-CSCF의 Outgoing Packet일 때 사용되는 알고리즘으로, 미디어 세션의 RTP 패킷은 SDP 부분에 정의된다. P-CSCF는 패킷이 도착하면 먼저 SDP 유무를 체크하여 SDP가 없으면 포워딩하고, SDP가 있다면 SDP의 연결 정보인 “c” 파라미터의 IP 정보와 패킷의 Source IP를 비교한다. 비교 결과가 같다면 NAT 장비가 없는 것이기 때문에 “nat = No”로 설정하고, 비교 결과가 다른 경우 “nat = Yes”로 설정해주고 포워딩한다.

NAT 장비의 유무에 따라 P-CSCF의 패킷에 대한 처리 방법이 달라지기 때문에 nat 파라미터를 설정함으로써, Incoming Packet을 처리하는 수신측 P-CSCF가 송신자의 NAT유무를 판단할 수 있다.

3.1.1.2 Incoming Packet



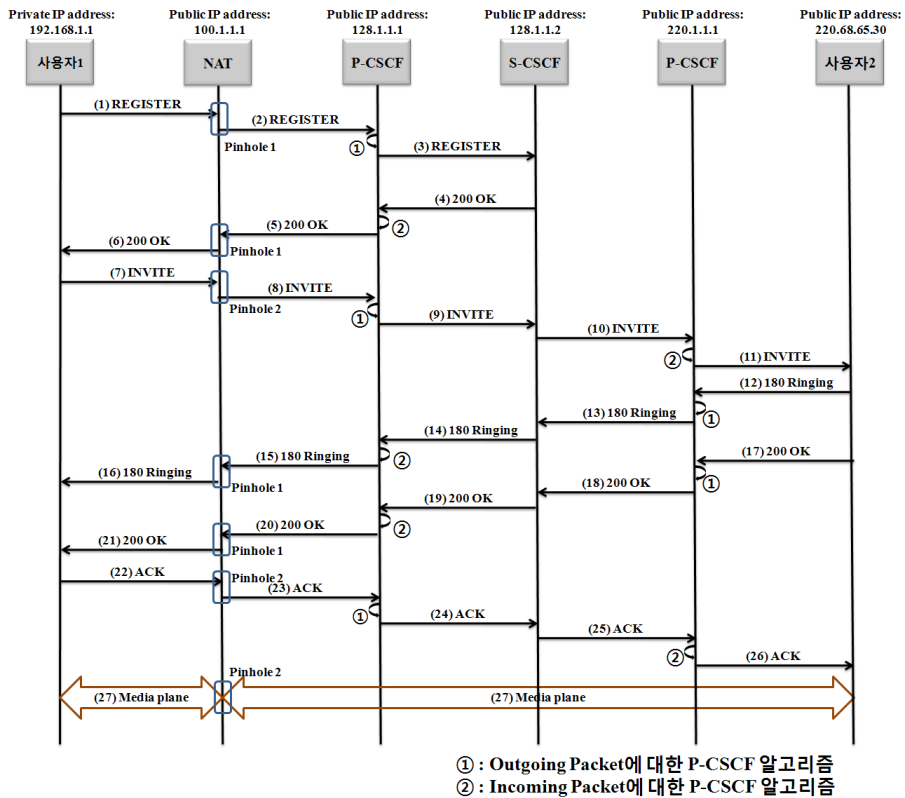
[Fig. 5] P-CSCF algorithm for incoming packet

Fig. 5는 P-CSCF에서 Incoming Packet일 경우 사용되는 알고리즘으로, P-CSCF에 Incoming Packet이 도착하면 “nat” 파라미터의 유무를 체크한다. “nat” 파라미터가 없다면 Source IP를 자신의 P-CSCF IP 주소로 바꾸어 레지스트레이션 과정에서 사용된 Pinhole을 통해 NAT 장비를 통과한다. “nat = Yes”의 경우 SDP의 IP 부분을 Source IP로 변경한다. 이렇게 하면 NAT 장비와 사용자 사이의 세션이 만들어지고, 미디어가 흐를 때 세션 과정에서 생성된 NAT의 Pinhole을 이용하여 미디어를 통과시킬 수 있다. 만약 “nat = No”이면 Source IP를 자신의 주소, 즉 P-CSCF의 IP 주소로 바꿔서 이전에 생성된 Pinhole을 통해 NAT장비를 통과한다.

3.1.2 문제 해결 시나리오

NAT Traversal 문제에 대한 해결 시나리오에 대한 메시지의 흐름을 Fig. 6에 나타내었다.

(1)REGISTER 메시지가 NAT에 도착하면 NAT는 사용자와 P-CSCF 사이의 “Pinhole 1”을 생성하고, (1)REGISTER 메시지의 Source IP 주소를 자신의 IP 주



[Fig. 6] Troubleshooting Scenario using P-CSCF

소 “100.1.1.1”로 변형한 후 포워딩 한다. “Pinhole 1”은 사용자1과 P-CSCF 사이를 연결하는 Pinhole 이므로, P-CSCF의 Incoming Packet에 대한 과정을 거친 패킷들은 모두 “Pinhole 1” 을 사용한다.

NAT 장비는 “Pinhole 1”을 생성 후 P-CSCF로 (2)REGISTER 메시지를 포워딩한다. P-CSCF는 Fig. 4에서 설명한 Outgoing Packet 알고리즘을 수행하여 IMS 망으로 (3)REGISTER 메시지를 포워딩한다.

IMS 망 내부의 등록 과정을 거쳐 등록이 완료되면 “(4)200 OK” 메시지가 사용자의 P-CSCF에 도착한다. “(4)200 OK” 메시지를 받은 P-CSCF는 Fig. 5에서 설명한 Incoming Packet 알고리즘에 따라, Source IP 주소를 자신의 IP 주소 “128.1.1.1”로 설정한 후 “(5)200 OK” 메시지를 NAT 장비로 포워딩한다. “(5)200 OK” 메시지의 경우 SDP가 없으므로 nat 파라미터가 존재하지 않기 때문에 패킷의 Source IP를 P-CSCF의 IP로 변경하고 “Pinhole 1”을 통해 NAT 장비를 통과한다.

등록 과정이 끝난 후에 사용자는 미디어 전송을 위한 SDP가 포함된 (7)INVITE 메시지를 사용자2에게 보낸다. 이 때 (7)INVITE 메시지의 Source IP 주소와 SDP의 IP 주소는 모두 “192.168.1.1”로 동일하지만, 사용자1의 NAT 장비를 거치면서 Source IP는 “100.1.1.1”로 바뀌게 된다. (8)INVITE 메시지의 SDP의 IP 주소와 Source IP 주소가 다르게 설정되고 NAT 장비에는 사용자1과 사용자2를 매핑하는 “Pinhole 2”가 생성된다. “Pinhole 2”는 NAT 장비와 사용자2 사이를 연결시켜주는 Pinhole로 두 사용자 사이의 미디어가 전송된다.

(8)INVITE 메시지를 받은 P-CSCF가 ①의 처리과정을 수행하면, (8)INVITE 메시지의 ‘nat’ 파라미터는 ‘Yes’로 설정되고, (10)INVITE 메시지가 사용자2의 P-CSCF에 도착하면 ②의 처리과정을 통해 SDP의 ‘c’파라미터 IP 주소가 사용자2의 P-CSCF의 IP 주소로 변경된다. (10)INVITE이 사용자2의 P-CSCF에 도착하면 P-CSCF는 ②의 처리과정을 통해 SDP의 ‘c’ 파라미터가 Source IP 주소인 “100.1.1.1”로 설정되고, Source IP 주소는 자신의 주소인 “220.1.1.1”로 바꾸고 된다. (11)INVITE 메시지가 사용자2에게 포워딩된다. 사용자2의 Ringing 메시지는 사용자1의 P-CSCF를 경유하면서 Source IP 주소가 “128.1.1.1”로 변형되어 “Pinhole 1”을 통과하게 된다. SIP의 “(17)200 OK” 메시지는 SDP를 가지고 있기 때문에 사용자2의 P-CSCF를 지나면서 “nat” 파라미터가 생성되고, 사용자2는 NAT 장비가 없으므로 “nat = No”로 설정된다. 수정된 “(19)200 OK” 메시지가 사용자1의 P-CSCF에 도착하면, ②의 처리 과정을 통해 패킷의 Source IP가 P-CSCF의 주소 “128.1.1.1”로 변경되어

“Pinhole 1”을 통해 사용자1에게 “(21)200 OK” 메시지가 도착하게 된다. “(22)ACK” 메시지의 경우, SDP가 없으므로 패킷의 변경 없이 사용자2의 P-CSCF로 전달되고, 사용자2의 P-CSCF에서 ①의 알고리즘에 따라 Source IP 주소만 “220.1.1.1”로 변형되어 사용자2에게 보내진다.

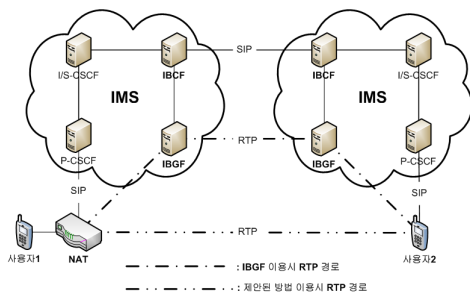
아래의 Table 1을 통해 Fig. 6의 시나리오가 적용되는 경우의 각 패킷들의 정보들을 나타내었다. Table 1의 ‘nat’는 P-CSCF가 NAT의 유무를 확인할 때 사용하는 파라미터 정보를 나타낸다. “SDP’s ‘c’ Parameter”는 SDP의 연결 정보인 ‘c’ 파라미터에 설정된 IP를 나타낸다.

[Table 1] Packet information of troubleshooting scenario

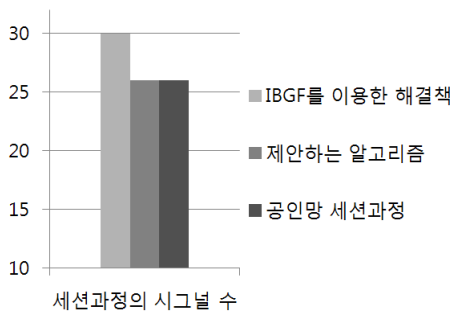
시그널 No.	Source IP address	Destination IP address	nat	SDP's 'c' Parameter
1	192.168.1.1	128.1.1.1	-	-
2	100.1.1.1	128.1.1.1	-	-
3	100.1.1.1	128.1.1.2	-	-
4	128.1.1.2	192.128.1.1	-	-
5	128.1.1.1	192.168.1.1	-	-
6	128.1.1.1	129.168.1.1	-	-
7	192.168.1.1	220.68.65.30	-	192.168.1.1
8	100.1.1.1	220.68.65.30	-	192.168.1.1
9	100.1.1.1	220.68.65.30	yes	192.168.1.1
10	100.1.1.1	220.68.65.30	yes	192.168.1.1
11	220.1.1.1	220.68.65.30	yes	100.1.1.1
12	220.68.65.30	192.168.1.1	-	-
13	220.68.65.30	192.168.1.1	-	-
14	220.68.65.30	192.168.1.1	-	-
15	128.1.1.1	192.168.1.1	-	-
16	128.1.1.1	192.168.1.1	-	-
17	220.68.65.30	192.168.1.1	-	220.68.65.30
18	220.68.65.30	192.168.1.1	no	220.68.65.30
19	220.68.65.30	192.168.1.1	no	220.68.65.30
20	128.1.1.1	192.168.1.1	no	220.68.65.30
21	128.1.1.1	192.168.1.1	no	220.68.65.30
22	192.168.1.1	220.68.65.30	-	-
23	100.1.1.1	220.68.65.30	-	-
24	100.1.1.1	220.68.65.30	-	-
25	220.1.1.1	220.68.65.30	-	-
26	220.1.1.1	220.68.65.30	-	-

4. 해결방안 비교

IMS에서 IBGF라는 미디어 중계 서버를 이용한 NAT Traversal 문제 해결 방안과 본 논문에서 제안하는 P-CSCF의 알고리즘을 이용한 해결방안에 대한 미디어 패킷의 전송 경로의 차이를 Fig. 7에 나타내고, SIP를 이용한 세션 처리 과정의 시그널 수의 비교를 Fig. 8에 나타내었다.



[Fig. 7] Comparison to the solution using IBCF



[Fig. 8] Signal comparison to the solution using IBCF

위의 Fig. 8의 IBCF를 이용한 해결책은 미디어 전송에 있어서 IBCF와 IBCF 사용하기 때문에 세션 과정에서 시그널이 증가하게 된다. 하지만 본 논문에서 제안하는 해결책은 P-CSCF의 패킷 처리 알고리즘만 추가 되므로 NAT를 이용하지 않는 일반적인 세션 과정의 시그널수와 동일하다. 즉, IBCF를 이용하는 IMS내의 해결책보다 시그널수가 줄어드는 것을 볼 수 있다.

본 논문에서는 기존의 미디어 중계 서버를 사용하는 방식을 사용하지 않고, 호 제어 및 세션 처리를 담당하는 P-CSCF를 이용할 수 있는 알고리즘을 제안하여 부가적인 서버를 사용하지 않고, 기존의 세션 과정의 시그널 수를 유지하면서 NAT Traversal 문제를 해결한다는 장점을 가지고 있다.

5. 결론 및 향후과제

IMS에서 NAT Traversal 문제를 해결하기 위해 별도의 추가적인 장비를 사용함에 따라 네트워크의 복잡성 증가 및 비용 증가 등의 문제점이 발생할 수 있다.

본 논문에서는 IMS 망에서 별도의 추가적인 장비를 사용하지 않고 NAT Traversal 문제를 해결하기 위한 P-CSCF의 알고리즘을 제안하고, 제안된 알고리즘을 적

용한 문제 해결 시나리오를 제시하였다.

제안한 알고리즘은 미디어 중계 서버와 같은 추가적인 장비가 불필요하기 때문에 네트워크가 단순화되고 시스템 구축 및 유지보수 비용이 줄어드는 경제적인 효과를 기대할 수 있을 것이다. 향후, P-CSCF의 기능 확장에 의한 지연 및 오버헤드에 대한 연구와 세션 설립 과정에서의 시그널 효율성에 관한 연구와 기존의 방식과의 전송 딜레이를 측정하여 비교 분석 할 것이다.

References

- [1] 3GPP TS 23.228, V10.0.0, "IP Multimedia Subsystem (IMS)," 2010.
- [2] Peterson, R. Sparks, M. Handlay and E. Schooler, "SIP: Session Initiation Protocol," RFC 3261, June 2006.
- [3] M. Handlay and V. Jacobson, "SDP: Session Description Protocol," RFC 2327, April 1998.
- [4] J. Rosenberg, J. Weinberger, C. Huitema, and R. Mahy, "STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)," IETF, RFC 3489, 2003.
- [5] J. Rosenberg, R. Mahy, C. Huitema, "Traversal Using Relay NAT (TURN)", IETF draft, October 2004.
- [6] Jonathan Rosenberg, "Interactive Connectivity Establishment: ICE", CISCO Fellow.
- [7] Matthaus wander, Sebastian holzapfel, Amo wacker, Torben weis, "NTALG-TCP NAT Traversal with Application-Level Gateway", The 9th IEEE CCNC, 2012.
DOI: <http://dx.doi.org/10.1109/CCNC.2012.6181044>
- [8] C. Boulon, Ed. J. Rosenberg, G. Camarillo, "Best Current Practices for NAT Traversal for SIP draft ietf-sipping-nat-scenarios-08," April-2008.
- [9] Annapurna agrawal, K.R. Prasanna kumar and G.Athithan, "SIP/RTP Session Analysis and Tracking for VoIP Logging", ICON 2008.
DOI: <http://dx.doi.org/10.1109/ICON.2008.4772653>
- [10] Tun-Shuai Yu, Ce-Kuen Shich, Wen-Shyang Hwang, Chien Chan Hsu, Che-Shiun, ji-Feng Chiu, "An efficient NAT Traversal for SIP and Its Associated Media sessions," Int Computer Symposium Dec. 2004.

한 석 준(Seok-Jun Han)

[정회원]



- 1996년 2월 : 한국기술교육대학교 정보통신공학과 졸업(공학사)
- 1999년 2월 : 고려대학교 전기전자전파공학부 졸업(공학석사)
- 2013년 2월 : 한국기술교육대학교 전기전자통신공학과 졸업(공학박사)

<관심분야>

IMS, QoS, NAT, 네트워크 관리, 인터넷워킹

이 재 오(Jae-Oh Lee)

[정회원]



- 1993년 2월 : 광운대학교 전산학과 졸업(공학박사)
- 1994년 3월 ~ 1995년 2월 : 코오롱 정보통신 연구소 과장
- 1995년 2월 ~ 2000년 12월 : KT 선임연구원
- 1999년 9월 ~ 2002년 8월 : (주) 웨어플러스 연구소장
- 2002년 8월 ~ 현재 : 한국기술교육대학교 전기전자통신공학과 교수

<관심분야>

네트워크 관리 및 IMS, 객체 지향 분산 처리기술, QoS 제어플랫폼, 개인화서비스, M2M, NAT

강 승 찬(Seung-Chan Kang)

[정회원]



- 1986년 2월 : 한양대학교 전자공학과 졸업(공학사)
- 1988년 2월 : 한양대학교 전자공학과 졸업(공학석사)
- 1993년 2월 : 한양대학교 전자공학과 졸업(공학박사)
- 1993년 3월 ~ 현재 : 한국기술교육대학교 전기전자통신공학과 교수

<관심분야>

네트워크 관리, QoS, 인터넷워킹, 멀티캐스트, 원격교육, 공학인증, e-learning, NAT