

NAT로 운영되는 private network에서 범용 IP 전화 시스템을 지원하기 위한 framework

최정현*, 이형수*, 최기무*, 강환중*

*LG 전자 디지털 네트워크 연구소 통신 s/w 실
e-mail : anna@lgic.co.kr

A Framework Supporting General IP Telephony System in NAT Based Private Network

Jeong-Hyun Choi*, Hyoung-Soo Lee*, Ki-Moo Choi*, Hwan-Jong Kang*
*Digital Network System Lab. LGE

요 약

NAT로 운영되는 private network에서 IP 전화 시스템을 지원하기 위해서는 caller 단말, gatekeeper 서버, callee 단말 간에 교환되는 H.225.0 메시지와 H.245 메시지의 NAT 주소 변환이 동적인 방법으로 투명하게 이루어져야 한다. 이를 위하여 본 논문에서는 NAT가 탑재된 라우터와 gatekeeper 서버를 연동하는 구조를 제안한다. 제안한 방식은 gatekeeper와 NAT 라우터 사이에 주소 변환을 위한 정보 교환용의 channel을 여는 단계, gatekeeper가 외부 단말로 향하는 H.225.0, H.245 메시지를 받았을 때 NAT 라우터에게 private 주소 정보를 알려주는 단계, NAT 라우터가 gatekeeper로부터 private 주소 정보를 받았을 때 public 주소 정보를 할당하여 gatekeeper에게 알려주는 단계, gatekeeper가 할당받은 public 주소 정보를 반영하여 외부 단말로 향하는 H.225.0, H.245 메시지를 재생성하는 단계 마지막으로 호가 종료될 때 gatekeeper가 NAT 라우터로부터 할당받은 NAT 자원을 반환하는 단계로 구성된다. 이러한 연동 구조를 사용함으로써 NAT 환경에서 H.323 개체들간의 signalling 메시지와 음성 데이터의 송수신을 보장할 수 있다.

1. 서론

인터넷의 사용이 급속히 확장됨에 따라 기존 IPv4 기반의 IP 주소 고갈 문제가 대두되었다. 이러한 IP 주소의 고갈에 대한 궁극적인 해결책은 IPv6를 도입하는 것이지만 이는 장기적인 해결책이고 모든 라우터가 IPv6로 migration하기 이전에 단기적인 해결책으로 NAT(Network Address Translation)가 제안되어 상용화되어 있다[1].

한편 ITU-T에서는 인터넷상에서 IP 전화 시스템을 지원하기 위하여 H.323 프로토콜을 제안하였다. H.323 프로토콜에서는 호를 설정하고 음성 데이터를 주고 받기 위하여 H.323 caller 단말, callee 단말과 gatekeeper 서버간에 단계별로 signalling 메시지를 교환해야 한다[2],[3],[4].

그런데 H.323에서는 각 단계의 signalling 메시지에 다음 signalling 단계에 필요한 IP 주소와 포트를 실어 보내기 때문에 필요한 주소와 포트 정보를 동적으로

설정할 수 있는 장점은 있으나, NAT로 운영되는 private network 망에서는 외부 단말과 통신을 하고자 할 때 라우터에서 다음에 사용될 주소와 포트를 알 수 없게 하는 단점을 가진다. 따라서 NAT로 운영되는 private network에서 IP 전화 시스템을 지원하기 위해서는 H.323에서 주고받는 각종 signalling 메시지의 NAT 주소 변환이 동적인 방법으로 투명하게 이루어질 수 있도록 NAT와 gatekeeper 서버를 연동하는 구조를 기술한다.

2. NAT와 IP Telephony

2.1 개요

NAT란 IP 패킷이 라우터를 통해서 포워드될 때 IP 주소를 변환하는 기능으로, private network 내에서는 private network 내에서만 구분되는 private 주소를 사용하고 public network으로 포워드되는 IP 패킷에 대해서

는 인터넷 상에서 유일한 public 주소로 변환한다. 라우터에서 IP 패킷의 주소 필드의 변환은 각 종단간에 투명하게 이루어지고 IP 프로토콜 및 상위 프로토콜들의 올바른 동작을 보장하기 위해서 주소 필드의 치환뿐만 아니라 주소의 변경으로 인한 IP/ICMP/TCP checksum 변경, TCP sequence/ acknowledge number 를 변경하는 등의 부가적인 처리가 필요하다.

NAT 는 public address 와 private address 의 변환 방식에 따라서 static NAT 와 dynamic NAT 로 나누어지고 dynamic NAT 는 사용하는 public address 를 하나로 사용하는지 복수의 public address 들을 pool 로 운영하는지에 따라서 NAT single mode (혹은 PAT: Port Address Translation, Masquerading)와 NAT global mode (혹은 normal dynamic NAT)로 분류된다.

Static NAT 는 public IP 주소 와 private IP 주소가 1:1 로 정적으로 할당되어 외부 단말이 송신한 패킷이 private network 으로 포워딩되면서 패킷의 public 목적지 주소가 정적 NAT 테이블에 따라 해당 private 주소로 변환되는 방식이다. Dynamic NAT 는 public 주소의 수가 private 주소의 수보다 적은 경우에 적용되는 방법으로, NAT global mode 는 내부 단말로부터 발생한 패킷이 public network 으로 포워딩되는 경우 private 주소가 기입되어 있는 패킷의 송신 주소를 대체할 public 주소를, 가용한 public 주소들 중에서 동적으로 할당하여 사용하는 방법이다. 이렇게 동적으로 할당된 public 주소는 해당 세션이 유지될 때까지 의미는 값이고 세션이 종료된 후에는 할당되었던 public 주소를 통해서 내부 단말을 access 할 수 없다. Dynamic NAT 를 사용할 때 외부 단말에서 먼저 내부 단말을 access 할 수 있게 하기 위해서는 해당 내부 단말을 위한 static NAT 엔트리(public 주소: private 주소)를 미리 생성해놓아야 한다. 따라서 private network 내에서 서버를 운영하기 위해서는 서버를 위한 public IP 를 private network 에서 사용하는 private IP 와 함께 미리 static NAT 엔트리로 설정해놓아야 한다. NAT single mode 는 변환용 public 주소를 하나만 사용하여 운용하는 방법으로 모든 private 주소가 하나의 public 주소로 변환되며 포트 번호를 이용하여 여러 개의 private 주소와 대응시킨다. 포트 번호의 할당은 dynamic 하게 이루어진다. NAT single mode 에서도 외부 단말에서 먼저 내부 단말을 access 할 수 있게 하기 위해서는 해당 내부 단말을 위한 static NAT 엔트리(tcp/udp 포트 번호: private 주소)를 미리 생성해놓아야 한다.

한편 ITU-T 에서 제안하는 통신 프로토콜인 H.323 은 Packet Based Network(PBN)에서의 새로운 전화 시스템으로 각광 받고 있다. H.323 프로토콜을 따르는 IP 전화 단말은 gatekeeper 가 있는 경우 반드시 gatekeeper 와 RAS signal 을 주고 받아야 하며, 터미널이 호를 생성하기 위해서는 RAS signalling 단계, Q.931 signalling 단계, H.245 signalling 단계, logical channel signalling 단계를 차례로 거쳐야 하며(그림 1), 각 단계에서 다음 단계에 사용할 주소와 port 를 알려주도록 되어있다[2]. 이러한 방식은 호 설정 과정에서 다음 단계로 넘어갈 때 필요한 주소를 dynamic 하게 설

정할 수 있는 장점은 있으나, NAT 로 운영되는 private network 망에서는 외부의 단말과 통신을 하고자 할 때 라우터에서 다음에 사용될 주소와 포트를 알 수 없게 하는 단점을 가지고 있다. 이 시스템에서 gatekeeper 는 기존 PBX 의 호처리 프로세스에 해당하는 역할을 수행하며, 사용자가 IP 주소를 모르더라도 전화 번호만으로 전화를 걸 수 있게 해준다. 시스템의 구성에 따라서 gatekeeper 없이 IP phone 이 직접 상대방의 IP 주소와 port 를 알아서 호를 설정하는 방법도 있으나, 이 경우 IP phone 의 사용자는 상대방의 IP 주소를 알아야 하며 전화 시스템의 종합적인 관리가 안되기 때문에 gatekeeper 를 이용하여 시스템을 구성하는 것이 일반적이다.

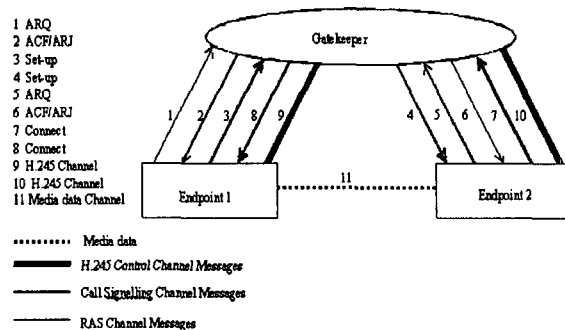


그림 1. H.323 signalling 절차

2.2 NAT 기반의 IP Telephony 시스템 동작설명

기존의 NAT 환경에서 IP 전화 단말과 gatekeeper 를 운영할 때 지원 가능한 유일한 경우는 NAT 내부 망에 caller 와 callee 단말이 모두 존재하는 경우이다. 내부망에서는 서로 유일한 private 주소로 통신하게 되므로, NAT 를 사용하지 않는 환경에서 모든 IP 전화 단말이 global IP 주소를 갖는 경우와 마찬가지로 문제가 발생하지 않는다.

H.323 단말이 사용하는 well known IP 와 포트는 gatekeeper UDP discovery multicast IP (224.0.1.41), gatekeeper UDP discovery 포트 (1718), gatekeeper UDP registration and status 포트 (1719), endpoint TCP call signalling 포트 (1720)이다. H.323 단말이 이미 gatekeeper 의 IP 주소를 알고 있다고 가정하면 단말은 gatekeeper discovery process 를 수행할 필요가 없다. Gatekeeper 에 등록된 두 H.323 단말이 RAS 와 Q.931 메시지를 사용하여 호를 설정하기 위한 과정은 그림 1 과 같은데 이 과정에서 반드시 필요한 well known 포트는 gatekeeper RAS (1719) 포트이다. Caller 단말은 gatekeeper 의 RAS well known 포트에 ARQ 를 송신하고 gatekeeper 로부터 ACF 를 수신하면 ACF 에 실린 Q.931 signalling 주소와 포트를 이용하여 Q.931 call signalling 절차를 시작한다. 이 때 ACF 에 실린 Q.931 주소에 따라서 call signalling 은 gatekeeper 를 통하는 경우와 callee 단말과 직접 통신하는 경우가 있다.

H.323 callee 단말은 Q.931 call signalling 이 끝날 때 Q.931 connect 메시지를 송신하고 이 메시지안에는 H.245 control channel 주소와 포트가 있어서 이후 caller 단말이 H.245 logical channel connection 절차를 개시할 때 해당 주소와 포트를 사용하도록 한다.

H.245 control channel 이 연결되면 H.245 logical channel signalling 과정을 거치면서 각 단말이 음성 데이터를 수신할 수 있는 주소와 포트를 상대방에 전달하게 된다. Caller 와 callee 단말은 해당 주소와 포트를 사용하여 상대방에게 RTP 음성 데이터를 전송한다.

2.3 기존 NAT 기반의 IP Telephony 시스템의 문제점

본 절에서는 NAT 기반의 private network 내에 gatekeeper 서버를 운영할 때, H.323 단말의 통신 과정에서 발생할 수 있는 문제점을 기술한다. 단말이 이미 gatekeeper 의 IP 주소를 안다고 가정할 경우, caller H.323 단말은 gatekeeper 의 RAS 포트를 알아야 한다. 이 때 RAS 메시지는 gatekeeper 와 H.323 단말간에만 사용하는 메시지이므로 gatekeeper 의 주소가 NAT static entry 로 설정되어있고 외부에 public IP 가 노출되어지면 signalling 에 문제가 없으며, Q.931 call signalling 도 gatekeeper 를 통해서 이루어진다면 문제가 없다. 그러나 Q.931 call signalling 을 gatekeeper 를 통하지 않고 종단간에 직접 송수신하고자 한다면 caller 단말의 NAT 내부 망에 있을 때는 문제가 되지 않으나 인터넷 상의 외부 단말에 존재한다면 NAT 내부 callee 단말을 global IP 로 직접 지칭할 수 없는 문제가 발생한다.

Gatekeeper 를 통한 Q.931 signalling 을 수행했다 하더라도 이후에 발생하는 H.245 signalling 시에 필요한 control channel address 및 port 를 Q.931 connect 메시지에 실어서 전달하게 되는데 이 과정에서 NAT 라우터는 새로 사용될 H.245 주소와 포트를 알 수 없게 된다. 만약 caller 단말이 NAT 내부망에 있다면 내부 caller 가 H.245 channel connection 을 시도하므로 별 문제가 없다. 그러나 caller 단말이 인터넷 상의 외부 단말이라면 H.245 channel connection 을 외부에서 시도하게 되므로 NAT 내부 callee 로의 연결은 실패하게 된다.

RTP channel 의 경우, H.245 control channel 이 연결된 후 H.245 의 logical channel signalling 과정을 거치면서 각 caller, callee 단말이 자신이 수신할 수 있는 주소와 포트를 상대방에게 전달함으로써 두개의 단방향 연결이 설정된다. 이 때 NAT 내부망의 단말이 수신할 주소와 포트를 인터넷상의 외부 단말에게 전달하게 되는데 이 경우에도 NAT 라우터는 새로 사용될 수신 주소와 포트를 알 수 없게 된다. 따라서 외부 단말이 송신하는 데이터는 내부 단말로 전송될 수 없게 된다. 이와 같은 과정은, 새롬기술(주)의 DialPad 나, MS-NetMeeting 등의 프로그램을 수행하여 NAT 로 운영되어지는 망에서 통화를 해보면 쉽게 알 수 있다. 외부에서 통화를 시도할 때는 통화에 실패하게 되고, 내부

에서 외부로 통화할 때는 내부에서 나가는 소리만 전달되고, 외부에서 들어오는 소리는 내부에서 들을 수 없게 된다.

3. NAT 와 Gatekeeper 연동 구조

본 절에서는 NAT 기반의 private network 에서 IP telephony 시스템을 지원하기 위하여 NAT 와 gatekeeper 서버를 연동하는 구조를 기술한다.

NAT 라우터와 gatekeeper 와 함께 사용할 때 NAT 가 알아야하는 주소 및 포트는 H.225.0 RAS 주소와 포트, H.225.0 Q.931 주소와 포트, H.245 control channel 주소와 포트, RTP channel 주소와 포트이다. 따라서 gatekeeper 와 NAT 라우터는 특별한 channel 을 열고 각 주소와 포트 정보를 주고 받아야 하며 gatekeeper 는 부팅 시에 NAT 라우터를 사용하는지를 검사하고 이 특별한 channel 이 끊어진 경우 수시로 재 연결을 시도해야 한다.

NAT 라우터와 gatekeeper 가 주고 받아야 하는 정보는 dynamic NAT 가 어떤 모드를 사용하는가에 따라 다르다. NAT single mode 일 경우에는 NAT 라우터가 gatekeeper 와 H.323 단말의 private 주소 정보와 함께 각 메시지에서 사용하는 포트 정보까지 저장해야 하므로 gatekeeper 가 H.323 단말간의 signalling 전과정에 참여(Gatekeeper routed call signalling. 그림 1 참조)하여 각 과정에서 사용하는 포트 정보를 NAT 라우터에게 알려주어야 한다. NAT global mode 일 경우에는 NAT 라우터가 gatekeeper 와 H.323 단말의 주소 정보만 필요하므로, 반드시 gatekeeper 를 점유하는 H.225.0 RAS 메시지를 교환할 때 gatekeeper 가 H.323 단말의 private 주소를 알려줄 수 있다. NAT 라우터가 이미 H.323 단말의 private 주소를 확보하였으므로 이후 signalling 과정에서 gatekeeper 는 public H.323 단말로 전송되는 메시지의 내용 중에서 gatekeeper 와 private H.323 단말의 private 주소 부분만 public 주소로 치환하여 전송한다. 3.1 절과 3.2 절에서는 NAT mode 에 따른 구체적인 동작 절차를 기술한다.

3.1 NAT single mode

NAT single mode 를 사용할 경우에는 각 메시지에서 사용하는 포트 정보가 달라지므로 gatekeeper 가 H.323 단말간의 signalling 전과정에 참여해서 필요한 정보를 NAT 라우터에게 알려주어야 함을 기술한 바 있다. 이를 위해 NAT 라우터와 gatekeeper 사이에는 정보 교환을 위한 channel 이 필요하고 이 channel 이 설정되고 나면 gatekeeper 와 NAT 라우터는 다음과 같은 절차를 수행한다.

1. Gatekeeper 는 부팅 시에 라우터가 NAT 를 사용하는지를 검사한다.
2. 라우터가 NAT 를 사용 중이면 gatekeeper 는 자신의 private 주소, RAS 포트, Q.931 call signalling 포트 정보를 NAT 라우터에게 전송한다.
3. 전화 연결이 시작되면 gatekeeper routed mode 를

선택하고, 그 전화가 외부로부터 걸려온 경우 외부 caller 로 'call proceeding', 'alerting', 'connect' 메시지를 전송하는 과정에서 앞으로 사용될 gatekeeper 의 H.245 control signal 포트 정보를 NAT 라우터에게 전송하고 NAT 라우터는 unique한 dynamic port 를 생성하여 gatekeeper 에게 할당해준다. Gatekeeper 는 'call proceeding', 'alerting', 'connect' 메시지의 기존의 H.245 주소 자리에 새로 할당 받은 주소와 포트 정보로 수정하여 메시지를 전달한다.

4. Gatekeeper 는 H.245 signalling 이 진행되면서 H.245 logical channel signalling 을 수행할 때, 후에 내부 H.323 단말이 media 데이터를 수신하기 위해 사용할 RTP, RTCP 주소와 포트를 알아내어 NAT 라우터에게 전송하고 NAT 라우터는 unique한 dynamic port 를 생성하여 gatekeeper 에게 할당해준다. Gatekeeper 는 H.245 logical channel signalling 과정에서 RTP 및 RTCP 에 사용되어질 주소와 포트 정보를 NAT 라우터로부터 할당 받은 주소와 포트 정보로 대체한 후 signalling 을 계속한다.
5. H.245 logical channel signalling 에서 media channel 을 닫기 위해 사용하는 close logical channel 메시지에 대해서는 닫히는 주소와 포트를 확인하여 NAT 의 자원을 반환한다.
6. 호가 종료될 때 H.323 단말로부터 DRQ 를 수신하거나, gatekeeper 가 DRQ 를 송신하는 경우, release complete 를 수신하거나 송신하는 경우에 gatekeeper 는 NAT 로부터 할당받은 포트들을 모두 반환해야 한다.

3.2 NAT global mode

NAT global mode 일 경우에는 NAT 라우터가 H.323 단말의 주소 정보만 필요하므로, 반드시 gatekeeper 를 경유하는 H.225.0 RAS 메시지를 교환할 때 gatekeeper 가 H.323 단말의 private 주소를 알려줄 수 있다고 기술한 바 있다. H.323 단말은 호를 시작할 때 반드시 gatekeeper 로 RAS ARQ 메시지를 송신한다. 이 때, caller 가 NAT 내부망에 있을 경우는 gatekeeper 가 터미널의 IP 를 알게 되므로 NAT 에게 내부 caller 의 IP 정보를 알려주고 가용한 public IP 를 할당 받는다. 만약 어떤 이유로 NAT 로부터 IP 를 할당받지 못하면 ARJ 를 H.323 단말로 송신하여 호를 종료시킨다. ARQ 를 송신하는 터미널이 외부망에 있을 경우는 ARQ 내의 alias address 필드를 보고 해당 callee 를 DB 에서 찾아서 callee 의 IP 주소를 NAT 에게 알려주고 가용한 public IP 를 할당받게 되며 할당 받지 못하는 경우는 ARJ 를 송신하여 통화를 종료한다. 이상의 절차를 아래에 단계별로 간략히 기술한다.

1. Gatekeeper 는 부팅 시에 라우터가 NAT 를 사용하는지를 검사한다.
2. 라우터가 NAT 를 사용중이면 gatekeeper 는 자신의

IP 정보를 라우터에게 전송하고 라우터의 NAT public address pool 에서 gatekeeper 서버용 well known public 주소를 할당받는다.

3. 내부에서 외부로 통화를 시도하는 경우, signalling 메시지에서 통화를 시도하는 H.323 단말의 private IP 정보를 NAT 에게 전송하고 NAT 로부터 가용한 public 주소를 할당 받는다. Gatekeeper 는 이후 내부에서 외부로 전달되는 모든 메시지에 대해서 private IP 주소를 새로 할당받은 public IP 주소로 대체한다.
4. 외부에서 내부로 통화를 시도하는 경우는 callee 전화번호에 해당하는 IP 를 찾아서 해당 IP 를 NAT 에게 전송하고 NAT 로부터 가용한 public 주소를 할당 받는다. Gatekeeper 는 이후 내부에서 외부로 전달되는 모든 메시지에 대해서 private IP 주소를 새로 할당받은 public IP 주소로 대체한다.
5. 호가 종료될 때는 NAT 로부터 할당받은 public IP 주소를 반환한다.

4. 결론

본 논문은 NAT 로 운영되는 private network 내에 IP 전화 시스템이 존재하는 환경에서 caller 단말, gatekeeper 서버, callee 단말 간에 교환되는 H.225.0 메시지와 H.245 메시지의 NAT 주소 변환이 동적인 방법으로 투명하게 이루어지도록 하기 위하여 gatekeeper 와 NAT 를 연동하는 구조를 제안하였다. 제안된 구조는 gatekeeper 와 NAT 라우터 사이에 주소 변환을 위한 정보 교환용의 channel 을 여는 단계, gatekeeper 가 외부 단말로 향하는 H.225.0, H.245 메시지를 받았을 때 NAT 라우터에게 private 주소, 포트 (이하 포트 정보는 NAT single mode 일 경우에 한함) 정보를 알려주는 단계, NAT 라우터가 gatekeeper 로부터 private 주소, 포트 정보를 받았을 때 public IP 와 포트를 할당하여 gatekeeper 에게 알려주는 단계, gatekeeper 가 할당받은 public IP 와 포트 정보를 반영하여 외부 단말로 향하는 H.225.0, H.245 메시지를 재 생성하는 단계, 마지막으로 호가 종료될 때 gatekeeper 가 NAT 라우터로부터 할당받은 NAT 자원을 NAT 라우터에게 반환하는 단계로 구성된다. 이상의 제안된 구조를 이용함으로써 IP 전화 단말과 gatekeeper 가 존재하는 IP telephony 환경에서도 IP 주소 부족의 문제를 해결할 수 있는 NAT 를 사용할 수 있다.

참고문헌

- [1] K. Egevang, "The IP Network Address Translator (NAT)", RFC 1631, May. 1994.
- [2] ITU-T, "Recommendation H.323 Packet Based Multimedia Communications Systems", 1997.
- [3] ITU-T, "Recommendation H.225.0 Call Signalling Protocols and Media Stream Packetization for Packet Based Multimedia Communications Systems", 1997.
- [4] ITU-T, "Recommendation H.245 Control Protocol for Multimedia Communication", 1998.