인터넷 전화 서비스를 위한 NAT 프럭시 서버
(A NAT Proxy Server for an Internet Telephony Service)

손 주 영 †
(Jooyoung Son)

요 약 인터넷 전화 서비스는 현재 상업적으로 성공한 인터넷 기반 응용 서비스 가운데 하나이다. 이 서비스를 위한 기반 기술은 VoIP이다. 이는 QoS 보장이 되지 않는 인터넷에서의 분산 멀티미디어 서비스를 위한 표준 프로토콜인 H.323 또는 SIP를 활용한다. 여기서 음성 데이타를 전송하기 위한 프로토콜로써 RTP/UDP/IP 프로토콜 스택을 채택하였다. 그러나 UDP 전송 프로토콜을 이용하는 인터넷 응용은 비공인 IP 주소를 이용하는 사설망 또는 일부 초고속인터넷망 서비스 접속자들에게 불완전하게 데이타를 전송하는 결과를 초래한다. 인터넷 전화 서비스 경우, 음성 수신이 불가능하여 상대방의 목소리가 들리지 않는 현상이 발생한다. 특히 본 논문에서 다룬 인터넷 전화 서비스에서는 음성 데이타 수신을 위해 모든 세션에 대해 동일한 하나의 UDP 포트 번호를 사용하는 특성을 가지고 있어 문제를 더욱 어렵게 하였다. 이 문제를 해결하는 방식으로 단말 프럭시, 게이트웨이 프럭시, 프로토콜 변환 방식 등을 제시하고, 그 가운데 실제 구현한 게이트웨이 프럭시 방식을 기반으로 한 NAT 프럭시 서버에 대해 자세하게 설명한다.
키워드 : 인터넷 전화 서비스, VoIP, NAT 문제, 프럭시 서버

Abstract The Internet telephony service is one of the commercially successful Internet application services. VoIP technology makes the service come true. VoIP deploys H.323 or SIP as the standard protocol for the distributed multimedia services over the Internet in which QoS is not guaranteed. VoIP carries the packetized voice over the RTP/UDP/IP protocol stack. The data transmission trouble is caused by UDP when the service is provided in private networks and some ISP-provided Internet access networks in the private address space. The Internet telephony users in such networks cannot listen the voices of the other parties in the public Internet or PSTN. Making the problem more difficult, the Internet telephony service considered in this paper gets the incoming voice packets of every session through only one UDP port number. In this paper, three schemes including the terminal proxy, the gateway proxy, and the protocol translation are suggested to solve the problems. The design and implementation of the NAT proxy server based on gateway proxy scheme are described in detail.
Key words : Internet telephony service, VoIP, NAT problem, Proxy server

1. 서 론

인터넷 전화 서비스는 인터넷을 통한 컴퓨터 대 컴퓨터(PC-to-PC), 컴퓨터 대 전화(PC-to-phone), 전화 대 컴퓨터(phone-to-PC) 또는 전화 대 전화(phone-to-phone) 형식의 전화 서비스를 의미한다. 이는 기존의 전화망을 이용한 전화 서비스보다 이용료 면에서 일반 사용자에게 유리하기 때문에 널리 쓰이고 있는 상황이다. 이 서비스 가운데 앞선 3 가지 형태는 인터넷 서비스 제공자(ISP : Internet Service Provider)에서 제공하는 초고속 인터넷 망을 이용하거나 아니면 전용선을 통한 인터넷 사용자들이 시내, 시외전화 및 국제전화를 걸 수 있도록 하는 서비스이다. 이를 구현하기 위해 적용되는 기술은 VoIP(Voice Over IP)이다[1]. VoIP는 인터넷을 이용하여 음성을 패킷 형태로 전송하는 기술을 의미한다. VoIP 시스템을 구성하는 요소는 계층 구조로 되어 있으며 응용 계층, 신호 계층, 그리고 매체 계층으로 구성된다[2]. 응용 계층은 서비스의 생성 및 수행 기능, 호 처리 및 서비스 관리를 담당한다. 신호 계층은 호 처리, 호 변환, 자원 관리, 그리고 매체 제어를 수행한다. 매체 계층은 실제적인 데이타 변환, 전달을 담당하며 전달되는 음성 품질의 보장, 그리고 톤 발

· 이 논문은 새롬기술(주)과 두뇌한국21사업단에 의해 지원되었음.
† 정 회 원 : 한국해양대학교 컴퓨터공학과 교수
mmlab@hhu.ac.kr
논문접수 : 2002년 6월 12일
심사완료 : 2002년 11월 4일

생 기능을 담당한다.

이 가운데 신호 계층 프로토콜 표준은 ITU-T에서 권고하는 H.323 또는 IETF의 RFC 2543 SIP(Session Initiation Protocol) 등이다[3,4]. H.323은 애초 QoS의 보장이 되지 않는 근거리망(LAN) 한 세그먼트 내에서 이루어지는 화상 회의 서비스 등 멀티미디어 서비스를 위해 제정된 프로토콜이다. 그것이 인터넷에서의 일반적인 전화 서비스의 문제를 커버하는 기술로 확대되었다. H.323은 단독 프로토콜이 아니다. 전체 H.323 시스템은 제어 기능을 위한 H.245, 광범위한 화상회의들을 관리하기 위한 H.332, 연결 관리용 H.225, 보안 처리를 위한 H.235, 화상회의에서의 문서 지원을 위한 T.120, 그리고 회선교환망과의 연동을 위한 H.246으로 구성되어 있다. SIP는 인터넷에서 두 종단간에 형성되는 미디어 세션에 관련된 제어 프로토콜이다. 종단의 위치, 세션 수립을 위한 접촉, 세션에서 사용될 미디어 정보 교환, 기존의 미디어 세션의 변경, 그리고 미디어 세션의 종료 등의 기능을 수행한다. 위의 두 프로토콜은 서로 다른 요구사항과 특성을 가지고 서로 다른 기관에 의해 개발되었다. 그러나 두 프로토콜은 인터넷 전화 서비스의 제어 프로토콜로서 채택되어 혼재하고 있는 현실이다. 이 둘 간의 차이점은, 크게 3 측면에서 두드러진다. 전송측면에서 SIP는 TCP, UDP 또는 다른 프로토콜을 사용할 수 있으나 H.323은 TCP만을 이용하도록 설계되어 있다. 화상회의를 하는 데이타 전송 측면에서는 SIP에서는 IP 멀티캐스트(IP multicast)를 활용하는 반면 H.323은 MCU(Multipoint Control Unit)을 채택해야 한다. 마지막으로 프로토콜 제어 메시지의 전달 방식에서 SIP는 ABNF(Augmented Backus Naur Format)을 사용하여 문자(text)를 기반으로 인코딩하여 전달하는 반면, H.323은 ASN.1(Abstract Syntax Notation 1)로 표현된 메시지를 PER(Packet Encoding Rule)에 의해 인코딩하여 전달하는 차이가 있다.

본 논문은 위의 신호 계층을 위한 프로토콜 가운데 H.323을 기반으로 하는 인터넷 전화 서비스에서 음성 패킷 전달 시에 발생하는 문제를 해결한 것이다. 인터넷에 접속하는 특정 통신망 환경에서는 음성 데이타의 송수신이 원활하게 이루어지지 않는다는 점에서 문제가 발생한다. 인터넷 전화 서비스를 위한 음성 데이타의 송수신은 RTP/UDP/IP 프로토콜 스택을 활용한다(그림 1). 이는 가벼운 프로토콜을 이용하여 지연에 매우 민감한 음성 데이타를 되도록 작은 전송지연과 처리지연으로 송수신하기 위한 방식이다. UDP는 최종단 간(end-to-end)의 데이타 송수신을 위한 사전 연결(connection)을 하지 않은 채 데이타 전송이 이루어지는 프로토콜이다[5]. 그러나 특정 형태의 통신망에서는 데이타의 최종단간의 데이타 송수신을 위해서는 반드시 사전에 연결 작업(call setup)을 필요로 한다. 이의 대표적인 사례가 보안을 위한 방화벽(firewall)인 경우와 IP 주소의 고갈 현상을 극복하기 위한 NAT(Network Address Translation)를 적용한 경우들이다. 본 논문에서는 NAT 경우에 대한 것만을 다룬다.

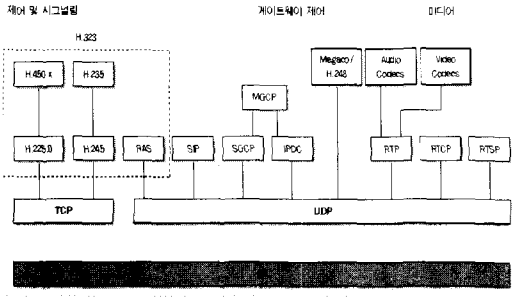


그림 1 VoIP 프로토콜 스택[6]

NAT는 공중 인터넷망과 사설망(private network)사이에 존재하면서 IP 주소의 부족 현상을 완화시키는 역할을 한다. 하나의 공중 인터넷에 접속할 수 있는 IP 주소를 할당받은 상황에서 이 주소를 이용하여 다수의 노드들이 동시에 인터넷에 접속할 수 있도록 하는 기능을 수행하는 것이다[7]. 종종 투명 프럭시(Transparent Proxying), IP 주소 오버로딩(IP Address Overloading), 또는 IP 마스크레이딩(IP Masquerading) 등으로 불리는 기술로서, 일반적으로 라우터에 구현되는 경우가 많다. NAT는 특정 영역의 IP 주소를 다른 IP 주소로 변환함으로써 동작을 한다. 변환될 IP 주소들은 어떤 조직(학교 또는 연구실 등)의 내부망에 존재하는 개별적인 컴퓨터에 지정된 것으로 어떤 IP 주소도 가능하나, 가장 일반적으로 사용되는 것은 RFC에서 지정되지 않는 범위(10.x.x.x, 172.16.x.x-172.32.x.x, or 192.168.x.x)의 IP 주소들이다. 반면 이들 주소에 대응되어 변환되는 단 하나의 IP 주소는 외부망에 노출되어 있는 정식으로 할당받은 것으로 라우팅이 가능한 IP 주소이다. 내부적으로 보았을 때, 모든 컴퓨터들은 인터넷에 있는 어떠한 노드로 직접 접속이 가능하다. 외부에서 보면, 모든 인바운드, 아웃바운드 TCP/IP 트래픽이 하나의 정식으로 할당받은 IP 주소로부터 발생하는 것으로 보인다. 엄격하게 말하면 NAT도 IP 라우팅 기법 가운데 특별한 형태의 하나라고

말할 수 있다.

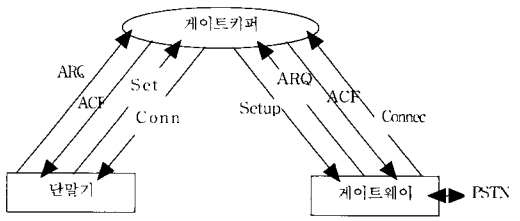
문제는, NAT 라우터를 통하여 전달되는 IP 데이타그램(datagram)에 나타나는 데이타의 발생지와 목적지 IP 주소는 실제적으로 각 node에 할당된 주소가 아니라 NAT 라우터에 정식으로 할당된 IP 주소로 변환되는 데서 발생한다. 결과적으로 집 또는 소규모 사무실 환경이나 일부 ISP 등에 의해 제공되는 IP 주소가 NAT에 의한 가상 IP인 경우 즉, 컴퓨터에 할당된 IP 주소가 비공인 IP 주소인 경우, 외부에 있는(public Internet) 노드 또는 일반전화망(PSTN)을 이용하는 일반 전화 서비스 사용자끼리 인터넷 전화 서비스를 이용하여 통화 시에는 상대방의 목소리가 서로 잘 들리지만(음성 패킷이 상호 잘 전달됨), NAT 내부에 있는 노드에서 인터넷 전화 서비스를 이용하여 외부에 있는 노드 또는 일반전화망 전화 사용자와 통화하는 경우, 외부망에 있는 상대방의 목소리가 들리지 않는 (외부망에 있는 음성 패킷이 내부망에 있는 노드에 전달되지 않음)현상이 발생한다. 이 현상은 외부망에 있는 노드로부터 NAT 라우터 내부에 있는 노드로 보내지는 UDP 데이타그램(incoming UDP datagram)은, 그전에 동일한 UDP 포트를 이용하여 외부망으로 데이타(outgoing data)가 전송되지 않았다면 NAT 라우터에서 내부망으로 전달하지 않고 그 데이타그램을 무시하여 폐기해 버리기 때문이다.

본 논문은 다음과 같이 구성되었다. 2 장에서 위에서 언급한 NAT 문제를 더욱 자세하게 조명하고, 3 장에서 이러한 NAT로 인한 문제를 해결하는 방법을 제시한다. 4 장은 제시된 방법을 구현한 예를 보인다. 그리고 마지막으로 5 장에서는 결론과 함께 향후 연구 방향 등을 논의한다.

2. NAT 문제

인터넷 전화 서비스를 위한 H.323의 기본 구성 요소는 단말(terminal), 게이트웨이(gateway), 게이트키퍼(gatekeeper), 그리고 MCU로 구성된다[8]. 단말기는 응용 계층의 기능을 구현한 것으로 일반 사용자들이 인터넷 전화 서비스를 이용하기 위해 직접 접촉하는 기계 또는 응용 소프트웨어이다. 그리고 이것은 H.323의 호 설정(call setup)기능 등을 구현함으로써 게이트웨이와 세션을 연결한다. 게이트웨이는 인터넷과 PSTN 망을 상호 연동시키는 역할을 담당한다. 구체적으로 H.323(특히, Q.931과 H.245를 통한)과 SS.7 호 설정 프로토콜(call setup protocol)의 변환, IP 주소와 E.164 주소(일반적인 전화번호)체제의 변환, 패킷으로 된 음성(packetized voice)과 디지털 음성(digital voice)의 변환 등이 주요 임무이다. 게이트키퍼는 클라이언트의 요청에 대해 서비스를 할 수 있는 게이트웨이를 할당하는 역할을 담당한다. 이는 분산되어 있는 게이트웨이들에게 작업의 분량을 적절하게 분산 처리하도록 만드는 기능을 수행하는 것이다. 따라서 게이트키퍼는 주기적으로 게이트웨이로부터 현재 세션 연결 상태에 대한 정보를 보고 받아 골고루 부담을 분산시키는 역할을 수행한다. MCU는 동시 여러 사람이 다중 통화하는 경우에 서로 중재하는 역할을 담당하므로 현재 일반적인 전화 서비스(일 대 일 전화)만을 고려한다면 구현되지 않아도 무방한 요소이다.

인터넷 전화 서비스를 위한 호 설정은 단말과 게이트웨이간에 상호연결을 위한 규약으로 H.225를 사용한다. H.225는 터미널과 게이트키퍼 사이에 주고받는 메시지(RAS)와 호 신호(Call signaling)에 대한 메시지(Q.931)로 구성된다(그림 2). 이는 TCP/IP 하에서 시행된다. 단말과 게이트웨이 사이에 TCP 기반 호 설정 과정을 거치게 되면 단말과 상대방 전화기(callee phone) 사이에 음성 통화를 위한 호가 형성된다. 그 이후에 단말과 일반전화망의 상대방과 통화가 이루어진다. 음성 데이타의 송수신은 RTP/UDP/IP 프로토콜 스택을 활용한다. 이때 1 장에서 언급한 바와 같이 NAT의 불완전한 UDP 데이타그램 전달로 인해 NAT에 의한 사설 IP 주소가 사용되는 소규모의 사설망에 연결된 노드 또는 특정 ISP들로부터 인터넷 접속 서비스를 받는 경우에 인터넷 전화 서비스를 이용하지 못하는 현상이 발생한다.



RAS messages = ARQ : Admission Request, ACF : Admission Confirm

Call signals = Setup : 호 설정, Connect : 호 연결(전화가 완전 연결된 상황)

그림 2 인터넷 전화 서비스를 위한 호 설정(Q.931)

NAT는 공인된 IP 주소가 쓰이는 공중 인터넷망(public Internet)과 비공인 IP 주소를 사용하는 사설망(private network)사이에 존재하고 기본적으로 IP 주소의 고갈 현상을 타개하기 위한 수단으로 활용된다. NAT 라우터를 통하여 외부망에 전달되는 IP 데이타그

램에 나타나는 발생지와 목적지 IP 주소는 실제적으로 각 노드에 할당된 사설 IP 주소가 아니라 NAT 라우터에 할당된 공인된 IP 주소로 변환된 것이다. NAT는 일반적으로 다음과 같이 5가지 형태로 구현된다.

1) 망 주소 및 포트 변환(NAPT) / IP 마스크레이딩 (IP Masquerading)

NAT로서 가장 일반적인 형태이다. 사설망에 단 하나의 공인된 IP 주소가 할당된 환경에서 활용된다. 예를 들어, 단일 ISP에 연결되는 형태에서 주로 적용이 된다. 사설망에 있는 각 노드들은 그 내부에서 모두 식별이 가능하여야 하므로 각기 다른 사설 IP 주소로 할당되어야 한다.

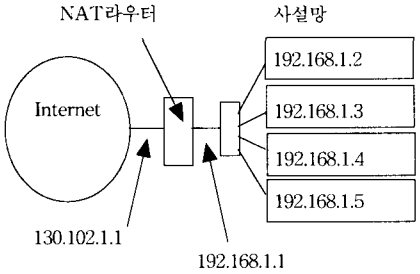


그림 3 망 주소 및 포트 변환(NAPT) / IP 마스크레이딩 (Masquerading) 예

그림 3의 예에서, 사설망 192.168.1.0은 인터넷 측면에서 바라 볼 때 공인된 IP 주소인 130.102.1.1 뒤에 숨겨져 있는 상태이다. NAT 라우터는 공인 IP 주소 130.102.1.1과 사설 IP 주소 192.168.1.1 등 2 개의 주소를 가진다. 각각 서로 다른 NIC(Network Interface Card)에 지정되어 있다. 사설망에서 발생하는 모든 패킷은 자신들의 발생지 IP 주소(사설 IP 주소)를 가지고 있다. 그러나 그것이 인터넷으로 전송될 때는 NAT 라우터에 의해 공인된 IP 주소인 130.102.1.1로 변환되어 전달된다. 그러면 인터넷에서는 사설망에서 발생하는 모든 패킷은 NAT 라우터가 발생시킨 것으로 간주하게 된다. 그러나 실제적인 데이타의 발생지를 구분할 필요가 있다. 그리고 인터넷에서 사설망으로 전송되는 패킷인 경우에도 각 패킷의 사설망 내의 최종적인 목적지를 식별하는 방법이 있어야 한다. 각 데이타를 발생시킨 사설망 내의 발생지 또는 최종 목적지 노드를 구분하는 것은, 전송 계층(Transport Layer)에서 쓰이는 포트 번호의 적절한 변환으로 이루어진다. 예를 들어, 사설망 내의 192.168.1.2의 포트 번호 1000번을 활용하는 TCP/IP 응용에서 인터넷으로 나가는 데이타(outgoing data)가 발생하면, NAT 라우터에서 표 1의 예와 같은 IP 주소/포트 번호 변환표가 만들어진다.

표 1 NAT 라우터 내의 변환표 예

Private Network Source	Masqueraded Port Number
192.169.1.2 / 1000	3000

그러면 이 TCP 세션에 해당되는 인터넷으로 나가는 IP 패킷(outgoing data)의 발생지 IP 주소와 포트 번호는 각각 130.102.1.1과 3000이 된다. 따라서 인터넷에서는 NAT 라우터에서 발생된 패킷으로 생각하게 되고 그곳에서 포트 번호 3000을 이용하는 TCP 응용이 IP 패킷을 발생시킨 것으로 보게 된다. 외부 인터넷에서 사설망으로 전달되는 데이타(incoming data)의 최종 IP 주소 및 포트 번호는 인터넷으로 패킷이 NAT 라우터를 거쳐 나갈 때 NAT 라우터에 형성된 IP 주소/포트 번호 변환표에 의해 찾아진다. 표 1의 예를 이용하면, 만약 사설망 안으로 들어오는 TCP 패킷의 목적지 IP 주소와 포트 번호가 각각 103.102.1.1과 3000이면, 그것의 최종적인 목적지는 사설 IP 주소 192.169.1.2를 가지는 노드에서 TCP 포트 번호 1000인 응용이 되는 것이다.

2) 동적 망 주소 변환(Dynamic NAT)

여기서는 포트 번호에 대한 변환 없이 IP 주소에 대해서만 변환이 일어난다. 외부에서 활용할 수 있는 IP 주소의 수가 NAT 라우터 뒤에 숨겨져 있는 사설망에서 활용하는 수보다 적은 경우에 적용이 된다. NAT 라우터는 현재 사용하지 않고 있는 외부 IP 주소를 선택해서 내부 주소에게 할당한다(그림 4). 이런 형태의 변환은 일반적으로 동시에 외부망과 통신하는 사설망 내의 노드 수가 NAT 라우터에 할당된 외부 IP 주소보다 적을 때 적용할 수 있다. 기능적으로 보면 DHCP (Dynamic Host Configuration Protocol)와 매우 유사하다. 다만 DHCP는 사설망에 있는 노드들에게 고정 IP 주소가 지정되는

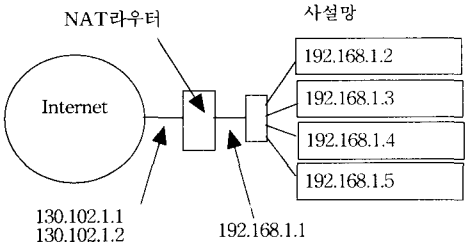


그림 4 동적 망 주소 변환(Dynamic NAT) 예

것이 아니라 그 노드가 부팅할 때의 상황에 따라 달라지는 점이 다르다.

3) 포트 변환 동반 동적 망 주소 변환(Dynamic Network Address Translation with Port Translation)

여기서는 1) 경우와 같이 IP 주소와 포트 번호가 함께 변환된다. 차이점은 외부에서 활용할 수 있는 IP 주소의 수가 다수인 점이다. 즉, 2) 경우와 같은 상황일 때 적용된다. 이 방법을 쓰면 동시에 형성할 수 있는 외부망에 대한 연결 요청의 수를 더욱 많게 할 수 있는 장점이 있다.

4) 정적 망 주소 변환(Static Network Address Translation)

일반적으로 사설망과 사설망 사이에 활용된다. 두 개의 망이 동일한 주소공간을 가지고 있는 경우에 활용할 수 있는 경우이다(그림 5).

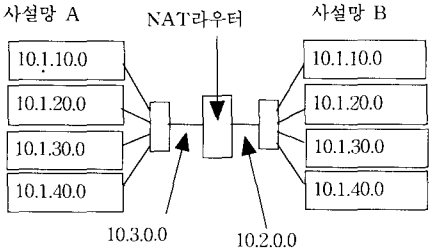


그림 5 정적 망 주소 변환 예

그림 5와 같은 경우, 사설망 A에서 사설망 B에 있는 노드들의 주소를 지정할 때는 10.2.xx.yy를 활용하고, 반대로 사설망 B에서 사설망 A에 있는 노드들의 주소를 지정할 때는 10.3.xx.yy로 한다.

5) 포트 매핑과 리다이렉션(Port Mapping and Redirection)

외부 인터페이스의 특정 포트가 사설망 내부의 서비스들에 재 매핑되어 있는 형태이다. 그림 6의 예에 의하면 외부에 알려진 공인된 IP 주소는 130.102.1.1 뿐이다. 그러나 서비스 측면에서 보면 각 서비스 별로 내부에 여러 서버가 운영되고 있는 형태가 된다. 예를 들어,

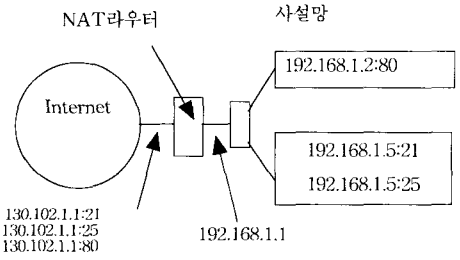


그림 6 포트 매핑과 리다이렉션 예

130.102.1.1:80으로 들어오는 요청은 192.168.1.2에 있는 웹 서버에게 다시 매핑되고, 130.102.1.1:21로 요청되는 파일전송 서비스는 192.168.1.5의 ftp 서버가 처리하는 것으로 다시 매핑되는 것이다. 만약 부하가 많이 걸리는 상황에서는 사설망에 동일 서비스를 제공하는 서버들을 복수개 둘 수 있다. 이때 NAT 라우터는 그들 사이에 부하가 균등하게 걸릴 수 있게 하는 기능도 담당하게 된다.

위와 같은 5 가지 NAT 구현 방식 가운데 본 논문과 직접적인 관계가 있는 NAT 방식은 1) 망 주소 및 포트 변환(NAPT) / IP 마스크레이딩이다. 이 방식에 의하면 사설망과 외부망과의 NAT에 의한 패킷 교환이 제대로 이루어지기 위해서는 NAT 라우터 내부에 있는 주소 변환표(IP Masquerading Table)내에 연결에 해당되는 변환 정보 엔트리가 존재해야 한다. 이것이 만들어지는 시점이 매우 중요하다. 그 시점은 사설망에서 외부망으로 향하는 데이타 전송이 처음 일어나는 순간이다.

TCP 경우에는 연결(connection)이 설정되기 위해서는 호 설정 과정을 거쳐야 하고, 그 과정에서 기본적으로 3 방향 핸드쉐이크(3 way handshaking) 방식으로 SYN 데이타 송수신이 쌍방향으로 오고 가게 된다. 이 때문에 TCP를 이용한 데이타 전송인 경우에는 NAT 라우터의 존재가 완전히 투명한 상황이 조성된다. 즉, NAT 라우터 내에 주소 변환표 상에 해당 연결에 대한 변환 정보 엔트리가 생성이 되는 것이다.

그러나 UDP 경우에는 다른 상황이 발생한다. 예를 들어, 사설망에서 외부망으로 나가는 데이타와 반대로 외부망에서 사설망으로 들어오는 데이타에 대해 서로 다른 UDP 포트 번호를 쓰는 응용 프로그램이 있다고 가정하면, 밖으로 나가는 포트 번호(outgoing port number)에 대한 주소 변환표 내에 변환 정보 엔트리는 생기게 되나, 안으로 들어오는 포트 번호(incoming port number)에 대한 변환 정보 엔트리는 결코 생기지 않게 되는 것이다. 따라서 NAT 라우터에서는 이러한 외부에서 사설망으로 들어오는 패킷이 도착하면, 사설망 내의 어떤 노드로 전달(forwarding)해야 하는지를 알지 못하므로 그 패킷을 버리는 현상이 발생되는 것이다.

예를 들어, A와 B 노드가 양방향 데이타 전송에 있어서 서로 다른 UDP 포트 번호를 사용하는 이런 응용을 통해 상호 통신한다고 가정할 때, 다음과 같은 각 상황에서 다음과 같은 현상이 발생하게 된다.

1) A, B 노드 모두가 NAT 라우터 뒤에 숨겨져 있는 사설망에 있는 경우 :

A 와 B 노드 모두에서 송신은 가능하여도 수신은

불가능함

2) A 노드가 NAT 라우터 뒤에 숨겨져 있는 사설망에 있는 경우 :
   A 노드는 송신은 가능하나 수신은 불가능함. B 노드는 송수신 모두 가능함
3) B 노드가 NAT 라우터 뒤에 숨겨져 있는 사설망에 있는 경우 :
   B 노드는 송신은 가능하나 수신은 불가능함. A 노드는 송수신 모두 가능함

요약하면, 외부망에 있는 노드로부터 NAT 라우터 뒤에 숨겨져 있는 사설망 내의 노드로 보내지는 UDP 데이타그램은, 그전에 동일한 UDP 포트를 이용하여 반대방향 전송이 이루어 진 상태가 아니라면 사설망 내부로 전송이 되지 않는다. 특히 UDP를 이용하여 데이타를 송수신하는 응용 프로그램이 실제 UDP를 이용한 데이타 송수신을 개시하기 전에 호 설정 등의 과정에서 데이타 송수신을 위한 IP 주소와 포트 번호를 데이타 패킷의 데이타 영역(data field)에 실어서 상대방에게 알리는 경우, NAT를 사이에 두고 그 응용이 실행된다면 내부망에서 외부망으로부터의 데이타 수신은 불가능하게 되는 것이다. 왜냐하면 NAT는 TCP 또는 UDP의 데이타그램 영역 가운데 헤더 필드만을 분석할 뿐, 나머지 데이타 영역은 전혀 보지 않기 때문이다. 따라서 NAT로서는 외부망으로부터 사설망으로 들어오게 될 데이타의 실제적인 목적지 노드에 대한 정보(사설망 내에서 할당된 IP 주소와 포트 번호)를 NAT 내의 주소 변환표에서 얻을 수 없게 된다.

위의 경우 더욱 심각한 현상이 발생되는 문제점을 안고 있다. 그것은, 호 설정 과정에서 NAT 뒤에 숨겨져 있는 사설망 내의 노드가 외부망에 있는 상대방에게 알려주는 사설망으로 들어오는 데이타를 위한 목적지 IP 주소(자신의 사설 IP 주소)가 공중 인터넷에서는 전혀 의미가 없는 주소이기 때문이다. 따라서 만약 알려준 목적지 IP 주소를 이용하여 공중 인터넷에 있는 상대방이 NAT 뒤에 있는 사설망 내의 노드로 데이타를 전송하더라도 그 데이타는 전혀 엉뚱한 곳으로 라우팅이 되거나 목적지를 찾지 못하고 TTL 값의 소진으로 인한 타임아웃으로 간주되어 알 수 없는 라우터에 의해 버려지게 되는 현상이 발생하는 것이다.

예를 들어 그림 7의 경우, NAT 라우터 뒤에 있는 사설망 내의 192.168.1.5 노드가 TCP를 이용한 호 설정 과정에서 203.230.252.4에게 "너(203.230.252.4)가 나(192.168.1.5)에게 UDP 데이타그램을 보낼 때 192.168.1.5 IP 주소와 10000 포트 번호를 이용하라."고 알려주고 있다. 그러나 이 사설망은 NAT 라우터에 의해 130.102.1.1 IP 주소를 이용해야 하는 망이다. 즉, 130.102.1.1 IP 주소를 목적지 주소로 써서 데이타를 보내야 NAT 라우터까지 만이라도 데이타가 도착될 수 있다. 그러나 203.230.252.4 노드에서 192.168.1.5가 알려준 대로 192.168.1.5 IP 주소와 10000 포트 번호를 목적지 주소로 하여 데이타를 보내면, 그 데이타는 공중 인터넷에서 존재하지 않거나 전혀 다른 목적지로 전송되는 결과가 되는 것이다(그림 8).

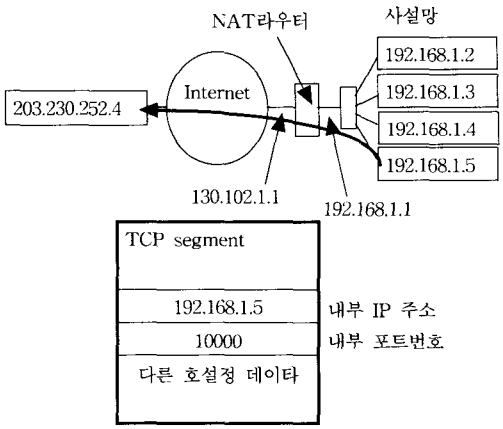


그림 7 호 설정에서의 목적지 주소/포트 지정 문제

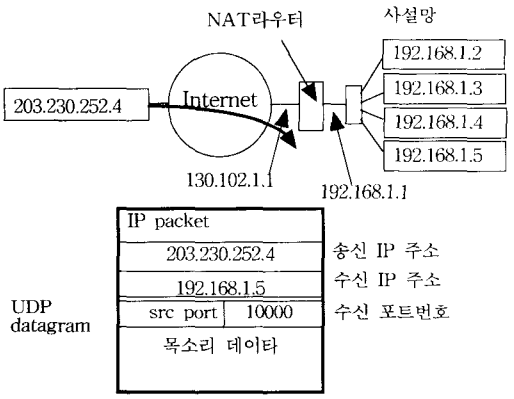


그림 8 사설 IP 주소를 목적지로 한 데이타 전송 예

3. NAT 문제 해결 방안

2장에서 제기된 문제가 인터넷 전화 서비스에서 RTP/UDP/IP 프로토콜 스택을 이용하는 음성 정보 전달 과정에서 그대로 나타난다. 즉, NAT 뒤에 숨어 있

는 사설망 내의 노드에서 전화를 거는 경우, 일반전화망을 통해 전화를 받는 상대방은 전화를 건 사람의 목소리가 잘 들리나, 사설망 내의 노드에서 전화를 건 사람에게는 상대방의 목소리가 들리지 않는 현상이 일어나는 것이다.

이러한 문제점을 해소하기 위한 일반적인 방법은, 응용 사이에 발생하는 양방향 UDP 트래픽 모두가 하나의 UDP 포트를 통해 송수신하도록 하는 것이다. 사설망에서 외부망으로 나가는 데이타그램이 특정 포트 번호를 이용해 전송하면, NAT에서 이루어지는 IP 주소와 포트 번호 변환 과정에서 주소 변환표에 변환 정보 엔트리가 생기게 된다. 그리고 외부망에서 사설망으로 향하는 데이타의 전송이 동일한 포트 번호(NAT에 의해 변환된 포트 번호로 사설망 노드가 사용하는 포트 번호와 반드시 일치하지 않는 값임)로 이루어진다면 이 변환 정보 엔트리를 통해 사설망 내의 노드로 전송이 가능해지는 것이다.

그러나 게이트웨이가 단말 노드로 음성 데이타를 전송할 때, 모든 세션에 대해 목적지 포트 번호로 특정 고정된 포트 번호만을 이용하여 전송하도록 설정된 서비스 경우에는 이러한 해결책을 그대로 이용하지 못한다. 다시 말해 단말 노드에서 발생하는 음성 데이타가 게이트웨이로 향할 때 이용되는 게이트웨이의 UDP 포트 번호와 게이트웨이에서 단말 노드로 음성 데이타를 전송할 때 이용하는 단말의 UDP 포트 번호가 서로 같지 않을 뿐만 아니라, 후자인 경우는 모든 세션에 대해 동일한 하나의 포트 번호만을 사용하는 것이다. 그림 9는 그 예를 나타낸다. 여기서 포트 번호 10000이 후자의 예이다.

이런 경우, 만약 NAT 라우터 뒤에 있는 사설망 내의 둘 이상의 노드들이 동시에 위와 같은 인터넷 전화 서비스를 쓰고 있는 상황에서는 NAT 라우터에 의해 사설망으로 향하는 음성 데이타에 대한 주소 변환표의 변환 정보 엔트리가 있다고 가정하더라도, 게이트웨이에서 NAT 라우터로 오는 모든 세션의 음성 데이타는 동일한 목적지 IP 주소(NAT 라우터의 IP 주소)와 포트 번호(그림 9. 예를 들면, 10000)를 가지고 오게 되므로 실질적 최종 목적지 구분이 어려워진다. 그러면 이 음성 데이타들은 현재 인터넷 전화 서비스를 이용하고 있는 두 노드 모두에게 전달되어 통화 내용이 뒤섞이는 현상이 발생하게 되는 것이다.

따라서 NAT 라우터내의 주소 변환표 정보 조작만으로 이 문제를 해결할 수 없음을 알 수 있다. 그러므로 이러한 인터넷 전화 서비스를 위한 NAT 문제를 해결하기 위해서는 위와 같은 일반적인 방법이 아닌 다른 방안을 강구해야 한다.

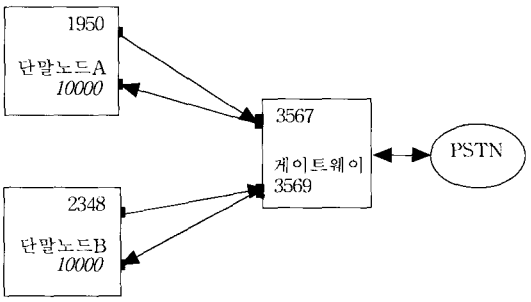


그림 9 음성 데이타 전송을 위한 UDP 포트 번호

위의 문제를 해결하기 위한 방법에는 다음과 같이 크게 세 가지가 있다.

1) 단말 프럭시

프럭시 서버를 사설망의 노드들과 NAT 라우터 사이에 두어, 단말 노드들의 프럭시 역할을 수행하도록 한다(그림 10). 프럭시 서버는 사설망으로 들어오는 음성 데이타가 NAT 라우터로부터 전달되면, 최종적으로 그것이 전송되어야 하는 사설망 내의 노드의 사설망 IP 주소와 UDP 포트 번호로 최종 목적지를 변환하여 사설망에서 그 패킷을 전송한다. 방법을 채택하였을 때 해결해야 하는 사항은 동시에 사설망 내의 둘 이상의 노드가 인터넷 전화 서비스를 이용하는 경우 이들간의 식별을 어떻게 하는가하는 문제이다. 그림 9를 통해 예를 들면 다음과 같다.

현재 프럭시 서버가 NAT 뒤 사설망 내에 있고 사설망에서의 IP 주소가 192.168.1.6이다. NAT 라우터의 주소 변환표에 UDP 포트 번호 10000이 목적지 포트 번호인 패킷이 오면, 무조건 프럭시 서버로 포트 번호 변환 없이 IP 자동 전달(IP auto forwarding)하도록 변환 정보 엔트리를 만들어 둔다. 이러한 상황에서 게이트웨

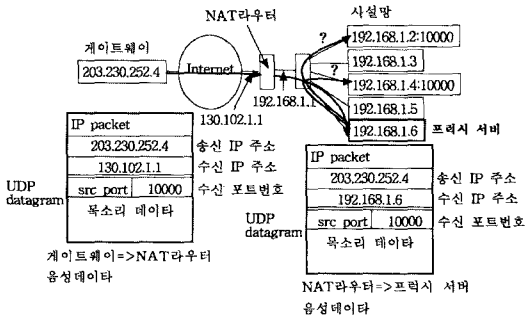


그림 10 음성 데이타 전송 해결 방법 : 단말 프럭시 서버

이로부터 사설망으로 향하는 음성 데이타가 NAT 라우터를 거쳐 프럭시 서버로 오면, 그 데이타의 목적지 IP 주소는 프럭시 서버의 IP 주소인 192.168.1.6으로 변환되어 있다. 거기서 프럭시 서버 내의 주소 변환표에 있는 현재 인터넷 음성 서비스를 이용하는 노드의 사설망 IP 주소인 192.168.1.2:10000 그리고 192.168.1.4:10000으로 변환된다. 따라서 두 노드 모두에 동일한 음성이 전달되게 되는 것이다.

이 문제를 해결하기 위해서는 게이트웨이로부터 오는 RTP/UDP/IP 음성 데이타그램에서 사설망 내의 최종 목적지를 정확하게 파악하는 방법을 찾아야 한다. RTP 패킷 헤더 내에 있는 SSRC(Synchronization Source Identification) 값이 만약 각 세션마다 다른 값으로 설정된다고 하면, 이를 바탕으로 각기 다른 세션의 RTP 패킷을 서로 구분할 수 있기 때문에 이를 이용하여 최종적인 노드로 정확하게 전달할 수 있게 된다.

2) 게이트웨이 프럭시

프럭시 서버를 NAT 바깥, 즉 NAT 라우터와 게이트웨이 사이에 둔다. 이 경우 프럭시 서버는 사설망내의 단말들에게는 게이트웨이 프럭시 역할을 담당하는 것으로 보인다. 사설망에 있는 최종 목적지 UDP 포트 번호와 외부 포트 번호(특정 고정된 포트 번호) 사이에 변환하는 방법이다(그림 11).

여기서는 우선 단말 프럭시 방법과는 달리 들어오는 음성 데이타를 위한 UDP 포트 번호로써 기존의 특정 고정된 포트 번호가 아니라, 개별적인 현재 사용하지 않는 임의의 것을 사설망에 있는 단말 노드로(정확하게는 NAT 라우터로) 전달할 때 사용한다. 이는 NAT 라우터와 프럭시 서버 사이에 세션 별로 서로 다른 포트 변환(mapping) 관계를 맺기 위한 것이다. 그림 11의 예를 보면, 게이트웨이로부터 프럭시 서버로 오는 음성 데이타는 일단 목적지 IP 주소가 프럭시 서버의 IP 주소로 되고, UDP 포트 번호는 고정된 UDP 포트 번호 10000이 된다. 이것이 프럭시 서버에 오면 목적지 IP 주소가 NAT 라우터의 것으로 변환되고 포트 번호도 해당 세션의 포트 번호로 변환된다. 발생지 IP 주소와 포트 번호도 프럭시 서버의 IP 주소와 그 세션을 위해 할당된 UDP 포트 번호로 바뀌어 나간다. 이렇게 함으로써 단말은 프럭시 서버가 게이트웨이로 여기게 되는 것이다.

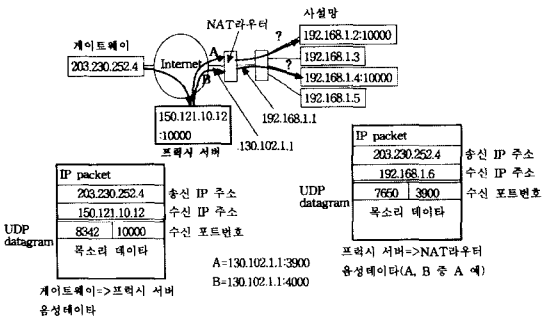


그림 11 음성 데이타 전송 해결 방법 : 게이트웨이 프럭시 서버

다시 NAT 라우터에서는 NAT 뒤에 있는 최종 목적지 사설망 IP 주소와 고정된 포트 번호(10000)로 변환하여 전송한다. 이를 위해서는 우선 NAT 라우터 내에 이를 위한 주소 변환표에 해당 변환 정보 엔트리가 사전에 생성되어 있어야 한다. 이를 위해 외부망으로 나가는 더미 UDP 데이타를 프럭시 서버로 그 포트(10000)를 이용하여 실제 음성 데이타가 전송되기 전에 전송한다.

이 해결 방법에서도 1)단말 프럭시 방법에서 만나는 문제인 프럭시 서버에서 최종 목적지를 식별하는 문제를 해결해야 한다. 즉, 게이트웨이로부터 동일한 주소(프럭시 서버의 IP 주소)와 고정된 포트 번호(10000)로 들어오는 음성 데이타를 어떤 세션의 포트 번호(IP 주소는 NAT 라우터의 것으로 변환되므로 고려하지 않아도 됨)로 변환해야 하는 것인가를 결정해야 하는 것이다. 이를 해결하는 방법은 게이트웨이로부터 프럭시 서버로 오는 UDP 데이타그램의 발생지 포트 번호를 보고 세션을 구분하는 것이다. 이를 위해 프럭시 서버 내에 표 2와 같은 주소 변환표를 둔다. 주소 변환표는 게이트웨이에서 단말 노드로 전달하기 위한 것과 단말 노드에서 게이트웨이로 전달하기 위한 것 등 2 종류가 있다. 표 2는 그림 11의 예에서 생성된 단말 노드로 전달하기 위한 주소 변환 엔트리를 보여준다. 그 가운데 음영으로 되어 있는 8342가 위의 발생지 포트 번호의 예이다.

표 2 프럭시 서버 내의 주소 변환표

NAT Router		Gateway		Proxy Server
IP Address	Port Number	IP Address	Port Number	Port Number
130.102.1.1	3900	203.230.252.4	8342	7650

3) 음성 데이타 전송 프로토콜 변환

NAT 라우터와 게이트웨이 사이에 프럭시 서버를 두고, 단말 노드와 프럭시 서버 사이에 전달되는 음성 데이타를 위한 전송 프로토콜을 UDP에서 TCP로 변경하는 방법이다. 그리고 프럭시 서버에서 게이트웨이 사이의 전송은 기존의 UDP 프로토콜을 그대로 사용하는 것이다. 따라서 프럭시 서버는 게이트웨이 프럭시 역할을

하는 측면에서는 2) 게이트웨이 프럭시와 동일하다. 그러나 NAT 라우터를 통과하기 위해 TCP 프로토콜을 활용하는 점이 다르다. 이렇게 되면 단말 노드의 클라이언트 프로그램의 변경이 불가피하게 되는 단점이 있다.

4. 프럭시 서버 구현

3 장에서 제시된 NAT 문제 해결 방법 가운데 1) 단말 프럭시 방법의 구현에는 RTP/RTCP 패킷 헤더 정보까지 추적, 이용해야 하는 문제가 있다. 그리고 더 큰 문제는 상용으로 인터넷 전화 서비스를 제공하는 사업자 입장에서 모든 사설망에 프럭시 서버를 설치하도록 사용자들에게 강제하는 것은 현실적으로 전혀 적절하지 않다. 그 대신 공중 인터넷망에 프럭시 서버를 두어 그것이 게이트웨이의 프럭시 역할을 하도록 배치하는 것이 타당하다. 3) 프로토콜 변경 방법은 훨씬 복잡한 변환과 호 설정 과정을 거쳐야 한다. 이러한 이유로 해서 본 논문에서는 2) 게이트웨이 프럭시 방법을 구현하였다.

구현된 인터넷 전화 서비스 시스템 구조는 그림 12와 같다. 단말 노드는 NAT 라우터 뒤의 사설망에 있을 수도 있고, 공중 인터넷에 직접 접속해 있을 수도 있다. 본 논문에서 구현한 프럭시 서버는 공중 인터넷 내에 존재하고 NAT 라우터와 게이트웨이 사이에서 프럭시 역할을 수행한다.

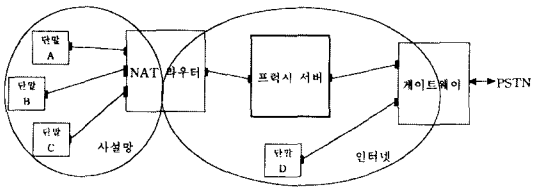


그림 12 게이트웨이 프럭시를 이용한 NAT 해결 인터넷 전화 서비스 구조

구체적으로 NAT 문제를 해결하기 위해 구현된 프로토콜과 프럭시 서버의 기능을 설명한다.

4.1 단말과 프럭시 서버 사이에 정의된 프로토콜

1) 프럭시 포트 번호(Proxy Port Number)

(1) 해설 : 음성 데이타를 송수신하는 프럭시 서버의 포트 번호를 전달하기 위한 메시지이다. 프럭시 서버는 이 포트를 통해 NAT 라우터와 음성 데이타를 주고받는다. 예를 들면, 그림 12에서 UDP 포트 번호 1950, 1952 이다. 음성 데이타의 송수신용 포트를 하나로 집중하는 것은 게이트웨이가 그렇게 하고 있고, 프럭시 서버가 게이트웨이 프럭시 역할을 수행하기 때문이다.

(2) 메시지 구조

필드 이름	바이트 위치
Proxy Port Number(0x0100)	0~1
Proxy Server IP Address	2~5
Proxy Server Port Number	6~7

- Proxy Server IP Address (Double Word)
  클라이언트가 접속하는 프럭시 서버의 IP 주소
- Proxy Server Port Number (Word)
  세션에 할당된 프럭시 서버의 음성 데이타 전달용 UDP 포트 번호. 이 포트 번호는 짝수로 함
  이유는 RTCP를 위한 UDP 포트 번호를 이 포트 번호의 다음 번호(홀수)로 지정하기 위함

(3) 메시지 전달 방향

- 프럭시 서버에서 클라이언트로 전달

2) 더미 UDP 데이타그램(Dummy UDP Datagram)

(1) 해설 : 단말이 프럭시 서버로 보내는 내용이 없는 UDP 데이타그램이다. 이는 실제 음성 데이타가 프럭시 서버에서 단말로 전달되기 전에 전송된다. 이것은 NAT 라우터가 프럭시 서버로부터 단말로 향하는 음성 UDP 데이타그램에 대한 주소 변환 정보 엔트리를 주소 변환표에 생성하게 하기 위한 것이다.

(2) 메시지 구조

필드 이름	바이트 위치
Dummy UDP Datagram(0x0101)	0~1
Dummy UDP data(0x5A5A...5A)	2~21

- Dummy UDP data(20 Bytes)
  클라이언트에서 프럭시 서버로 전달되는 아웃바운드 음성 데이타에 대한 NAT 라우터 내의 주소변환 정보 생성을 위한 UDP 데이타. 내용은 16진수 0x5A의 20번 반복값

(3) 메시지 전달 방향

- 클라이언트에서 프럭시 서버로 전달

3) UDP 경로 확인(UDP Path Confirmation)

(1) 해설 : 프럭시 서버가 단말에게 보내는 메시지로서 2) 더미 UDP 데이타그램을 프럭시 서버가 잘 수신하였다는 사실을 단말에게 알리기 위한 메시지이다. 이는 단말에게 NAT 라우터 내에 주소 변환 정보가 성공적으로 만들어졌음을 알리는 기능을 가진다. 숫자 0 또는 1을 가진다. 0인 경우, UDP 데이타그램이 정상적으

로 수신되지 못했음을 알리고, 1은 정상 수신을 뜻한다.

(2) 메시지 구조

필드 이름	바이트 위치
Path(0x0102)	0~1
State(0 or 1)	2

- State (Byte)

  더미 UDP 데이타 수신에 대한 상태 정보(0 또는 1)

(3) 메시지 전달 방향

- 프럭시 서버에서 클라이언트로 전달

4.2 프럭시 서버 기능

1) 게이트웨이와 호 설정 및 메시지 중계

단말을 대신하여 게이트웨이와 호 설정 작업을 수행한다. 기존의 단말과 게이트웨이 사이에 전달되는 H.232 메시지를 중계하는 역할을 한다.

2) 프럭시 서버 내에 주소 변환표 생성

음성 데이타를 송수신하기 위한 게이트웨이의 UDP 포트 번호를 얻는다. 이때, 게이트웨이와 음성 데이타를 송수신하기 위한 포트 번호를 할당하여 주소 변환표 내에 한 엔트리를 생성하여 게이트웨이 방향 값으로 기록한다. 단말 노드에서는 음성 데이타 송수신 포트 번호가 서로 다른 것으로 각각 지정되어 있다. 이 가운데 단말 노드로 오는 음성 데이타를 위한 포트 번호는 고정된 번호를 활용하는 제약을 가지고 있다. 이것들을 프럭시 서버에서는 하나로 처리하도록 게이트웨이에게 알린다.

3) 음성 데이타 단말 방향 전송 UDP 포트 설정

단말 노드로부터 더미 UDP 데이타그램을 수신한다. 이 데이타그램의 발생지 주소와 포트 번호를 주소 변환표 내의 단말 방향 값으로 기록한다. 이 주소(NAT IP 주소, 포트 번호)는 NAT 라우터에 의해 변환된 단말 노드의 음성 데이타 수신용 주소이다. RTP와 RTCP용으로 2개의 엔트리가 주소 변환표에 생성된다. 더미 UDP 데이타그램의 수신에 대한 응답으로 단말로 UDP 경로 확인 메시지를 송신한다.

4) RTP/RTCP 데이타 전달

단말과 게이트웨이 사이에 전달되는 음성 데이타를 위해 위에서 생성된 변환표에 의거 UDP 소켓을 생성한다. NAT 라우터와 상대하는 송수신용 UDP 소켓 2개와 게이트웨이 사이에서 송수신하기 위한 UDP 소켓 하나를 생성한다. NAT 라우터와 게이트웨이 등 양방향에서 수신되는 음성 데이타를 게이트웨이와 NAT 라우터로 각각 중계한다. 이때, 주소 변환표에 따라 송수신 IP 주소 및 포트 번호 변환이 일어난다.

4.3 적용 및 성능 평가

기존의 인터넷 전화 서비스를 위한 시스템을 기반으로 위의 기능을 추가 구현한 후 실제 상황에 적용하였다. 구현 환경은 클라이언트 시스템은 웹 기반 응용 프로그램으로 자바 애플릿(Java applet)으로 동작한다. 프럭시 서버는 리눅스(Linux) 시스템에서 구현되었다. NAT 라우터는 리눅스 시스템에서 제공되는 IP 마스크레이딩 기능을 활용하였다. 이는 일반 NAT 라우터보다 엄격한 NAT 기능을 수행하는 것으로 확인되었기 때문이다[9]. 일반 NAT 라우터인 경우, 인바운드 데이타에서 생성된 주소변환 정보에 따라서 동일한 출발지와 목적지를 가지는 아웃바운드 데이타(인바운드 데이타의 출발지가 목적지로, 목적지가 출발지로 되어 있는 것임)를 통과시킨다. 이에 반해, 리눅스의 IP 마스크레이드는 인바운드 주소변환과 아웃바운드 주소변환을 별도로 처리함으로써 비록 동일한 출발지와 목적지라 할지라도 각각 주소변환 정보가 생성되어야만 쌍방향으로 UDP 패킷을 통과시키는 점이 더욱 엄격한 점이다.

실험은 그림 13의 환경에서 이루어졌다. 실험 결과 정성적으로 음성 전달 상의 지연과 끊어짐 현상이 전혀 발견되지 않았다. 그리고 IP 스니프(sniff) 프로그램을 이용하여 전체 구간에서 송수신되는 IP 패킷을 모니터링하여 정량 분석하였다.

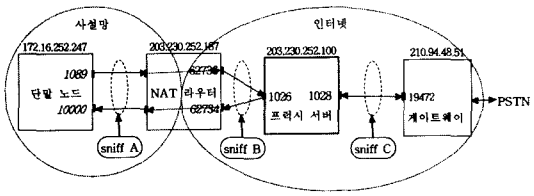


그림 13 구현된 프럭시 서버 동작 실험 환경

음성 전달 선로 상의 세 군데에서 IP 패킷을 모니터링하였다. 스니프 A, B, 그리고 C는 각각 단말 노드와 NAT 라우터, NAT라우터와 프럭시 서버, 그리고 프럭시 서버와 게이트웨이간에 송수신되는 IP 패킷을 수집하였다. 이를 면밀히 분석한 결과, 구현된 프럭시 서버가 단말 노드와 게이트웨이에서 각각 오는 음성 RTP/UDP 데이타그램을 IP 주소와 포트 번호 변환을 통해 빠짐없이 상호 전달함으로써 단말 노드에게는 게이트웨이 기능을, 그리고 게이트웨이에게는 단말 노드의 기능을 정확하게 수행하는 것을 검증할 수 있었다. 표 3은 스니핑 결과의 일부를 그대로 나타내었다.

표 3에서 Frame proto:0800은 Frame data가 IP 패

표 3 프럭시 서버 동작 실험 결과(스니핑 데이타)

A 지점 IP 패킷	B 지점 IP 패킷	C 지점 IP 패킷
Frame proto: 0800 IP proto: 11 00:e0:98:13:46:f0->00:50:cc:18:25:18 172.16.252.247[1089]->203.230.252.100[1026] 0000 80 04 37 f1 14 e2 d4 3f - b0 d8 66 57 a4 bc 5e 15 ..7....?..fW..^. 0010 35 12 23 fa 29 47 7a a2 - 48 0b 06 45 ba e7 05 25 5.#.)Gz.H..E...% 0020 c3 df 22 b0 bc 46 1d 31 - 01 20 4a 69 16 08 81 50 .."..F.1. Ji...P 0030 08 35 f5 d4 56 97 cc f8 - 48 07 b0 18 8c ba 46 70 .5..V...H.....Fp 0040 fe 92 06 59 81 03 91 92 - a0 65 c1 05 ac c1 96 51 ...Y.....e.....Q 0050 9c c1 f4 79 - ...y Frame proto: 0800 IP proto: 11 00:50:cc:18:25:18->00:e0:98:13:46:f0 203.230.252.100[1026]->172.16.252.247[10000] 0000 80 04 4f 0b 99 58 4b 81 - 18 99 1c 33 74 00 16 2f ..O..XK....3t../ 0010 7c 05 58 77 81 6b 08 70 - 38 1f ff 81 ac 12 31 09 |.Xw.k.p8.....1. 0020 00 d4 dc fc - .... Frame proto: 0800 IP proto: 11 00:50:cc:18:25:18->00:e0:98:13:46:f0 203.230.252.100[1026]->172.16.252.247[10000] 0000 80 04 4f 0c 99 58 4c 71 - 18 99 1c 33 f8 4e 8a 0e ..O..XLq...3.N.. 0010 20 37 80 63 ce 10 1c c6 c2 59 28 b1 fa 64 5f 0a 7.c.....Y(..d_. 0020 b7 5f ea b3 - ._..	Frame proto: 0800 IP proto: 11 00:90:08:00:75:e1->00:01:02:43:ea:7d 203.230.252.187[62736] >203.230.252.100[1026] 0000 80 04 37 f1 14 e2 d4 3f - b0 d8 66 57 a4 bc 5e 15 ..7....?..fW..^. 0010 35 12 23 fa 29 47 7a a2 48 0b 06 45 ba e7 05 25 5.#.)Gz.H..E...% 0020 c3 df 22 b0 bc 46 1d 31 - 01 20 4a 69 16 08 81 50 .."..F.1. Ji...P 0030 08 35 f5 d4 56 97 cc f8 - 48 07 b0 18 8c ba 46 70 .5..V...H.....Fp 0040 fe 92 06 59 81 03 91 92 - a0 65 c1 05 ac c1 96 51 ...Y.....e.....Q 0050 9c c1 f4 79 ...y Frame proto: 0800 IP proto: 11 00:01:02:43:ea:7d >00:90:08:00:75:e1 203.230.252.100[1026]->203.230.252.187[62734] 0000 80 04 4f 0b 99 58 4b 81 - 18 99 1c 33 74 00 16 2f ..O..XK....3t../ 0010 7c 05 58 77 81 6b 08 70 - 38 1f ff 81 ac 12 31 09 |.Xw.k.p8.....1. 0020 00 d4 dc fc - .... Frame proto: 0800 IP proto: 11 00:01:02:43:ea:7d >00:90:08:00:75:e1 203.230.252.100[1026] >203.230.252.187[62734] 0000 80 04 4f 0c 99 58 4c 71 - 18 99 1c 33 f8 4e 8a 0e ..O..XLq...3.N.. 0010 20 37 80 63 ce 10 1c c6 - c2 59 28 b1 fa 64 5f 0a 7.c.....Y(..d_. 0020 b7 5f ea b3 - ._..	Frame proto: 0800 IP proto: 11 00:01:02:43:ea:7d->40:00:82:10:10:0c 203.230.252.100[1028]->210.94.28.51[19472] 0000 80 04 37 f1 14 e2 d4 3f b0 d8 66 57 a4 bc 5e 15 ..7....?..fW..^. 0010 35 12 23 fa 29 47 7a a2 48 0b 06 45 ba e7 05 25 5.#.)Gz.H..E...% 0020 c3 df 22 b0 bc 46 1d 31 - 01 20 4a 69 16 08 81 50 .."..F.1. Ji...P 0030 08 35 f5 d4 56 97 cc f8 - 48 07 b0 18 8c ba 46 70 .5..V...H.....Fp 0040 fe 92 06 59 81 03 91 92 - a0 65 c1 05 ac c1 96 51 ...Y.....e.....Q 0050 9c c1 f4 79 ...y Frame proto: 0800 IP proto: 11 40:00:82:10:10:0c >00:01:02:43:ea:7d 210.94.28.51[19472] >203.230.252.100[1028] 0000 80 04 4f 0b 99 58 4b 81 - 18 99 1c 33 74 00 16 2f ..O..XK....3t../ 0010 7c 05 58 77 81 6b 08 70 - 38 1f ff 81 ac 12 31 09 |.Xw.k.p8.....1. 0020 00 d4 dc fc .... Frame proto: 0800 IP proto: 11 40:00:82:10:10:0c->00:01:02:43:ea:7d 210.94.28.51[19472] >203.230.252.100[1028] 0000 80 04 4f 0c 99 58 4c 71 - 18 99 1c 33 f8 4e 8a 0e ..O..XLq...3.N.. 0010 20 37 80 63 ce 10 1c c6 - c2 59 28 b1 fa 64 5f 0a 7.c.....Y(..d_. 0020 b7 5f ea b3 ._..

킷임을, IP proto:11은 IP data가 UDP임을 각각 나타낸다. 단말 노드에서 게이트웨이로 나가는 RTP/UDP 데이타그램은 RTP 헤더 12 바이트를 포함하여 84 바이트로 구성되어 있다. 따라서 단말 노드에서 발생한 음성 데이타는 72 바이트이다. 반면 게이트웨이에서 단말 노드로 들어오는 음성 데이타는 24 바이트이다. 이 크기들은 전화가 연결된 상태에서 항상 일정하다. 표 3에는 게이트웨이로 나가는 음성 데이타 1개 패킷과 연이어 들어오는 음성 데이타 2개 패킷을 보여준다.

단말 노드(172.16.252.247[1089])에서 발생되는 음성 데이타를 게이트웨이로 전송하기 위해서는 게이트웨이의 프럭시 역할을 하는 프럭시 서버(203.230.252.100[1026])로 전송한다. 이 데이타는 NAT 라우터에서 마스크레이딩되어 자신의 IP 주소와 이 세션(게이트웨이로 나가는 음성 데이타)에 할당된 포트(203.230.252.187[62736])로 생성지가 변경된 후 프럭시 서버로 전송된다. 프럭시 서버는 이 데이타를 수신하고, 이 세션에 할당된 게이트웨이와의 데이타 송수신용 UDP 포트(1028)로 데이타 생성지를 변경한 후 게이트웨이(210.94.28.51[19472])로 전송한다.

단말 노드로 들어오는 인바운드 음성 데이타 전송에 대해 두 가지 경우가 나타나 있다. 첫째 경우를 보면, 게이트웨이(210.94.28.51[19472])가 단말 노드로 간주하는 프럭시 서버(203.230.252.100[1028])로 전송한다. 이것을 수신한 프럭시 서버는 데이타의 발생지를 자신(203.230.252.100[1026])으로 하고, 단말 노드의 NAT 마스크레이딩 목적지인 NAT 라우터(203.230.252.187[62734])로 중계한다. 이는 NAT 마스크레이딩 표에 의거하여 실질적인 목적지인 사설망 내의 단말 노드(172.16.252.247[10000])로 목적지 주소가 변환된 후 전

달된다. 이 전화 세션을 위해 형성된 NAT 마스크레이딩 표와 프럭시 서버내의 주소 변환표를 각각 표 4와 표 5로 나타내었다.

표 4 프럭시 서버 동작 실험 결과(NAT 마스크레이딩 표)

in		out		masquerade
172.16.252.247	1089	203.230.252.100	1026	62736
172.16.252.247	10000	203.230.252.100	1026	62734

표 5 프럭시 서버 동작 실험 결과(프럭시 서버 내의 주소 변환표)

	NAT Router		Gateway		Proxy
단말 방향	203.230.252.187	62734	210.94.28.51	19472	1026
게이트웨이 방향	203.230.252.187	62736	210.94.28.51	19472	1028

본 논문에서 실제 구현한 게이트웨이 프럭시 서버는 표 6과 같이 다른 기법에 비해 성능 및 기능 측면에서 우월성을 가지고 있다.

5. 결 론

본 논문에서는 인터넷 전화 서비스에서 발생하는 NAT로 인한 음성 전달 상의 문제를 고찰하고, 그 해결책을 제시하였으며, 실제 그것을 구현한 결과를 설명하였다. NAT는 외부 인터넷과 사설망 사이에서 UDP 데이타를 전송할 때 문제를 발생시킨다. 이를 해소하기 위해서는 UDP로 전달되는 음성 데이타를 외부 인터넷으로부터 수신하기 전에 NAT 라우터 내에 주소 변환 정보를 생성시켜야 한다. 이를 NAT 라우터와 게이트웨이 사이에 프럭시 서버를 두어 해결하였다. 본 논문에서 해결한 NAT 문제는, 게이트웨이의 독특한 특성으로 인해 더욱 어려운 점이 있었다. 게이트웨이에서 발생하는 음성 데이타를 단말로 전송할 때, 사용하는 UDP 포트 번호가 모든 세션에 대해 동일한 점이다. 이런 특성으로 인해 단순한 NAT 라우터 내에서의 주소 변환 정보 생성만으로는 해결이 되지 않았다. 부득이 프럭시 서버가 게이트웨이에서 단말로 전송하는 음성 데이타를 대신 수신하여 그 데이타의 발생지 주소와 포트 번호로서 세션을 식별하여, 해당 세션에게 고유하게 할당된 NAT 라우터로 향하는 UDP 포트를 사용하여 NAT 라우터로 중계하였다. 그렇게 함으로써 NAT 라우터 내에서 해당 단말로 목적지 주소와 포트로 변환되어 최종적으로 전달되게 하였다.

이런 고유한 환경에서의 NAT 문제 해결로 인해 비공인 IP 주소를 할당받아 인터넷에 접속하는 모든 사용자들이 인터넷 전화 서비스를 제약 없이 이용할 수 있게 되었다. 나아가 인터넷 전화 서비스뿐만 아니라 UDP 전송 프로토콜을 사용하는 다른 응용에서도 위와 같은 해결 방식을 채택하는 것도 가능하다. 앞으로 인터넷의 활용이 폭발적으로 증가 추세에 있고, 인터넷을 이용한 상거래 등 사이버 경제 활동이 함께 증가되고 있다. 이에 따라 인터넷 보안에 관한 대비를 더욱 철저하게 시행하고 있다. 이런 맥락에서 설치되고 있는 방화벽[10]은 UDP 전송 프로토콜을 사용하는 인터넷 응용 서비스에게 또 하나의 장벽으로 작용한다. 이런 문제를 해결할 뿐만 아니라, 이 이외 인터넷 응용 서비스에도 본 논문에서 제시되어 있는 기법과 구현 기술을 적용하는 것이 향후 숙제이다.

표 6 게이트웨이 프럭시 기법의 성능 비교

	단말 프럭시 기법	전송 프로토콜 변환기법	게이트웨이 프럭시 기법
NAT IP/포트	변환된 NAT IP/포트를 게이트웨이에게 알려야 함. NAT 변환은 실제 음성 데이타가 발생해야 설정되는 것으로 그 값을 호 설정 시에 프럭시 서버가 알기 어려움	UDP에서 TCP로 변환 한 후 음성 데이타를 전송함으로써 재전송 등으로 인하여 실시간성이 떨어지고, 변환에 따른 프럭시 서버의 부담이 매우 큼	NAT에 의해 지정된 음성 데이타 전송용 NAT IP/포트를 게이트웨이에게 알릴 필요 없음. 따라서 게이트웨이와의 프로토콜을 신설할 필요 없음
동시 세션 지원	RTP 헤더 내용을 분석하여야 함	TCP 패킷 내에 RTP 데이타 전송함	NAT에 의해 이루어지므로 고려할 필요 없음
프럭시 서버 위치	사설망 내에 위치하므로 사설망별로 프럭시 서버를 각각 설치해야 함	공중 인터넷망에 설치하므로 여럿 사설망에서 공유하여 이용 가능함	공중 인터넷망에 설치하므로 여럿 사설망에서 공유하여 이용 가능함

참 고 문 헌

[1] U. Black, "Voice Over IP," Prentice Hall, 2000.
[2] 민재홍, 조평동, "VoIP 기술 동향", ETRI IT정보센터, 2001. 11.
[3] U. Black, "Internet Telephony Call Processing Protocol," Prentice Hall, 2001.
[4] A. B. Johnston, "SIP Understanding the Session Initiation Protocol," Artech House, 2001.
[5] D. E. Comer, "Internetworking with TCP/IP 4th Ed.," Prentice Hall, 2000.
[6] 김지영, "VoIP - H.323을 중심으로", 한국정보통신기술협회, 2000.10.
[7] T. Mittelstaedt, "Network Address Translation," Computer Bits, vol.7, No. 8, Aug. 1997.
[8] B. Douskalis, "IP Telephony The Integration of Robust VoIP Services," Hewlett-Packard Professional Books, Prentice Hall, 2000.
[9] D. Ranch, A. Au, "Linux IP Masquerade HOWTO," http://www.e-infomax.com/ipmasq/howto/m-html/ipmasq-HOWTO-m.html, May 2002.
[10] D. B. Chapman, E. D. Zwicky, "Building Internet Firewalls," O'Reilly, 1998.

손 주 영
1981년~1985년 서울대학교 계산통계학과 졸업. 1991~1993년 서울대학교 컴퓨터공학과 졸업(석사). 1993년~1997년 서울대학교 컴퓨터공학과 졸업(박사). 1985년~1998년 LG전자(주) 책임연구원. 1998년~현재 한국해양대학교 컴퓨터공학과 교수
관심분야는 인터넷 기반 멀티미디어 통신 프로토콜, VPN Ad-hoc network