# UDP 홀 펀칭과 경험적 홀 유지시간 탐색을 이용한 NAT 환경단말의 SNMP 원격 접속요청 메커니즘

## (A Remote SNMP Connection Request Mechanism for NATed Devices using UDP Hole Punching and Heuristic Hole Binding Time Search)

박 춘 걸 † 김 성 일 †† 정 기 태 ††† 이 영 석 ††††
(Choongul Park) (Seongil Kim) (Kitae Jeong) (Youngseok Lee)

**요 약** 공유기 사용자 수의 증가로 더 많은 IP단말들이 NAT 하위에 존재하게 됨에 따라 단말 관리 시스템은 알려지지 않은 NAT를 통과해서 단말에 SNMP 원격관리 명령을 전달하고 응답을 받을 수 있는 접속요청 메카니즘이 필요하게 되었다. 본 논문은 응용 프로그램에 대한 UDP Hole Punching 방법을 SNMP 프로토콜 상에서 적용하기 위해 관리 소프트웨어의 구조 및 동작의 단순한 변경, NAT 바인딩 정보 수집을 위한 관리객체(MIB)의 추가 정의를 통해 기존 연구가 가지고 있는 확장성 및 Symmetric NAT 문제를 비용 효율적인 방법으로 해결하였다. 더불어 Hole Punching을 위해 서버가 가지는 홀 유지시간 탐색 시간을 줄일 수 있는 개선된 방법을 제안하였다. 본 논문에서 제안하는 방법을 실 환경에 존재하는 22대의 사용중인 VoIP 단말에 적용하였으며, 실험을 통해 99%의 SNMP 원격접속 명령이 성공함을 보였고, UDP Hole 유지시간 탐색시간에 대한 25%의 향상을 보였다.

**키워드** : NAT 통과문제, 단말관리, UDP 홀 펀칭, SNMP, NAT 동작

***Abstract*** Recently, the NAT middlebox widely deployed in the home network environment prohibits DM operations from reaching user devices behind NAT. In this article, we focus on NAT issues to manage home network devices. Particularly, we discuss standardization efforts, and present our proposal to deploy DM services for VoIP and IPTV devices under NAT. By slightly changing behaviors of Simple Network Management Protocol (SNMP) Manager and Agent, and defining additional Management Objects (MOs) to gather NAT binding information, we could solve the NAT traversal problem under symmetric NAT. Moreover, we propose an enhanced method to search the UDP hole binding time of the NAT box. We applied our method to randomly selected 22 VoIP devices out of 194 NATed hosts in the real broadband network and have achieved 99% of the success ratio for exchanging SNMP request messages and 26% of enhancement for searching the UDP hole binding time.

**Key words** : NAT Traversal, Device Management, UDP hole punching, SNMP, NAT behavior

· 본 연구는 지식경제부 및 정보통신연구진흥원의 대학IT연구센터 지원사업의 연구결과로 수행되었음 (IITA-2008-C1090-0801-0016)

† 정 회 원 : KT 기술연구소 차세대망연구담당
lion@kt.com
†† 비 회 원 : KT 기술연구소 차세대망연구담당
sikim@kt.com
††† 비 회 원 : KT 기술연구소 차세대망연구담당 상무대우
kjeong@kt.com
†††† 정 회 원 : 충남대학교 컴퓨터공학과 교수
lee@cnu.ac.kr
(Corresponding author임)

논문접수 : 2008년 2월 12일
심사완료 : 2008년 6월 9일



정보과학회논문지: 정보통신 제35권 제5호(2008.10)

## 1. 서 론

인터넷 공유기는 하단(LAN 인터페이스)에 있는 다수의 IP단말에 사설 IP 주소를 할당하고 이를 사용자가 서비스 사업자로부터 부여 받은 하나의 공인 IP주소에 대응시키는 NAT(Network Address Translation) 기능을 제공함으로써 다수의 IP 단말이 인터넷을 이용할 수 있도록 한다. 그러나, 인터넷 공유기는 이러한 NAT의 사용으로 많은 장점을 제공하는 동시에 많은 결점을 가지고 있다. 이러한 결점 중 가장 큰 문제는 NAT가 외부로부터의 세션을 차단하는 방화벽 역할을 함으로써 인터넷을 통해 제공되는 응용 프로그램들이 동작하지 못하게 하고, 새로운 응용 프로그램의 배포를 어렵게 만드는 데 있다. 이러한 문제를 일반적으로 NAT 통과(NAT Traversal)문제 라고 부르며, 이를 해결하기 위해 STUN[1], ALG(Application Level Gateway)[2]등 다양한 방법들이 연구되고 있다.

단말관리는 일반적으로 원격에 존재하는 단말의 설정과 관리객체(Managed Object)를 관리하기 위한 방법으로, 무선 단말관리를 위해 OMA(Open Mobile Alliance)에서 표준화한 OMA-DM[3], 유선 단말관리를 위해 DSL(Digital Subscriber Line) Forum 에서 표준화된 TR-069[4], 라우터 및 스위치에 대한 관리를 위해 가장 많이 사용되고 있는 SNMP(Simple Network Management Protocol) 등이 단말관리를 위한 프로토콜로 흔히 사용되고 있다.

그러나, OMA에서는 NAT 하위에 존재하는 단말에 대한 관리를 위한 고려가 되어 있지 않으며, DSL Forum에서는 알려지지 않은 공유기 하위에 존재하는 단말을 관리하기 위해 부가적인 STUN서버를 이용하는 TR-111[5]이 제안되었으나 확장성 및 Symmetric NAT문제를 해결하지 못하였다.

한편, SNMP는 MIB에 대한 연산을 위해 SNMP 요청/응답 메시지와 트랩메시지를 UDP(User Datagram Protocol) 패킷에 실어 보내게 되는데, NAT 환경에서는 다른 응용 프로그램과 마찬가지로 NAT 통과 문제에서 벗어날 수 없다. 즉, 단말이 NAT 기능이 내장된 IP 공유기 하위에 존재하면, NAT 기능으로 인해 단말관리 시스템은 원격에서 사용자 단말에 명령을 전달할 수 없는 문제점이 있다.

따라서 본 논문에서는 알려지지 않은 NAT 하위에 존재하는 단말에 대해 원격에서 SNMP 명령을 전달하고 그 결과를 수신할 수 있는 효율적인 SNMP 접속요청 메카니즘을 제안하고자 한다. 이를 위해 2.1에서는 우리가 해결해야 할 문제를 정의한 후에 2.2에서는 NAT Traversal을 위한 기존연구 및 단말관리 표준에서 제안된 NAT 환경 단말에 대한 접속 메카니즘에 대해 살펴보기로 한다. 2.3에서는 문제해결을 위해 본 논문이 제안하는 방법에 대해 설명하기로 한다. 3장에서는 제안된 방법을 평가하기 위한 실험환경 및 분석결과를 보이고, 4장에서는 결론을 도출하고 향후 과제에 대해서 기술하고자 한다.

## 2. NAT 환경단말 SNMP 원격 접속요청 메커니즘

### 2.1 문제 정의

NAT는 내부로부터 시작되는 세션에 대한 타이머를 유지하고, 주어진 시간 동안 트래픽이 없으면 바인딩 정보를 삭제한다. 만약, 테이블에 존재하지 않는 외부로부터의 세션이 시작되면 NAT는 해당 세션을 차단한다[6]. 이 때문에 그림 1과 같이 NAT 하위의 사설환경에 존재하는 단말에서 시작된 SNMP 트랩 메시지는 UDP 패킷에 실려 공인 망에 존재하는 단말관리시스템으로 전달될 수 있지만, 단말관리시스템으로부터 시작된 SNMP Get/Set 메시지를 담은 UDP 패킷은 NAT에 의해 막혀 단말에 전달되지 못한다.

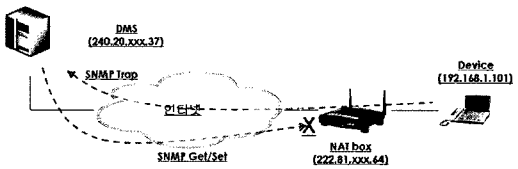


그림 1 단말관리시스템에서 NAT Traversal문제

이에 본 논문은 다음과 같은 두 가지 문제를 정의하고 해결하고자 한다.

첫째, 단말관리시스템은 알려지지 않은 공유기(NAT box) 하위에 존재하는 단말에 원격에서 접속 요청을 할 수 없다. 즉, 단말관리시스템은 수신된 패킷을 전송한 단말이 NAT 환경에 존재하는 단말인가를 판별하기 어려우며, 판별할 수 있다 하더라도 어떤 종류의 NAT가 존재하는 지도 알 수 없기 때문에 단말에 대한 접속 요청을 하는 것이 불가능하고, 공유기에 존재하는 NAT의 특성을 알기는 더욱 어렵다. 또한, 단말관리시스템이 원격에서 전송하는 SNMP 명령을 담은 UDP 패킷은 NAT에 의해 차단되어 단말에 전달되지 못한다.

둘째, NAT Traversal을 위해 사용된 기존 연구들은 SNMP 기반의 단말관리에 적용하기 어렵다. 즉, 기존 연구들이 제안하는 NAT Traversal 방법은 추가적인 서버나 Agent를 이용해야 하거나 모든 NAT의 업그레이드가 필요하기 때문에 단말관리시스템에 적용하기 위해서는 비용(Cost) 문제를 불러일으키며, 모든 종류의 NAT에서 적용 가능해야 하나 Symmetric NAT에서는

동작하지 않는 확장성(Scalability) 문제를 가지고 있다. 또한 기존에는 SNMP 기반의 단말관리 방법에 유연하게 수용될 수 있는 방법에 대한 연구가 없었다.

### 2.2 관련 연구

멀티미디어 통신, P2P 통신, 게임과 같은 응용에 있어서 서버와 클라이언트 또는 Peer와 Peer 사이의 경로상에 NAT가 존재함으로 인해서 발생하는 NAT 통과 문제를 해결하기 위해 많은 방법들이 연구되어 왔다. 그러나, NAT의 동작이 표준화되지 않았기 때문에 현재까지 나온 어떤 기술도 모든 NAT 환경에서 동작하지는 않는다[7].

ALG는 NAT 장치에 내장되어 어플리케이션 계층에서 동작하여 필요한 매핑을 수행한다. SNMP기반의 단말관리 프로토콜을 지원하기 위해 SNMP ALG는 기존 관리구조를 변경하지 않고 모든 NAT 통과문제를 해결할 수 있는 장점이 있으나, 이 방식의 문제점은 사용자들이 사용하는 모든 공유기를 SNMP를 지원할 수 있도록 업그레이드를 해야 하는데 이는 비용이 많이 들고 확장성 측면에서 문제가 있기 때문에 현실적으로 적용이 어렵다[8].

STUN은 Symmetric NAT, Cone NAT 등의 NAT 종류와 포트 매핑 정보를 검출할 수 있는 프로토콜이다. 사설망 내부의 클라이언트는 세션을 시작하기 전에 공인망에 존재하는 STUN서버에게 STUN 쿼리를 요청해 자신이 사용할 IP와 포트번호를 할당 받은 후, 세션과 미디어 트래픽 전송 시에 사용한다. 그러나 STUN은 공인망에 부가적인 서버를 두고 STUN 클라이언트를 단말에 추가해야 하므로 추가적인 비용이 필요하며, SNMP 프로토콜을 이용한 사설IP 환경 단말의 관리에 적용할 경우 단말관리서버와 단말 에이전트와의 연동 및 복잡한 절차가 필요하고 Symmetric NAT에서는 동작하지 않는 문제점을 가진다.

DSL Forum에서 TCP 기반의 단말관리 프로토콜인 TR-069를 홈 네트워크 단말의 원격관리에 응용하기 위해 제안된 TR-111은 NAT 환경에 존재하는 단말을 관리하기 위해 2가지의 방법을 제안하고 있다.

첫째는 단말관리 서버인 ACS(Auto-Configuration Server)가 NAT기능을 제공하는 게이트웨이와 하위 단말을 제어될 수 있는 환경에서만 적용 가능한 방법으로 DHCP 옵션을 이용하는 것이고, 둘째는 알려지지 않은 공유기 환경에서 적용 가능한 방법으로, STUN 서버를 사용한다. 하지만, STUN의 문제점인 부가적인 서버 및 Agent의 추가가 필요하며, Symmetric NAT에서는 동작하지 않는 문제점을 해결하지 못하고 있다.

SNMP와 같이 UDP를 기반으로 하는 응용 프로그램에 있어서 NAT 통과문제를 해결하기 위하여 가장 잘 알려진 방법으로 UDP Hole Punching [9] 방법이 있다. UDP Hole Punching 방법은 사설망 내에 있는 두 클라이언트가 알려진 공인 환경에 존재하는 랑데부 서버를 이용해서 Peer-to-Peer간 UDP 세션을 설정하기 위한 방법으로, NAT 내부의 사설 망 환경에서 시작된 UDP 세션에 의해 만들어진 홀(또는 바인딩, 세션)을 유지하기 위해 사설 망 환경에 존재하는 클라이언트가 주기적인 keep alive 메시지를 보내어 NAT에서 유지되는 바인딩 세션의 타임아웃 시간을 reset 하는 방법을 사용한다. 그러나, UDP Hole Punching 방법도 역시 공인 환경에 추가적인 랑데부 서버를 필요로 하며, UDP 프로토콜에 대해서만 적용이 가능하다는 단점을 가진다.

본 논문에서는 문제 해결을 위해 UDP Hole Punching의 개념을 적용하였으며, 기존 SNMP 구조의 일부 변경을 통해 UDP Hole Punching의 단점을 극복할 수 있도록 하였다. 표 1은 기존 NAT 통과방법을 본 연구에 적용하였을 때와 제안방법과의 비교이다.

표 1 기존 연구와의 비교

| 비교항목 | ALG | STUN(TR-111) | 제안방법 |
|---|---|---|---|
| SNMP 적용 | 가능 | 가능 | 가능 |
| 확장성 | 낮음 | 중간 | 좋음 |
| 비용 | 높음 | 높음 | 낮음 |
| 바인딩정보 획득 | 용이 | 복잡 | 단순 |
| 홀 유지시간 탐색 | 없음 | 보통 | 빠름 |
| DMS 변경 | 없음 | 복잡 | 단순 |
| Agent 변경 | 없음 | 복잡 | 단순 |
| Symmetric NAT | 해결 | 해결 못함 | 해결 |

본 논문이 제안하는 방법은 응용 프로그램에 대한 NAT Traversal 방법으로 잘 알려진 UDP Hole Punching 방법을 SNMP 프로토콜 상에서 적용하기 위해 관리 소프트웨어의 구조 및 동작의 단순한 변경, NAT 바인딩 정보 수집을 위한 관리객체(MIB)의 추가 정의를 통해 기존 연구가 가지고 있는 단점인 추가적인 서버나 Agent를 사용한 확장성 문제와 Symmetric NAT 문제를 비용 효율적인 방법으로 해결하였다.

NAT에서의 바인딩 테이블의 유지를 위해 알려지지 않은 공유기에 대한 UDP 홀 유지시간의 탐색이 필요한데, 이는 알고리즘의 성능에 따라 서버의 부하가 발생할 수 있다. 그러나, 기존 방법들은 Binary Search 방법을 사용한다고 명시되어 있으나, 상세한 절차는 언급되어 있지 않는 반면, 본 논문에서는 본 논문에서는 통계적 방법과 이진탐색 방법을 결합하여 UDP Hole 유지시간 탐색을 줄일 수 있는 향상된 방법을 제안하여 서버의 부하를 줄일 수 있도록 하였다.

### 2.3 제안 방법

1) UDP Hole Punching 개념의 적용

NAT는 내부에서 시작된 SNMP 트랩과 같은 UDP 세션에 대해 포트 변환을 수행하고, (SrcIP:SrcPort, DestIP:DestPort)에 대한 바인딩 테이블을 생성한다. 즉, UDP 홀이 NAT 환경에 있는 단말과 공인환경에 있는 단말관리 서버간에 생성된다.

따라서 단말관리 서버는 이 홀이 계속 유지시키기 위해 세션에 대한 타임아웃으로 바인딩 정보가 삭제되지 않을 정도의 간격으로 주기적으로 홀에 UDP 패킷을 전달하여야 한다. 이를 위해 SNMP 에이전트는 Keep-Alive 트랩을 주기적으로 홀을 통해 DMS로 전송함으로써 홀을 유지시키는 방법을 사용한다.

단말관리 서버는 이 홀을 이용하여 NAT환경에 있는 단말에 SNMP 명령을 전달하여야만 사설IP 단말을 관리할 수 있다.

2) SNMP 매니저/에이전트 구조 변경

SNMP 프로토콜을 통해 NAT환경에 존재하는 단말을 관리하기 위해서는 기존 SNMP 매니저와 에이전트의 구조 및 SNMP 에이전트가 관리하는 관리객체에 대한 추가적인 정의가 필요하다.

표 2에서 보는 바와 같이 SNMP 에이전트는 단말관리 서버가 단말이 NAT 환경에 존재한다는 사실을 판단할 수 있도록 주기적인 KeepAlive 트랩의 객체에 단말의 기본정보, IP 유형(고정, 유동), SNMP 에이전트의 로컬주소를 포함시켜 전송하도록 한다.

표 2 SNMP 관리객체

| SNMP Trap | | |
|---|---|---|
| NAME | OBJECTS | |
| KeepAlive | 단말기본정보, IP유형, IP주소 | |
| MIB(Management Information Base) | | |
| NAME | SYNTAX | ACESS |
| KeepAliveControl | Integer | R/W |
| KeepAliveInterval | TimeTicks | R/W |

SNMP 매니저가 그림 2와 같이 SNMP 에이전트가 전송한 트랩을 수신하면, SNMP 트랩에 포함된 OBJECT의 에이전트 IP주소와 IP 헤더의 주소가 다른 것을 보고 단말이 NAT 사설IP 단말임을 알게 된다. 이 때 수신된 트랩의 IP 헤더와 UDP 헤더의 주소를 통해 최종 주소변환을 수행한 NAT의 공인 IP 주소 및 사용한 포트를 수집하고, SNMP 메시지로부터 단말의 소스 IP주소를 알 수 있다.

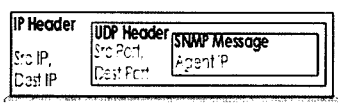


그림 2 SNMP 트랩 패킷 구조

3) Symmetric NAT 문제 해결

Symmetric NAT는 내부 IP주소와 포트로부터 특정 목적 IP주소와 포트로의 각 요청이 유일한 외부 소스 IP주소와 포트로 매핑되는 것으로, 같은 주소와 포트를 가진 내부 호스트가 다른 목적지로 패킷을 보내더라도 다른 매핑이 사용된다. 때문에 내부 호스트로부터 패킷을 수신한 외부 호스트만이 내부로 패킷을 전송할 수 있다.

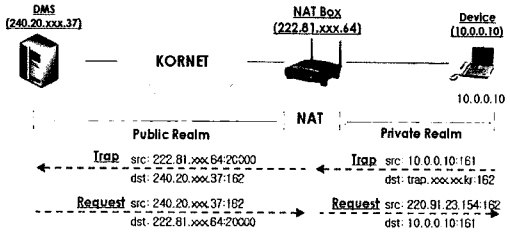


그림 3 Symmetric NAT 문제 해결

그림 3은 Symmetric NAT 문제 해결을 위한 것으로, SNMP기반 단말관리에서 단말은 일반적으로 SNMP 명령에 응답하기 위해 UDP 161번 포트를 수신대기 하고 있으므로, 외부의 단말관리 서버가 NAT 환경에 존재하는 단말에 SNMP 명령을 전달하기 위해서는 UDP 161번 포트에 대한 바인딩 정보가 NAT에 존재해야 한다. 하지만, 일반적으로 SNMP Trap을 전송할 때 소스 포트는 임의의 포트가 할당되므로, 본 논문에서 제안하는 방법은 Symmetric NAT 문제를 해결하기 위해 소스포트를 SNMP 명령 수신을 대기하고 있는 161번 포트로 고정해서 보내도록 해서 내부 사설IP 단말과 외부 단말관리시스템과의 바인딩 정보를 NAT에 확보할 수 있도록 한다. 또한, Symmetric NAT인 경우 NAT 내부에서 외부로 나가는 내부의 IP와 Port가 동일하더라도 목적지의 주소나 포트가 달라지면 NAT에서 바인딩 되는 포트도 달라지기 때문에 우리는 단말관리 시스템이 SNMP 트랩을 수신한 162번 포트로 SNMP 명령을 내리도록 SNMP 매니저를 변경하였다.

4) NAT 환경단말 원격 접속요청 절차

그림 4는 본 논문에서 제시하는 NAT 환경에 존재하는 단말에 대한 원격 접속요청 절차를 보여주고 있다. 단말은 공인 IP를 가지는 IP공유기(222.81.xxx.64)로부터 사설IP 주소(192.168.1.101)를 할당 받는다. 단말에 존재하는 SNMP 에이전트는 IP주소를 할당 받으면, 단말을 제어하기 위한 SNMP 제어포트인 161번 포트를 소스포트로 하여 단말관리시스템(240.20.xxx.37)으로 SNMP Trap을 전송한다. 이 때 SNMP 메시지의 내부에 자신의 IP주소(여기서는 사설IP주소인 192.168.1.101)를 포함시

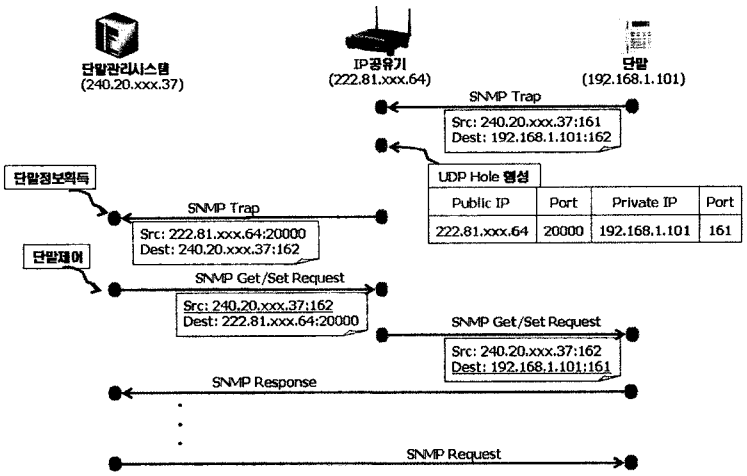


그림 4 NAT 환경단말 원격 접속요청 절차

켜서 전송한다. NAT는 내부에서 시작된 패킷에 대하여 IP와 포트변환을 수행하여, IP Header의 소스 IP주소가 공유기의 IP주소인 222.81.xxx.64로 변경하고, UDP Header의 소스포트가 NAT에서 할당한 20000번으로 바꾸어 단말관리시스템으로 전달된다. 여기서 NAT가 변경하는 UDP 헤더의 소스포트는 고정이 아니라 각 공유기의 특성에 따라 랜덤 혹인 연속적으로 포트가 할당된다. 즉, NAT에는 (222.81.xxx.64:20000, 192.168.1.101:161)의 UDP 홀(바인딩 테이블의 엔트리)이 생성된다.

단말관리 시스템은 SNMP 메시지에서 단말의 사설IP주소(192.168.1.101)를 얻고, IP Header및 UDP Header를 통해 공유기에서 생성한 UDP hole의 IP주소 및 포트(222.81.xxx.64:20000)를 얻어내어 비교하고 다르면 단말이 NAT 환경에 존재한다고 판단하고 정보를 관리한다. 단말관리시스템은 단말로부터 전달된 SNMP 트랩 메시지를 통해 단말의 사설IP, UDP Hole Punching에 이용할 공유기 포트, 공유기의 IP를 이용하여 단말의 SNMP 에이전트 제어 포트인 161번 포트로 SNMP명령을 전달한다.

이후 단말관리시스템은 단말을 제어하기 위하여 공유기의 NAT에 형성된 UDP 홀인 222.81.xxx.64:2000으로 SNMP 명령 메시지를 생성하여 전송하게 되고 이를 피하기 위해 소스포트를 162번으로 고정한다. 단말은 이 명령을 수신하여 응답을 단말관리시스템으로 전송한다. 여기서 NAT의 UDP Hole은 단말이 전송한 SNMP 트랩 메시지에 의해 생성된 것이며, IP공유기에 의해 (공인IP 주소:포트번호, 사설IP주소:포트번호), 즉 222.81.xxx.64:20000, 192.168.1.101:161)형태로 유지된다.

5) UDP 홀 유지시간 탐색

일반적으로 NAT 내부에서 시작된 UDP 패킷에 의해 생성된 UDP 홀(바인딩정보)의 유지시간은 표준화가 되어 있지 않기 때문에 제조사의 NAT 구현방식에 따라 다양하게 존재한다.

공인 망에 존재하는 단말관리 시스템이 NAT 환경에 있는 단말에 대한 원격관리가 항상 가능하도록 하려면 1)에서 설명한 바와 같이 단말이 UDP 홀이 닫이기 전에 주기적으로 패킷을 전송해야 한다. 이를 위해 단말관리시스템은 단말의 초기 접속 시 UDP 홀 유지시간을 탐색하여 그 값을 단말에 설정해 주어야 한다.

홀 유지시간의 탐색은 단말관리 서버가 수행하는데, 관리해야 할 단말이 늘어날 경우 서버에 부하를 줄 수 있기 때문에 효율적인 탐색 알고리즘이 필요하다. 표 3은 Hole 유지시간 탐색을 위해 사용 가능한 탐색 방법의 개념을 나타내는 것으로 STUN 서버에서는 일반적으로 이진탐색 방법을 사용하는 것으로 알려져 있다.

본 논문에서는 시중에서 널리 유통되는 알려지지 않은 공유기의 수가 제한적이라는 사실에 착안하여 탐색된 홀 유지시간의 실험적 통계에 의해 상위 10개의 홀 유지시간을 리스트로 유지하고 먼저 통계 리스트에서 탐색한 후 이진탐색을 수행하여 확률적으로 탐색시간을 줄이는 방법을 사용한다.

## 3. 성능평가

### 3.1 실험환경

본 논문에서 제안하는 방법을 평가하기 위해 현재 운용중인 단말관리 시스템에 적용하여 실제로 알려지지않은 NAT 환경에 존재하는 VoIP 단말을 대상으로 실험하였다. 단말관리시스템의 OS는 IBM AIX 서버이며, SNMP 매니저를 구현하기 위하여 JAVA기반의 오픈

표 3 Hole 유지시간 탐색방법 개념

| 탐색방법 | 개념 |
|---|---|
| 선형 | 예측 값을 허용오차만큼 선형적으로 증가시켜 탐색 |
| Slow Start | 초기는 예측 값을 2배씩 증가시키고, 실패한 시점에는 선형 증가시켜 탐색 |
| 이진 | 탐색구간을 ½씩 줄여가며 탐색 |
| 경험적 | Hole유지시간 Top10을 리스트로 유지한 후, 확률이 높은 리스트 내에서 먼저 탐색 수행하고 예측 값과의 차이가 허용 오차범위에 들어오지 않으면, 그 사이에서 이진 탐색 |

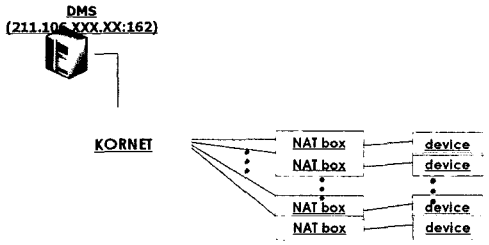


그림 5 실험 환경

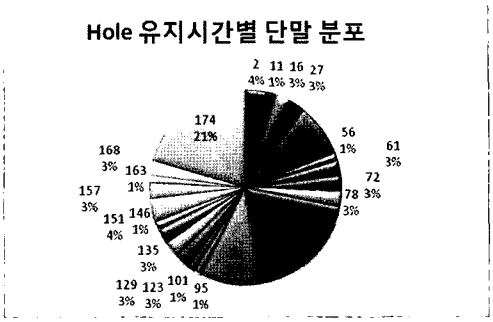


그림 6 이진탐색에 의한 홀 유지시간 별 단말분포

소스인 SNMP4J를 이용하였다.

SNMP 명령을 수행하는 SNMP 매니저는 그림 5와 같이 SNMP 매니저에서 하나의 포트(162번)로 SNMP Trap 수신과 SNMP 명령 및 응답 수신을 동시에 수행할 수 있도록 구현하였다. 또한 단말의 에이전트는 본 논문이 제안하는 단말관리를 위한 규격을 따르는 SNMP 에이전트로 구현하였으며, SNMP 트랩의 소스포트를 161번으로 하였으며, UDP 홀을 유지하기 위한 Keep-Alive 트랩을 주어진 주기로 전송하도록 구현하였다.

### 3.2 실험방법 및 결과

먼저, Hole Punching 방법의 적용 타당성 검증을 위해 Hole Punching 방법을 적용하지 않을 때와 Keep-Alive 트랩의 주기를 일반적인 NAT의 평균 Hole 유지시간인 180초 주기로 하는 정적 Hole Punching을 적용했을 때 명령의 성공률을 실험하였다. 표 4에서 보는 바와 같이 Hole Punching을 미 적용했을 경우에는 외부에서 단말로의 명령이 NAT에 의해 모두 차단되지만, 정적 Hole Punching을 적용하였을 때는 75%의 성공률을 보임으로써 본 논문의 제안이 타당함을 검증할 수 있었다.

두 번째로 Hole 유지시간의 반복성 확인을 위하여 Hole 탐색방법으로 흔히 사용되는 이진탐색 방법을 사용하여 실험하였다. 그림 6은 홀 유지시간 별 단말 분포를 나타내는 것으로 NAT의 유형에 따라 단말의 홀 유지시간이 다양하며, 그 중 84초, 90초, 174초의 홀 유지시간을 가진 단말이 많이 분포되어 있음을 보이고 있다. 이를 통해 우리는 실제로 시중에서 유통되는 공유기의 수가 제한적이고, 인기 있는 몇 종의 공유기가 대부분을 차지할 것이라는 우리의 가정을 뒷받침해 주고 있다.

이에 우리는 세 번째로 홀 유지시간 탐색방법의 개선을 위해 NAT Hole 유지시간 탐색을 통해 얻은 데이타를 기반으로 통계적 리스트를 만들고 리스트 내에서 이진탐색을 수행한 후 오차범위 내에 들어오지 않으면 이전 예측 값과 현재 예측 값 사이에서 이진탐색을 수행하도록 하는 통계적 방법을 사용하여 탐색시간을 측정하고, 다른 탐색방법과의 탐색시간 비교를 해 보았다. 그 결과 표 5에서 보는 바와 같이 단말 별 평균 탐색시간을 비교해 본 결과 통계적 탐색방법이 평균 탐색회수 2.3회, 평균 탐색시간 348초로 가장 우수한 것으로 나타났다.

표 6은 Hole Punching 방법을 적용하기 전과 180초의 정적, 단말 별 최적화를 통한 동적 Hole Punching을 적용했을 경우의 성공률 비교를 보여주고 있다. Hole Punching을 적용하기 전에는 NAT 환경에 존재하는

표 4 Hole Punching 적용 전후 명령 성공률 비교

| Hole Punching | 단말수 | 시험 | 성공 | 성공률(%) |
|---|---|---|---|---|
| 미 적용 | 22 | NA | NA | 0 |
| 정적(180초) | 22 | 2160 | 1636 | 75 |

표 5 탐색방법 별 평균 탐색시간 비교

| 탐색 방법 | 단말수 | 시험 회수 | 평균탐색 회수(회) | 평균탐색 시간(초) |
|---|---|---|---|---|
| 선형 | 22 | 196 | 25.6 | 4608 |
| Slow Start | 22 | 275 | 19.2 | 2984 |
| 이진 | 22 | 488 | 2.9 | 470 |
| 통계적 | 22 | 541 | 2.3 | 348 |

표 6 홀 펀칭 방법 별 평균 탐색시간 비교

| Hole Punching | 단말수 | 시험 | 성공 | 성공률 |
|---|---|---|---|---|
| 미 적용 | 22 | NA | NA | 0% |
| 정적(180초) | 22 | 2160 | 1636 | 75% |
| 동적 | 19 | 1221 | 1207 | 99% |

단말에 대한 SNMP 명령에 대한 응답을 수신할 수 없었지만, 정적 Hole Punching을 적용했을 때 75%의 성공률을 보였고, 각 단말 별 Hole 유지시간 탐색을 통한 최적화 적용 후에는 99%의 성공률을 보임으로써 본 논문이 제안하는 방법이 타당함을 증명하였다.

## 4. 결론 및 향후연구

홈 네트워크에서 공유기 사용자 수의 증가로 원격에서 NAT환경에 존재하는 단말의 관리를 위한 SNMP접속요청이 어렵다. 단말관리에 있어서 원격 접속요청의 어려움을 해결하기 위해 본 논문은 UDP Hole Punching을 응용한 단말 원격 접속요청 메카니즘을 제안하였다.

본 논문은 UDP Hole Punching 방법을 응용하여 NAT 환경에 존재하는 단말에 대한 원격 접속 요청이 가능하도록 하였으며, 또한 알려지지 않은 NAT의 Hole 유지시간 탐색을 위한 방법으로 통계적 방법과 이진탐색 방법을 병행한 방법을 통해 기존 방식에 비해 탐색시간을 향상 시킬 수 있음을 보였다.

본 논문에서 제안하는 방법을 실제 사용중인 VoIP 단말에 대한 실험을 통해 99%의 SNMP 원격 접속요청 명령이 성공함을 보였고, 경험적 탐색 방법을 통해 기존 연구들이 UDP Hole 유지시간 탐색을 위해 사용했던 이진탐색 방법과 비교해서 25%의 탐색시간 개선을 보였다.

향후에는 실험 대상을 증가시켜 홀 유지시간의 경험적인 수치를 확보할 필요가 있고, 실제 가장 많이 사용되는 공유기의 홀 유지시간을 측정하여 공유기의 탐지가 가능하도록 할 필요성이 있으며, 단말의 수 증가로 인한 홀 펀칭을 위해 발생하는 불필요한 트래픽 및 서버 부하를 줄일 수 있는 방안에 대한 연구가 필요하다.

## 참 고 문 헌


[1] D. Chaum, "Blind Signatures for Untraceable Payments," Advanvances in Cryptology-Proceeding of Crypto'82, Springer-Verlag, pp. 199-204, 1982.

[2] J. Rosenberg et al, "STUN-Simple Traversal of User Datagram Protocol through Network Address Translators," IETF RFC 3489, Mar. 2003.

[3] P. Srisuresh, M. Holdrege, "IP Network Address Translator (NAT) Terminology and Considerations," IETF RFC2663, Aug. 1999.

[4] Open Mobile Alliance, "OMA Device Management V1.2 Approved Enabler," Feb. 2007.

[5] Digital Subscriber Line Forum, "Technical Report-069 CPE WAN Management Protocol," Dec. 2006.

[6] Digital Subscriber Line Forum, "Technical Report-111 DSLHomeTMApplying TR-069 to Remote Management of Home Networking Devices," Dec. 2005.

[7] G. Huston, "Anatomy: A Look Inside Network Address Translators - Volume 7, Issue 3," Internet Protocol Journal, Sep. 2004.

[8] Newport networks whithepaper, "Solving the Firewall and NAT Traversal Issues for MoIP," Newport Networks, 2006.

[9] D. Raz, J. Schoenwaelder, and B. Sugla, "An SNMP Application Level Gateway for Payload Address Translation," IETF RFC 2692, Oct. 2000.

[10] B. Ford, P. Srisuresh, "Peer-to-peer communication across network address translators," USENIX Annual Technical Conference, 2005.



박 춘 걸

2001년 부산대학교 컴퓨터공학과 학사 2008년 현재 충남대 컴퓨터공학과 박사과정 재학중. 2002년~현재 KT 기술연구소 선임연구원. 관심분야는 차세대망운용관리, Device Management, Traffic Enginering

김 성 일

1992년 충북대학교 컴퓨터공학과 학사 1994년 충북대학교 컴퓨터공학과 석사 1994년~현재 KT 기술연구소 수석연구원. 관심분야는 차세대망운용관리, Device Management, Work Flow Management

정 기 태

1983년 경북대 전자공학과 학사. 1996년 일본 Tohoku Univ.전자공학과 박사 1986년~현재 KT 기술연구소 상무. 관심분야는 차세대망운용관리, Device Management, FTTH

이 영 석

1995년 서울대학교 컴퓨터공학과 학사 2002년 서울대학교 컴퓨터공학부 박사 2002년~2003년 University of California, Davis 방문연구원. 2003년~현재 충남대학교 전기정보통신공학부 컴퓨터전공 조교수. 관심분야는 차세대 인터넷, IPv6, 인터넷 트래픽 측정/분석