

---

# 순수 P2P를 위한 NAT 내부의 Relay Server 토폴로지에 관한 연구

손형도\* · 강승찬\*\*

A Study on Relay Server Topology inside NAT for Pure P2P

Hyung-doh Shon\* · Seung-chan Kang\*\*

## 요 약

최근 IPv4 주소의 고갈과 더불어 P2P 트래픽의 증가로 인해 NAT의 사용은 피할 수 없다. NAT 내부에 있는 서버는 외부의 릴레이 서버를 통해서만 접속이 이루어지는 속성을 가지고 있다. 따라서 NAT 외부에 있는 서버는 많은 자원을 소비하고 네트워크 트래픽을 증가시킨다. 본 논문에서는 NAT 외부에서 NAT 내부로의 세션을 형성할 수 있고, NAT 외부의 릴레이 서버를 NAT 내부에 둬으로써 네트워크 트래픽을 감소시킬 수 있는 토폴로지를 제안한다.

## ABSTRACT

Lately, the use of the NAT has become unavoidable with the increase of P2P traffic along with the exhaustion of IPv4 IP address. Due to NAT properties, NAT's internal host can only be connected through a relay method using the outside server. Accordingly, there is a lot of resource exhaustion of the relay server on the NAT exterior and network traffic increases. This essay proposes a topology that can form sessions to the NAT interior from the NAT exterior and that will decrease network traffic by placing NAT exterior relay servers in the NAT interior.

## 키워드

Pure P2P, NAT, Relay Server, IPv4

## I. 서 론

IPv4의 IP 부족 상태를 해결하고자 현재 IPv6로의 전환 및 연구가 활발히 진행되고 있지만 시간과 경비의 문제로 인해 IPv6로의 전환은 많은 시일이 필요할 것이다.

IPv4에서 IP 부족을 해결할 수 있는 방법으로 현재 광범위하게 사용되고 있는 방법은 NAT(Network Address Translator)를 이용하여 부족한 공인(public) IP를 사설

(private) IP로 맵핑(mapping)하여 여러 개의 사설 IP를 하나의 공인 IP로 전환하여 망을 사용한다.

그러나 NAT를 이용할 경우 NAT 외부에서 NAT 내부에 위치한 호스트로의 세션 연결이 불가능하여 NAT 내부에 각종 서버를 운영할 수는 없게 된다[1]. 그래서 NAT 외부에서 내부로의 세션 연결을 할 수 있는 해결 방법으로는 NAT 외부에 릴레이 서버를 두고 이를 이용하여 세션을 미리 연결한 상태에서 NAT 내부의 호스트에 세션

---

\* 한국폴리텍IV대학 아산캠퍼스

\*\* 한국기술교육대학교

을 연결하는 것이다. 이 방법은 네트워크 트래픽을 증가시키고 NAT 외부 서버에게 높은 성능을 요구하게 되는 문제점이 있다.

그리고 현재 네트워크 트래픽의 대부분을 차지하고 있는 것은 파일공유, P2P(Peer-To-Peer), 원격통신, 멀티레이어 온라인 게임등인데 이러한 응용을 사용하는데 있어 NAT 내부에 있는 호스트들은 NAT 외부의 서버를 이용할 수 밖에 없는 상황이다[2]. 그러므로 각종 애플리케이션들과 호스트의 성능은 점점더 높은 성능을 갖추고 있음에도 불구하고 별도의 서버를 사용하여야 한다는 문제점이 나타나게 된다.

이에 따라 본 논문에서는 NAT 외부에 있는 릴레이 서버를 제거하고, NAT 내부에 릴레이 서버를 들으로써 네트워크 트래픽의 감소와 NAT 외부에서의 내부로의 세션 연결을 가능하게 하여 순수 P2P 및 각종 애플리케이션의 성능을 충분히 발휘할 수 있도록 하는 새로운 토폴로지를 제안한다.

2장에서는 많은 네트워크 트래픽을 만드는 P2P에 대하여 알아보고, 3장에서는 NAT의 종류와 동작 그리고 기존의 NAT 외부에서 NAT 내부로의 세션연결 방법을 알아보고, 4장에서는 새로운 토폴로지를 제안한다. 마지막으로 5장에서 결론 및 고찰을 기술한다.

## II. P2P 고찰

### 2.1. P2P의 개요

P2P는 인터넷의 제3혁명이라 불릴 만큼 인터넷 사용에 큰 변화를 가져왔다. 호스트가 클라이언트 역할 중심에서 서버 역할로의 이동으로 인터넷을 수평적 구조로 변화시켰다. 이미 P2P 트래픽이 웹 트래픽을 넘어선 상태이다. 이에 따라 P2P 트래픽 문제가 가장 큰 이슈이다.

P2P는 중앙집중식이 아닌 방식으로 주요 기능을 수행하기 위해 분산된 자원을 이용하는 시스템들과 응용들의 집합체이다. 또한 분산 컴퓨터 및 자원 공유(SETI@Home, Korea@Home 등) 뿐만아니라 그리드(Grid) 컴퓨팅과도 비교가 된다. 그리고 협업(Collabration) 등에서 많이 사용되고 있다.

P2P 트래픽은 호스트가 서버와 클라이언트 역할을 동시에 수행함으로써 NAT 환경하에서는 P2P 트래픽의 원활한 흐름이 이루어지질 않는다.

## 2.2. P2P 네트워크 구조

### 2.2.1 혼합형(Hybrid) P2P 네트워크 구조

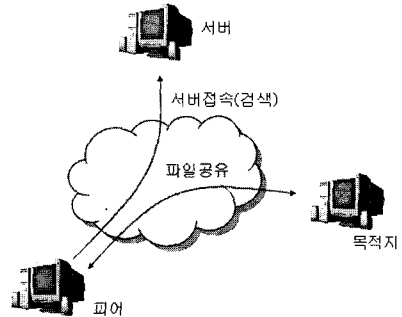


그림 1. 혼합형 P2P 네트워크 구조  
Fig. 1. Hybrid P2P Network Structure

그림1과 같이 혼합형 P2P는 중앙서버와 호스트 즉 피어(Peer)로 구성되어 있다. 중앙서버는 각 피어들간의 통신을 중재하는 역할 및 공유자원에 대한 메타데이터를 유지하여 자원 검색 및 기타 통신기능을 한다. NAT 구조하에서 보면 중앙서버는 NAT 외부에 있는 릴레이 서버로 볼 수 있다.

피어는 서버에 접속하여 자원을 검색한 후 서버의 개입 없이 직접 정보를 교환하게 된다. NAT 내부에 있는 피어는 NAT 외부에 있는 서버에 접속하므로 NAT 환경에서도 접속에 문제는 되지 않는다. 하지만 중앙서버에 지나친 로드(load)를 주게되고 트래픽이 집중되는 문제점이 있다[3].

### 2.2.2. 순수(Pure) P2P 네트워크 구조

그림2와 같이 순수 P2P는 서버와 클라이언트의 구분이 없고 모든 노드가 서버와 클라이언트의 역할을 수행한다. 즉 Ad Hoc 기반의 그룹 통신에 응용이 가능하며 추후에는 P2P 뿐만 아니라 모바일 분야[4]에서도 순수 P2P 형태의 네트워크 구조를 가지게 될 것이다.

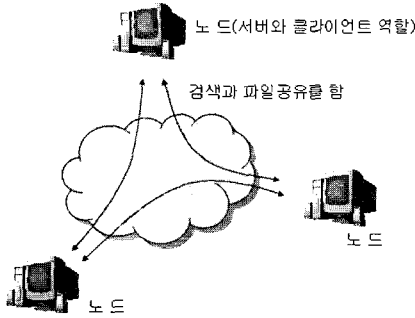


그림 2. 순수 P2P 네트워크 구조  
Fig. 2. Pure P2P Network Structure

순수 P2P 형태의 응용에서 노드가 공인 IP를 가지고 있다면 문제가 되지 않지만, IPv4의 IP 고갈 상태에서 NAT 환경을 사용한다면 NAT 내부에 위치한 노드로의 접근이나 디스커버리(Discovery)를 할 수 없는 상태가 됨으로 해서 순수 P2P 응용을 사용할 수 없게 된다.

### III. NAT에 대한 고찰

NAT는 IPv4의 IP 고갈 해결을 위해 다양하게 사용되고 있다. 그리고 현재 NAT는 클라이언트/서버 모델(웹 브라우저, 외부접속 응용등)에서는 전혀 문제없이 동작되고 있지만, P2P나 멀티레이어 온라인 게임 및 파일공유에서는 문제가 된다. 그 이유는 NAT 내부에 있는 호스트들은 공인 IP와 포트번호를 영구적으로 유지하지 못하기 때문에 NAT 외부에서 내부로의 세션 연결이 되지 않는다[5]. 반드시 NAT 내부에서 외부로의 세션이 연결이 되어야만 통신이 가능하다.

#### 3.1. NAT의 종류

NAT는 크게 Cone NAT와 Symmetric NAT로 구분된다. 첫 번째로 Cone NAT는 여러 개의 세션을 유지하기 위하여 포트를 재사용하며, 공인 IP와 포트번호를 사실 IP와 포트번호로 바인딩하여 통신이 되는 NAT이다. Cone NAT는 클라이언트의 포트번호를 유지한다.

두 번째로 Symmetric NAT는 여러 개의 세션을 유지하기 위하여 포트를 재사용하지 않는 NAT이다.

또한 Cone NAT는 수신된 UDP 트래픽을 어떻게 처리하느냐에 따라 다음과 같이 세가지로 나뉘어 진다.

- ① Full Cone NAT : NAT 외부로부터의 트래픽 중 공인 포트 번호와 대응되는 트래픽은 모두 NAT 내부로 트래픽을 전달한다.
- ② Address Restricted Cone NAT : NAT 내부에서 외부로 트래픽이 전송된 다음 외부에서 들어오는 트래픽 중 공인 IP와 대응되는 트래픽을 모두 NAT 내부로 전달한다.
- ③ Port Restricted Cone NAT : NAT 내부에서 외부로 트래픽이 전송된 다음 외부에서 들어오는 트래픽 중 공인 IP 및 공인 포트와 대응되는 트래픽을 모두 NAT 내부로 전달한다.

NAT의 종류를 구분함에 있어 Dynamic NAT 와 Static NAT로 구분을 하기도 한다. Dynamic NAT는 사실 IP N 개를 공인 IP 1개 또는 M개로 변환하는 outgoing NAT이고, static NAT는 공인 IP 1개를 사실 IP 1개로 고정시켜서 트래픽을 전달할 수 있는 incoming NAT이다.

#### 3.2. NAT 환경하에서 P2P 트래픽 통신 기술

NAT 환경하에서 P2P 트래픽을 처리하는 통신기술에는 다섯가지가 있다. 이 다섯가지 기술 모두 NAT 외부에 별도의 릴레이 서버를 두어 세션을 만들어 통신하는 방법이다[1].

##### 3.2.1. Relaying

이 방식은 가장 신뢰성은 있지만 비효율적인 방식이다. 마치 클라이언트/서버 모델과 같이 동작되며 NAT 내부의 호스트들은 NAT 외부에 있는 서버를 이용하여 세션을 연결한다. 항상 클라이언트의 세션이 연결되어 있는 장점이 있지만 서버의 높은 성능과 네트워크의 많은 대역폭을 요구하게 된다. 그림3은 Relaying 기법을 보여준다.

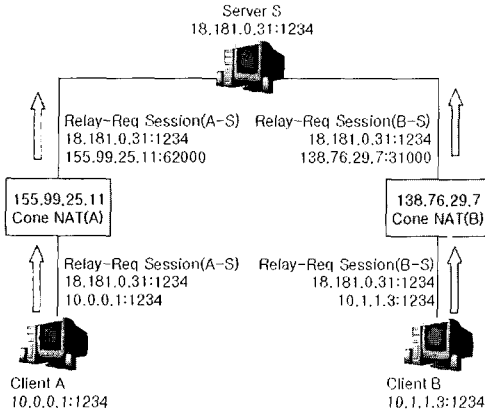


그림 3. Relaying  
Fig. 3. Relaying

클라이언트 A는 NAT A를 통하여 서버 S로 세션 연결을 하고, 클라이언트 B는 NAT B를 통하여 서버 S에 세션 연결을 한다. 클라이언트 A는 클라이언트 B와 연결하기 위하여 서버 S를 통하여 NAT B의 공인 IP를 얻어 직접 클라이언트 B와의 세션을 연결할 수 있게 된다.

### 3.2.2. Connection reversal

이 기술은 클라이언트 하나만 NAT 내부에 있는 경우에 공인 IP를 가진 클라이언트가 NAT 내부에 있는 클라이언트에 접속 시도를 하면 NAT는 접속 거절을 할 것이다. 그러면 접속을 실패한 공인 IP를 가진 클라이언트가 서버 S를 이용하여 “reversed” 메시지를 NAT로 보내면, NAT 내부에 있는 클라이언트가 Relaying 방식으로 서버 S에 세션을 연결한다. 그 다음에 양쪽 클라이언트는 세션 연결이 가능하게 되는 방식이다. 이 방식은 한쪽만 NAT 내부에 있는 특별한 상황에서만 사용 가능한 방법이다.

### 3.2.3. UDP Hole punching

이 방법은 UDP 패킷에 대하여 신뢰성 있게 동작되는 방식으로 Relaying 방식과 유사하다. 그림 4는 이 방법에 대하여 보여주고 있다.

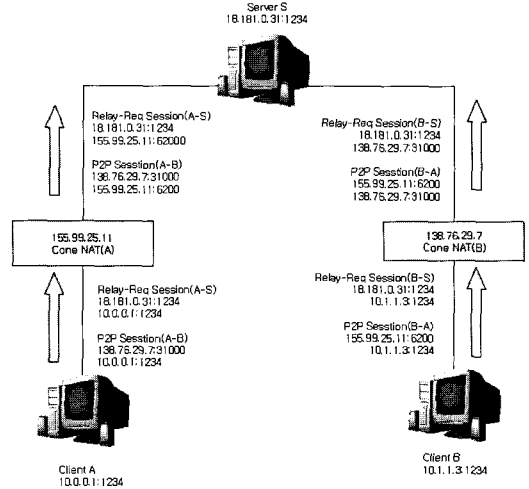


그림 4. UDP Hole Punching  
Fig. 4. UDP Hole Punching

클라이언트 A가 UDP 메시지를 NAT B의 공인 IP로 보내면, NAT B는 해당 메시지의 공인 IP 및 포트번호와 대응되는 것이 없으므로 해당 메시지를 받지 않는다. 그 다음 클라이언트 A는 서버 S와 클라이언트 B는 서버 S와 각각 Relaying 기법을 이용하여 세션을 연결한다. 마지막으로 클라이언트 A와 B는 P2P 트래픽을 위한 세션 연결에 성공한다.

이 방식은 여러개의 NAT가 중복이 되어 있는 경우, 동일한 NAT에 클라이언트 A, B가 모두 있는 경우 또는 한쪽 클라이언트만 NAT 내부에 있더라도 신뢰성이 확보된다.

### 3.2.4. UDP Port Number Prediction

이 방식은 세션이 연결된 포트번호에 +1을 하여 다음 세션을 위한 포트번호를 예측하는 방식인데 이방법은 문제점이 많아 추천되어 사용되지 않는다.

### 3.2.5. Simultaneous TCP OPEN

이 방식은 양쪽 클라이언트에서 동시에 SYN 패킷을 보내므로써 세션을 연결하는 방식이다. 하지만 이것은 시간적으로 동시에 되어야 함으로 문제점이 많아 추천되어 사용되지 않는다.

#### IV. NAT 내부에 있는 Relay Server Topology

3장에서 살펴보았듯이 Relaying이나 UDP Hole Punching 기법은 신뢰성은 있으나 NAT 외부에 별도의 서버를 두어 세션을 연결하는 방법이다. 이 방법들은 트래픽을 증가시키고 서버에게 높은 성능과 많은 대역폭을 요구하게 된다.

본 논문에서는 그림 5와 같이 릴레이 서버를 NAT 내부에 위치시키고, NAT와 내부 릴레이 서버는 고정(static)으로 할당하여 NAT 외부에서 들어오는 모든 패킷을 서버에서 처리하도록 구성하였다.

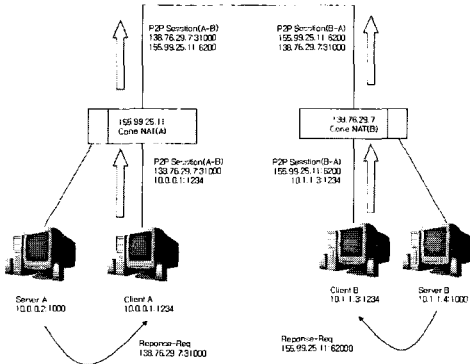


그림 5. NAT 내부에 있는 Relay Server Topology  
Fig. 5. Relay Server Topology Inside NAT

클라이언트 A는 클라이언트 B와 세션을 연결하기 위하여 NAT B의 공인 IP로 접속을 시도하면, 해당 패킷을 Server B에서 받아들여 세션 연결을 위해 Server B에서 클라이언트 B에게 "Response Request" 신호를 주어 클라이언트 B가 응답을 하도록 한다. 일단 클라이언트 B가 응답을 한 후에는 Server B의 개입없이 직접 클라이언트 A와 클라이언트 B는 통신을 할 수 있다. Server B는 NAT에서 처리할 수 없는 외부 트래픽에 대해서만 개입을 하여 처리하여 준다.

이러한 방식을 사용함으로써 NAT 외부에 서버를 두지 않아도 되므로 해서 Relaying이 필요없어지게 된다. 즉 트래픽도 감소하게 된다. 또는 NAT 외부에 있는 서버의 역할을 NAT 내부로 분산하여 기능을 수행함으로써 네트워크 속도도 향상시킬 수 있으며 순수 P2P와 같이 NAT 내부에서도 서버로서의 동작이 가능하게 된다. 또한 어떠한 NAT 상황(동일한 NAT에 클라이언트가 있는

경우, 다중 NAT 구성, 한쪽만 NAT가 있는 경우, NAT가 없는 상황등)에서도 신뢰성 있게 동작이 될 수 있다.

표1은 본 논문에서 제안하는 토폴리지와 기존의 방식을 비교한 것이다.

표1. 토폴리지 방식 비교  
Table 1. Comparison of Topology

방식	NAT환경	대역폭	외부 서버	신뢰성
Relaying	모든환경	대규모	있음	높음
Connection Reversal	특정환경	대규모	있음	낮음
UDP hole punching	모든환경	대규모	있음	높음
UDP port number Prediction	모든환경	소규모	없음	낮음
Simultaneous TCP OPEN	모든환경	소규모	없음	낮음
Relay Server inside NAT	모든환경	소규모	없음	높음

표1에서 보듯 본 논문에서 제안하는 방식이 모든 환경에서 소규모의 트래픽으로 외부 서버없이 신뢰성 있게 P2P 트래픽을 처리할 수 있는 것을 볼 수 있다.

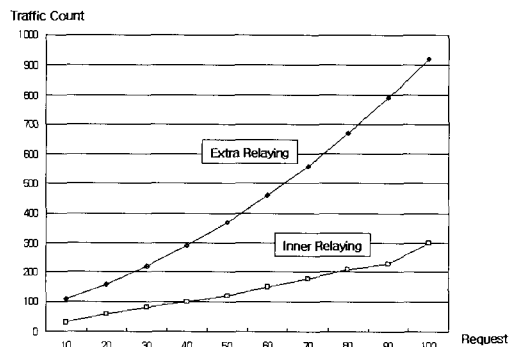


그림 6. 트래픽 분석  
Fig. 6. Traffic Analysis

그리고 그림6에서 보는 것과 같이 본 논문에서 제안하는 방식의 트래픽이 외부에 릴레이서버가 있는 경우와 비교하였을 경우 현저히 트래픽의 양이 감소됨을 알 수 있다.

V. 결 론

IPv4에서의 IP 고갈 상황을 극복하기 위하여 NAT는 다양하게 사용되고 있다. 현재 운영되고 있는 NAT는 클라이언트/서버 모델에서만 동작이 되도록 되어 있지만 순수 P2P, 파일공유등의 P2P 트래픽인 경우에 문제점을 만들어 낸다[6].

본 논문에서는 P2P의 네트워크 형태가 혼합형 보다 순수 네트워크 형태가 앞으로의 네트워크 구성 방향에 부합된다는 것과 NAT를 이용하여 P2P 트래픽을 처리하는 다섯가지 방법을 살펴보고, 이러한 다섯가지 방법은 모두 NAT 외부에 서버를 두고 Relaying 기법을 이용하여 세션을 연결하는 것이므로 많은 트래픽을 만들어 내게 되고, NAT 외부 서버에게 높은 성능이 요구되며, 네트워크 대역폭도 많이 필요하게 된다는 것을 확인하였다.

이에 따라 서버를 NAT 내부에 두어 트래픽 감소와 서버의 부하를 분산시키기 위한 새로운 토폴로지를 제안하였다.

NAT 내부에 서버를 두어 NAT 외부에 있는 서버의 기능을 분산하고, Relaying을 위한 트래픽도 함께 감소시켰다. 또한 본 논문에서 제안된 토폴로지는 어떠한 네트워크 구성에서도 동작이 가능하며, P2P와 같은 서버들을 NAT 내부에 위치시켜 사용할 수 있게 됨으로써 그 동안 NAT의 제한된 기능을 확장하여 사용할 수 있도록 하였다.

앞으로 P2P와 같은 응용에 적합하도록 애플리케이션이 작성되어야 겠으며, NAT 내부에서 "Response Request"를 보내기 위한 클라이언트 디스커버리(Discovery)기법등이 개발되어야 겠다. 더불어 NSIS(Next Steps In Signaling)등을 적용하여 NAT의 기능 확장 및 디스커버리등에 대한 연구가 진행되어야 할 것이다.

참고문헌

- [1] B. Ford, "Peer-to-Peer(P2P) communication across Network Address Translators(NAT)", Internet Draft, 2004.3
- [2] Melinda Shore, "Establishing Reachability Behind NATs", Internet Draft, 2004.9
- [3] D. Senie, "Network Address Translator (NAT)-Friendly Application Design Guidelines", RFC 3235, 2002.1
- [4] H. Levkowitz, "Mobile IP Traversal of Network Address Translation(NAT) Devices", RFC 3519, 2003.4
- [5] 김동성, "NAT/Firewall Traversal of VoIP Applications", 디지털웨이브, 2005.6
- [6] P. Srisuresh, "IP Network Address Translator (NAT) Terminology and Considerations", RFC 2663, 1999.8

저자소개



손 형 도(Hyung-doh Shon)

2006년 한국기술교육대학교  
박사과정 수료  
2001년~ 한국폴리텍IV대학  
아산캠퍼스 조교수

※관심분야: 홈네트워킹, 자바, 리눅스



강 승 찬(Seung-chan Kang)

1993년 한양대학교 전자공학과  
공학박사  
1993년~ 한국기술교육대학교  
정보기술공학부 교수

※관심분야: 인터넷워킹, 멀티캐스트