한국산학기술학회논문지
Vol. 5, No. 6, pp. 526-532, 2004

네트워크 주소변환 장치 구현

조태경[1*] · 박병수[2]

Implementation of Network Address Translator

Tae-kyung Cho[1*] and Byoung-soo Park[2]

요 약 IP 주소 부족 문제를 해결하고자 주소 필드의 길이가 대폭 확장되는 IPv6 라는 새로운 인터넷 프로토콜을 개발하게 되지만, 이러한 신 표준안을 인터넷에 실제로 적용하고 운영하기에는 많은 어려운 문제들이 남아있다. 그 대안으로 NAT(Network Address Translation)이지만 외부 망으로부터의 접근이 불가능하다는 특성을 가지고 있다. 이것은 보안 유지측면에서는 장점으로 작용하지만, 소규모 기업이나 사무실이 웹서버 나 메일서버 등을 사용하는 경우에는 외부에서의 접근이 허용되어야 하므로 단점이 된다. 본 논문에서는 이러한 단점을 극복하기 위하여 NAT 테이블에 수정을 가함으로써 사설망 내부의 특정 서버에 접근할 수 있는 확장된 개념의 NAT를 제안한다. 아울러 이러한 NAT 기능을 이용하여 구성된 사설망 간의 연결기능을 제공할 수 있는 방법을 제안함으로써 기존의 VPN(Virtual Private Network)의 일부 기능도 수용할 수 있도록 한다.

Abstract The insufficiency on IP address cause to develope a new internet protocol, IPv6 that the length of address field is expanded. But there are actually many problems on applying and operating this standard for internet. Though NAT(Network Address Translation) is instead of it, NAT has the characteristics that is not allowed to access from outside. This is a big merit in security but a week point because the access from outside should be allowed when a small organization operate web sever or mail server. Therefore, this paper proposes the expanded NAT which can solve such problems as modifying the table of NAT. Furthermore, the function of existing VPN(Virtual Private Network) will be acceptable partly through such a method that provide the linkage among VPNs.

Key Words : Network Address Translation, Virtual Private Network

1. 서 론

현재 인터넷에서 사용하고 있는 네트워크 계층 프로토콜은 IP 버전 4인데, 이러한 주소 부족 문제를 해결하고자 IP 주소 필드의 길이가 대폭 확장되는 IPv6라는 새로운 인터넷 프로토콜을 개발하게 된다. 그러나 이러한 신 표준안을 인터넷에 실제로 적용하고 운영하기에는 많은 어려운 문제들이 남아있어 그 대안으로 NAT(Network Address Translation)가 등장하게 된다. NAT 는 주소 할당 메커니즘을 이용하여 사설망의 IP 주소를 글로발망(Global Network) IP 주소로 변환시켜주는 기능으로서, 라우터나 방화벽 등에 내장되어 특히 IP 주소의 절약을 목적으로 사용된다. 최근 인터넷 방 등을 비롯한 SOHO(Small Office Home Office) 환경의 인터넷 사용자들이 늘어나면서 이러한 NAT 기능의 중요성은 점점 증가하고 있다[1-4].

그러나 이러한 NAT 기능은 외부 망으로부터의 접근이 불가능하다는 특성을 가지고 있다. 이러한 특성은 보안 유지측면에서는 장점으로 작용하나, 소규모 기업이나 사무실이 Web서버나 메일 서버 등을 두고 싶어 하는 경우에는 외부에서의 접근이 허용되어야 하므로 커다란 단점이 된다. 따라서 웹 혹은 메일서버를 구축하기 위해서는 이러한 서버를 NAT 기능의 외부에 설치하거나 인터넷 서비스 업체의 서비스를 받아야 한다. 이렇게 되면 사용해야 할 IP 주소가 증가하게 되거나 서비스 업체로 들어가는 비용이 추가로 발생하게 된다[5-6].

본 논문에서는 이러한 단점을 극복하기 위하여 NAT 테이블에 수정을 가함으로써 사설망 내부의 특정 서버에 접근할 수 있는 확장된 개념의 NAT를 제안하고자 한다. 또한 이를 실제로 구현하고 그 성능을 인터넷 사용 환경에서 측정함으로써 본 시스템의 활용도를 알아

[1]상명대학교 정보통신공학과
[2]상명대학교 컴퓨터시스템공학과
*교신저자: 조태경(tkcho@smu.ac.kr)

보고자 한다. 확장된 NAT 기능은 서비스 별로 한 개씩의 서버를 지정할 수 있으며, 이러한 특정 서버로의 접속 이외의 접속은 금하면서 외부에 알리고 싶은 서버는 내부에 둘 수 있게 된다. 결국 원하는 기능은 수행하면서 NAT IP 주소는 여전히 하나만 있으면 되는 것이다.

아울러 이러한 NAT 기능을 이용하여 구성된 사설망 간의 연결을 제공할 수 있는 방법을 제안함으로써 기존의 VPN의 일부 기능도 수용할 수 있도록 하였다. NAT를 이용하여 구성된 사설망은 상호 접속이 불가능하여 주로 외부 접속용으로만 사용된다. 따라서 지역적으로 떨어진 여러 개의 사무실을 갖는 회사에서는 따로 전용선을 이용 기업망을 구축하여 사설망을 구성하여야 한다. 그러나 이러한 방법들은 망 구축 시 소요되는 비용이 매우 비싸 VPN을 이용하여 구축하는 사례가 늘어나고 있다[7-8].

VPN은 전용선을 설치하는 것보다 비용이 적게 들고, 인터넷을 이용하여 사설망을 구성할 수 있다는 이점을 가지고 있다. 그러나 VPN은 매우 복잡한 암호화 알고리즘을 수행해야하고 다양한 Tunneling Protocol을 사용하여 구성이 되어야 한다. 따라서 VPN을 이용한 기업망의 구축은 ISP (Internet Service Provider)가 제공하는 서비스에 전적으로 의존할 수밖에 없다. 또한 이러한 복잡한 작업들의 대부분을 라우터에서 수행해야 하므로 장비에서의 성능 저하로 원하는 속도를 얻기가 어려워 아직까지는 VPN을 이용한 사설망의 구축이 활성화 되지 못하고 있는 실정이다[9-12].

본 논문에서는 이러한 단점을 해결하기 위해 NAT 테이블을 약간 수정하여 외부망의 패킷이 사설망의 내부에 접근할 수 있도록 제안한, 확장된 NAT를 이용하여 VPN을 구현하고자 한다. 확장된 NAT는 기존의 NAT에 약간의 수정만을 가하여 원하는 패킷만 사설망 내부에 들어올 수 있도록 한 것이기 때문에, 이를 이용하여 구현한 VPN은 추가 비용이 적게 들고 기존에 있던 공개망을 최대한 활용할 수 있다. 또한 간단한 방법으로 보안 프로토콜이나 암호화 알고리즘을 대체함으로써 속도도 빨라진다. 게다가 소프트웨어적으로 약간의 수정만 가함으로써 실제 인터넷 환경에 적용하기가 쉽다. 따라서 확장된 NAT를 이용한 VPN의 구현은 그 활용가치가 높을 것으로 사료된다.

2장에서는 NAT 기능 및 확장된 NAT 기능에 대해 설명하고, 3장에서는 사설망 연결 기능을 지원하기 위한 확장된 NAT기능에 대해 설명한다. 4장에서는 이러한 확장된 NAT를 구현한 시스템을 이용하여 인터넷 환경에서의 성능 측정 결과를 기술하고 5장에서 결론을 맺는다.

2. NAT(Network Address Translation)

NAT는 IP 주소가 부족해지는 상황을 극복하기 위해 나온 기능이다. 여기에는 여러 가지가 있으나, 그 중에서 m을 내부망 IP 주소의 수라고 하고, n을 NAT IP 주소의 수라 했을 때, m:n-translation, m, $n \geq 1$ and n=1 (m, $n \in N$) 인 경우를 가장 많이 사용한다. 이 경우에는 NAT IP 주소가 하나밖에 없으므로 여러 개의 접속을 위해, TCP 포트를 사용한다. 그리하여, 동시다발적인 접속은 이용 가능한 TCP 포트 번호 수에 제한된다.

이러한 NAT의 기능도를 그림 1에 나타냈다. NAT는 내부망에 있는 어느 호스트1에서 외부망의 다른 호스트

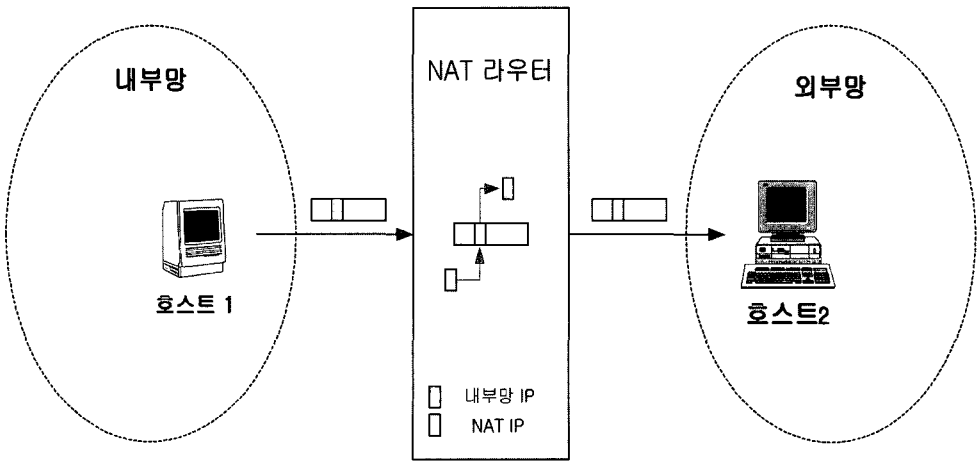

그림 1. NAT 기능도

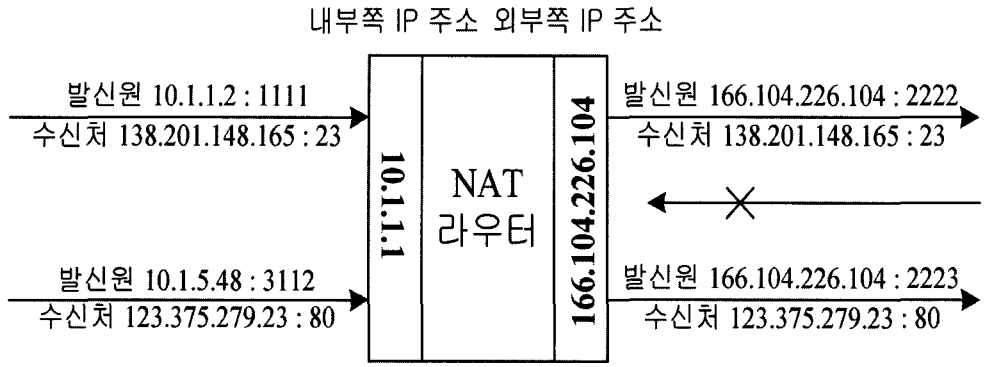

그림 2. NAT 개념도

그림 3. NAT 테이블

테이블

내부 IP 주소	포트 번호	로컬 NAT 포트 번호
10.1.1.2	1111	2222
10.1.5.48	3112	2223
.	.	.
.	.	.

2로 패킷을 전송할 때 내부망에서 사용하던 IP 주소를 NAT IP 주소로 바꾸어 보낸다. 이와 같은 형태를 가지고 있는 NAT는, 그것이 수행되어질 때 NAT 내부의 주소체계는 외부에 알려지지 않지만 모든 외부주소체계는 내부에 알려지게 된다.

그림 2는 NAT 내부망에서 NAT 라우터를 거쳐 외부망으로 접속이 이루어지는 것을 나타낸 개념도이고, 그림 3은 이 때 NAT 라우터에 생기는 테이블을 나타낸 것이다. 패킷은 이렇게 생기게 된 테이블을 참고로 하여 NAT 내부망과 외부망 사이에서 교환된다.

서버 접속기능을 갖는 NAT 기능 동작의 핵심은 NAT 테이블에 대한 수정을 가함으로써 우리가 원하는 특정서버로의 연결 요구 시 이를 적절히 처리하는 것이다[8]. 위에서 기술한 NAT 방식을 보면 알 수 있듯이, NAT 라우터의 외부 쪽으로 들어오는 패킷은 수신지 포트번호와 테이블의 local NAT port를 비교하여 같은 것이 있을 때에만 그에 관련된 데이터를 참고하여 들어올 수 있다. 그리고 우리가 NAT 내부에 달고 싶어 하는 서버는 특정한 몇 종류뿐이다. 그러므로 우리가 원하는 웹이나 메일, 텔넷 등의 서버에 관련된 포트번호를 NAT 테이블의 local NAT port에 고정시켜둔다면 그러한 특정서버를 목적하는 패킷은 들어올 수 있을 것이다. 물론 기존의 NAT 기능은 그대로 수행한다.

3. 제안한 NAT 기능

기존의 NAT 기능을 이용하는 경우에는 사설망은 또 다른 사설망과는 접속할 수 없다. 만약 2개 이상의 NAT를 이용한 사설망간의 접속이 가능하다면 VPN 형태의 운영도 가능할 것이다. 그리하여 앞에서 기술한 바와 같이, 확장된 NAT는 NAT 테이블을 약간 수정함으로써 받기 원하는 패킷만을 받을 수 있으므로 이를 이용하여 VPN을 구현할 수 있을 것이다. 본 논문에서 제안한 확장된 NAT를 이용하여 구현된 VPN의 형태는 다음의 그림 4와 같다. 이 그림은 NAT를 이용하여 구성한 10.1.100.X 네트워크와 10.1.200.X 네트워크가 연결된 모습이다.

3.1 사설망간 연결 테이블

사설망간 연결 테이블은 접속 하고자 하는 사설망의 네트워크 주소와 여기에 도달하기 위한 공인 IP 주소의 매핑으로 이루어지며, 망 관리자에 의하여 Static하게 구성된다. 즉, 망 관리자간의 사전 약속 및 조작에 의해서만 사설망 간의 연결이 이루어지도록 하였다. 앞의 10.1.100.X 네트워크에서 10.1.200.X 네트워크로 접속하기 위해서는 공인주소 210.1.1.1을 경유하여야 하며, 반대의 경우에는 200.1.1.1을 경유하여야 한다. 이 테이블은 실제 사설망간에 교환되는 IP 패킷이 NAT Router에 도달하면 Router에 의하여 참조되어 가상 IP 헤더 기능을 이용하여 인터넷으로 릴레이 된다.

3.2 확장된 NAT 알고리즘

기존의 NAT는 사설망에서 외부망으로 접근하기 위한 호스트의 주소와 포트번호를 참조하여 주소 변환을 수행한다. 이 경우 목적지 구소는 반드시 공인 IP 주소이어야만 한다. 사설망 간의 연결 시 목적지 주소는 미

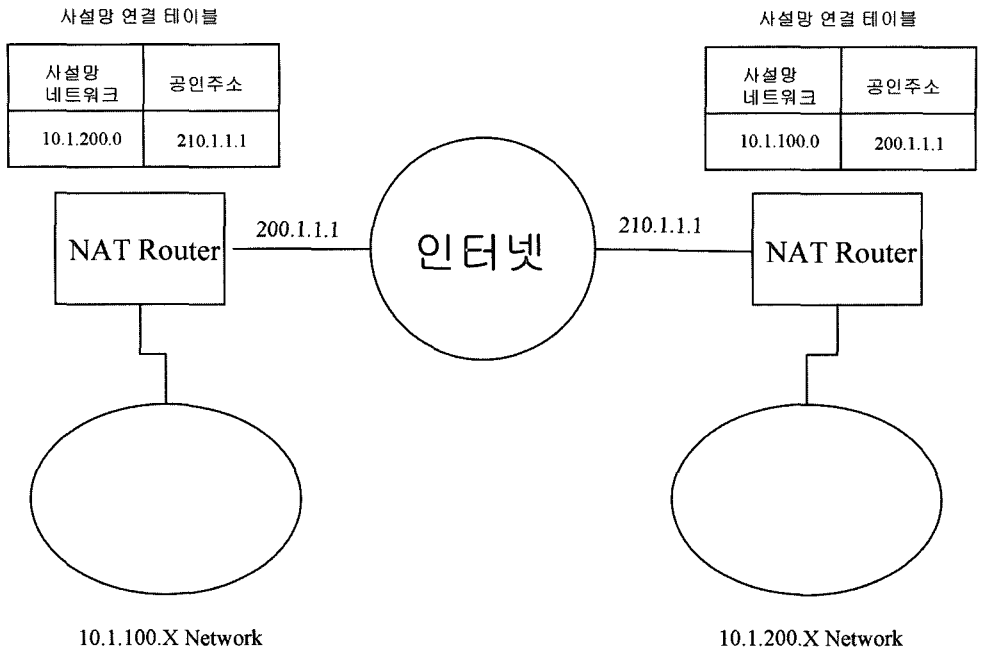

그림 4. 제안한 확장된 NAT를 적용한 VPN 구성도

리 약속 된 또 다른 사설망 주소이며, 사설망간 연결 테이블에 등록되어 있다. 다른 사설망으로 향하는 패킷이 도달하면 사설망간 연결 테이블을 참조하여 가상 IP 헤더 기능을 수행한다. 반대로 다른 사설망에서 패킷이 도달하면, 가상 IP 헤더의 기능이 역으로 수행된다. 즉, 확장된 NAT 알고리즘의 적용은 기존 NAT 테이블에 해당 항목이 존재하지 않으면서, 사설망간 연결 테이블에 항목이 존재하면 적용된다.

3.3 가상 IP 헤더

가상 IP 헤더는 사설망간 연결 기능의 핵심으로, 공인 IP 주소를 사용하여 가상의 IP 헤더를 생성하고, 이를 인터넷을 통하여 라우팅 하기 위하여 원래의 사설망간 IP 패킷을 Encapsulation 하는 과정을 말한다. 가상 IP 헤더의 구성은 목적지 IP 주소는 사설망간 연결 테이블에서 얻으며, 발신지 IP 주소는 NAT Router에서 얻을 수 있다. 가상 IP 헤더의 각 필드 구성 시 데이터 길이와 Checksum은 새로 계산되어야 한다.

가상 IP 헤더는 사설망간 IP 패킷을 인터넷을 통하여 라우팅 하기 위한 목적 이외에도 복잡한 암호화 알고리즘을 사용하지 않고도 어느 정도 보안성을 유지할 수 있다. 즉, 원래의 IP 패킷이 새로운 IP 헤더 내에 Encapsulation 되므로 인터넷상에서 라우팅 될 때 원래의 내용이 쉽게 노출되지 않는다.

4. 성능 측정

본 연구에서 제안한 시스템의 실용성을 증명하고 성능을 측정하기 위하여 실제로 PC를 사용하여 서버 접속 기능을 제공하는 NAT 시스템을 구현 하였다. 또한 성능 측정 시 NAT를 사용하지 않은 경우와 비교 측정함으로써 본 시스템 성능의 객관성을 높였다.

4.1 시스템 구현

Linux에서 NAT의 기능을 구현하기 위하여 Kernel Space와 User Space에서 각각 작업이 이루어 졌으며, 각각의 Space에서 구현한 기능은 다음과 같다.

커널에서의 작업은 시스템의 성능에 많은 영향을 끼칠 수 있으므로 가능한 한 가장 작은 양의 작업을 수행하도록 코딩 하였다.

- IP Routing Enable: 기본적인 IP Routing 기능을 수행 함
- IP Filtering Enable: IP Filtering 기능을 수행 함
- NAT Table: 외부에서 특정 서버로의 접근을 허용하기 위한 NAT Table의 수정 작업 수행
- Aging Out 기능: Active 되었다가 사용하지 않는 Entry를 삭제 함
- NAT 기능: NAT Table 에 등록된 정보를 참조하여 패킷의 IP 주소를 변환 함

▶ Statistics 기능: NAT를 사용한 패킷들의 통계 자료를 저장 및 전송 함

▶ ICMP, FTP Proxy 기능: ICMP 와 FTP에 대한 처리를 수행 함

또한 User Space에서는 사용자의 편의를 위해 Menu 방식의 조작이 가능하도록 하였다.

▶ Configuration 기능: NAT 기능 및 IP 주소 등 필요한 각종 정보들을 구성 함

▶ Display 기능: 현재 구성되어 있는 구성 정보들을 Display 해 줌

▶ NAT Table List-up: NAT Table 에 등록되어 있는 Active List를 보여 줌

▶ Accessable Server List: 접근 가능한 서버 및 현재 지정되어있는 서버 List를 보여 줌

▶ Statistics 기능: NAT 기능을 사용한 패킷들의 통계자료를 보여 줌

4.2 시험 환경

본 연구에서 구현한 시스템의 성능을 객관적으로 측정하기 위하여 우선 네트워크의 트래픽은 실제 인터넷 환경에서의 측정이 가장 현실성이 있기 때문에 실제 인터넷을 사용하는 트래픽으로 시험하기로 하였다. 또한 이러한 트래픽 중에서 가장 트래픽 양이 많은 FTP를 사용하여 측정 하였다. 이의 시험을 위하여 FTP 서버용 워크스테이션 1대와 FTP Client 기능이 있는 PC 11대, 그리고 Hub 와 NAT 시스템이 동원되었다.

그림 5는 NAT 시스템을 사용하지 않은 일반 LAN 환경에서의 구성도이고, 그림 6은 본 연구에서 구현한 NAT 시스템을 사용한 환경에서의 구성도이다.

4.3 성능 측정 결과

본 연구에서 구현한 NAT 시스템의 성능 측정은 NAT 시스템을 사용하지 않은 일반 LAN 환경에서의 성능을 최대로 보고, 이 측정치와 비교하여 분석 하였

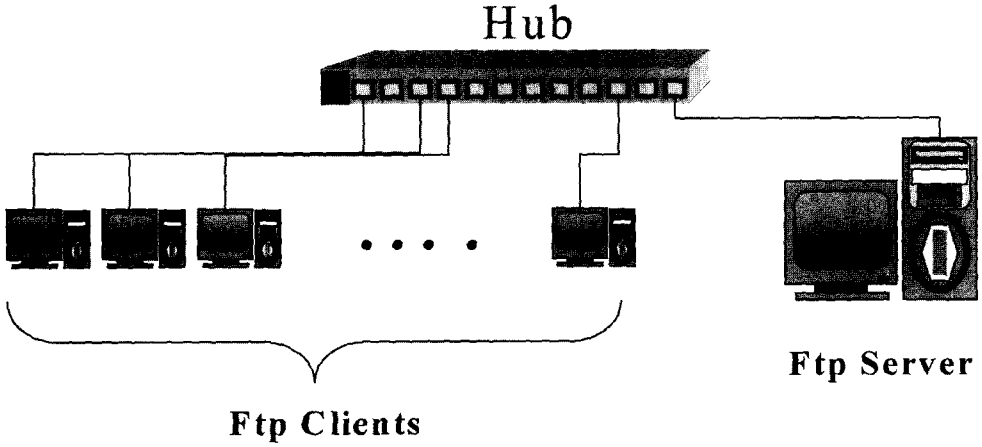

그림 5. 일반 LAN 환경에서의 구성도

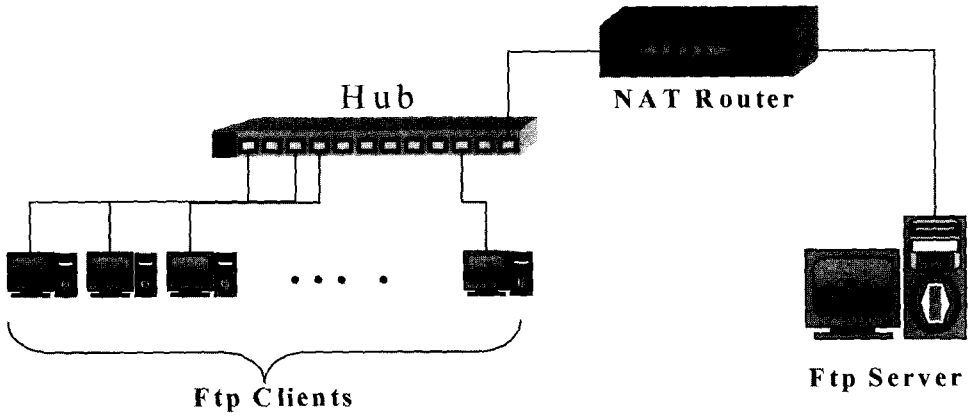

그림 6. NAT의 성능 평가를 위한 구성도

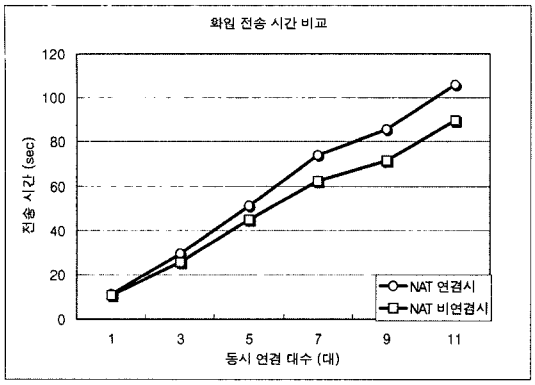

그림 7. 파일 전송시간

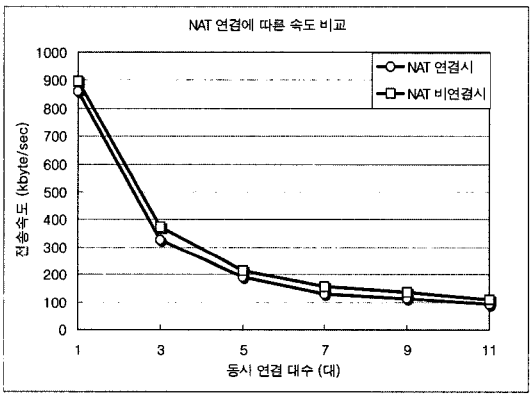

그림 8. 파일 전송속도

다. 또한 FTP Client도 1, 3, 5, 7, 9, 11 등으로 증가시키면서 측정 하여 노드 수의 변화에 따른 일반 LAN 과 NAT시스템을 사용한 경우의 성능을 비교 분석 하였다. 2가지 시험환경에서 사용한 FTP 서버와, PC, Hub 등은 동일한 것을 사용하여 시험의 객관성을 높였다.

시험의 측정치는 우선 FTP를 시행 하였을 때 파일이 완전히 전송되는 시간과, 이에 따른 전송속도(byte/sec)를 계산하였다.

그림 7은 시험 PC의 개수를 증가시키면서 측정한 파일 전송시간을 그래프로 나타낸 것이다. 그래프에서 살펴보면 노드의 수가 증가할수록 각 PC에서의 파일 전송시간도 역시 증가함을 볼 수 있다. 이는 LAN의 best-effort 전송특성에서 기인된 것으로 사료된다. 또한 NAT를 사용한 시험과 NAT를 사용하지 않은 일반 LAN 에서의 시험에서 약간의 차이가 남을 볼 수 있는데, 이는 NAT 기능을 수행하면서 발생하는 오버헤드이다.

그림 8은 이러한 시험을 수행하였을 때 각 PC에서 전송한 시간당 데이터의 양을 분석한 결과이다. 이 그

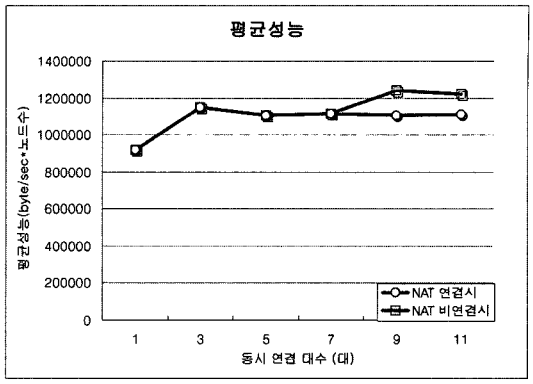

그림 9. 평균성능

래프에서도 알 수 있듯이 LAN에서는 노드의 수가 증가할수록 각 노드에서 전송할 수 있는 데이터의 양은 감소함을 알 수 있다. 또한 NAT를 사용한 시험과 사용치 않은 시험에서는 약간의 성능 차이가 나타나며, 이는 NAT 기능을 수행하면서 발생하는 오버헤드로 분석된다.

그림 9는 이러한 분석 결과를 토대로 하여 최종 정리한 망의 평균성능 값이다. 망에서 수행하는 성능은 모든 노드에서 발생한 데이터 양을 합산한 것으로 노드의 수가 변하여도 일정한 수치를 나타낸다. 또한 NAT를 사용하지 않은 환경에서의 성능과 비교하여 NAT를 사용하였을 경우에 약 3~4% 정도의 성능이 감소됨을 알 수 있다. 즉, 실제 환경에서 이러한 주소 절약 기능을 사용하더라도 큰 무리 없이 망을 구축하고 사용할 수 있음을 알 수 있다.

5. 결 론

최근 몇 년 동안의 인터넷의 발전 상황을 살펴보면, 앞으로 수 년 후의 상황을 예측하기 힘들 정도로 많은 변화를 보이고 있다. 인터넷 사용자의 수, 접속 호스트의 증가뿐만 아니라 망 접속 형태, 다양한 응용 프로그램, 등등 이제 인터넷은 마치 전화기와 마찬가지로 우리의 생활에 필수적인 기술로 자리 잡고 있다.

그러나 현재 인터넷의 표준 프로토콜인 TCP/IP는 기술적으로 몇 가지 문제점을 안고 있다. 그 중에서도 보안에 취약한 특성과, 주소 공간의 부족은 최근의 폭발적인 인터넷의 확산에 걸림돌이 되고 있는 실정이다. 이에 따라 많은 수의 인터넷 접속 시 방화벽이나 라우터 등에 NAT 기능 및 보안 기능을 탑재하여 망을 운영하는 형태를 취하고 있다.

본 연구에서 제안한 확장된 NAT 기능은 이러한 단

점을 극복할 수 있는 간단하면서도 매우 유용한 방법으로서, 향후 많은 적용이 이루어지리라 사료된다. 현재 인터넷 구성의 핵심 장비인 라우터나 방화벽 등에 쉽게 적용이 가능하며, 망 관리 방법 또한 매우 용이하게 이루어 질 것으로 사료된다. 특히 앞으로의 그 사용 형태를 예측하기 힘들 정도로 다양한 양상을 보이고 있는 소호 사용자들의 다양한 요구를 수용하는 데에 적절히 사용할 수 있을 것이다.

참고문헌

[1] K. Egevang, P. Francis, RFC 1631, "The IP Network Address Translator (NAT)", 1994

[2] K. Washburn, J. Evans, TCP/IP, Addison Wesley, 1994.

[3] Michael Hasenstein, IP Address Translation, 1997.

[4] Network Address Translation Technical White Paper, www.meridiansystems.com/nat-wp.html.

[5] Deering, S., and R. Hinden, RFC 1883, "Internet Protocol, Version 6 (IPv6) Specification", Dec. 1995.

[6] Gerich, E., RFC 1466, "Guidelines for Management of IP Address Space", May 1993.

[7] Stevens, W. R., TCP/IP Illustrated, Volume: The Protocols, Addison-Wesley, 1994.

[8] Eun-Sang Lee, Hyun-Seok Chae, Myung-Ryul Choi, "An Expanded NAT with Server Connection Ability", TENCON'99, 1999.

[9] Quality of Service for Virtual Private Networks, Copyright of 1999 Cisco systems, Inc.

[10] Implementing a Cisco Virtual Privat Network, Copyright of 1999 Cisco systems, Inc.

[11] members.tripod.co.kr/~goni02/vpn/neonet_misc01 .htm.

[12] http://members.iworld.net/wits/vpn/krnet99/index.htm.