TCP/IP 주소 변환 기능 구현
(Implementation of the TCP/IP Network Address Translation)

고 문 준 † 민 상 원 ††
(Moon-Joon Ko) (Sang-Won Min)

요 약 폭발적인 TCP/IP 단말의 증가로 가용한 IP 주소가 부족하여지고 있다. IPng (IP next generation)의 차세대 인터넷 프로토콜 방안이 이를 해결할 수 있는 적합한 방안이기는 하지만 적용 운용되기까지는 상당시간이 소요될 것으로 예상된다. 따라서 사설망과 공중 인터넷과 연결 기능 중 네트웍 주소 변환 (NAT : Network Address Translation) 방안이 과도기적이기는 하지만 차세대 인터넷 망이 활성화될 때까지 IP 주소의 고갈 문제를 해결할 수 있을 것이다. 본 논문에서 구현한 NAT 기능은 라우터에 할당된 공중 인터넷 주소를 이용하여 공중 인터넷 사용과 외부로부터 사설 망을 보호할 수 있는 기능을 제공한다. NAT 구현을 위해서는 제공하는 서비스의 사용 프로토콜을 파악해야 하며, 각 서비스 종류에 적합한 ALG (Application Level Gateway) 요구 사항을 분석하여야 하며 본 논문에서는 NAT 구현 과정에 필요한 사항을 구체적이고 체계적으로 제시하였다.

Abstract The major problem facing the Internet growth is the lack of the availability of network addresses. For solving a limitation on the current Internet, the IPv6 protocol and the IPv6 address scheme would be used as best solutions by the IP next generation (IPng) working group. However, it will take a long time to deploy the IPv6 proposal. Among current available solutions, the network address translation (NAT) method is considered as an appropriate solution in a time of transition period. In this paper, we focus on the NAT function, which provides the interconnection to the global Internet and the protection of a private network from a malicious invasion. In order to implement the NAT module into an Internet router, a detail protocol specification is investigated and the requirements for appropriate application level gateways (ALGs) are analyzed. Also, we present necessary modules and steps for implementing the NAT function in a detailed and systematical manner.

1. 서 론

네트워크의 모든 호스트들에 인터넷 IP 주소 할당을 유발하여 가용한 IP 주소 공간이 빠른 고갈을 초래하고 있다. 사용 가능한 IPv4 주소 한계로 인한 인터넷 연결 제한을 극복하고자 IP 주소 필드 길이가 대폭 확장되는 IPv6 (IP version 6)라 불리는 새로운 인터넷 프로토콜을 개발하였지만, 새로 제안된 표준안을 인터넷에 실제 적용, 운영하기까지는 수년이 걸릴 것으로 예상되므로 기존 IP 주소 형태를 연장하기 위한 방법이 필요하게 되었다.

· 이 논문은 1998년도 광운대학교 교내학술연구비 지원에 의해 연구되었음
† 비 회 원 : SJTEK(주) 전송연구소
mjko@sjtek.co.kr
†† 종신회원 : 광운대학교 전자공학부 교수
min@daisy.kwangwoon.ac.kr
논문접수 : 2000년 9월 8일
심사완료 : 2000년 10월 23일

인터넷 IP 주소 할당의 종류는 호스트 수에 기초하여 세 가지의 클래스로 주소 공간을 분리시키는 것으로 편의상 주소 클래스는 8bit단위로 구분되며 C 클래스는 약 250개, B클래스는 약 64,000개, A클래스는 약 1천6백만개의 호스트를 허용한다. 대부분의 기관들은 B 및 C클래스 정도를 가지고 있지만, B클래스의 상당 부분이 여유 주소 공간으로 낭비를 막기 위해 복수의 C클래스를 할당한다. 직접적인 인터넷 접속 호스트 대 비접속 호스트의 비율은 초대형 네트워크에서 대체로 1:1000에서 1:10,000정도이다 [1]. 그러므로 인터넷 접속을 원하지 않는 수많은 호스트들을 위한 유일무이한 IP 주소의 할당은 결과적으로 주소 고갈 문제를 더욱 악화시킬 것이다.

현재의 IPv4에는 인터넷 연결을 하지는 못하지만 네트워크 기능을 수행하는 사설 IP 주소 영역을 정의하고 있다. 1개의 A 클래스, 16개의 B클래스, 255개의 C클래스로 이들 주소는 인터넷과 직접적인 연결을 필요로 하지 않는

호스트들을 위해 쓰여질 것이다[2]. 사설 IP 주소를 이용하여 네트워크를 구성하게 되면, 인터넷 연결 기능을 갖지는 못하지만 네트워크 내부적으로는 다른 주소 영역과 똑같은 기능으로 사용될 수 있다. 따라서 사설 IP 주소 영역을 할당한 네트워크가 인터넷과의 연결 기능만을 갖게 된다면 기존 IP 체계를 한동안 유지할 수 있어 IPv4의 할당 주소 부족을 어느 정도 해결할 수 있다. 현재까지 사설망의 인터넷 접속 방법으로 Proxy server, DHCP, NAT 등의 제시되고 있다[3][4][5]. 그러나, 이와 같은 방법들도 IPv4의 가용한 IP 주소 부족 문제를 근본적으로 해결하지는 못한다.

Proxy Server는 호스트와 인터넷 사이에 놓인 장비로써 사용자가 어떤 작업을 위해 인터넷에 연결이 필요할 경우 Proxy Server가 인터넷과 연결하여 원하는 정보만을 요청한 사용자에게 되돌려 주는 것이다. Proxy Server는 응용 계층의 데이타만을 전달하는 것으로 네트워크의 설정에 혼잡성을 가중시키며 병목 현상이 발생할 수 있다. DHCP(Dynamic Host Configuration Protocol)는 한정된 개수의 인터넷 IP 주소들을 관리할당해 주는 프로토콜로 호스트가 인터넷 접속 시에 자동으로 인터넷 IP 주소를 할당하여 인터넷에 접속할 수 있게 해 준다. IP를 할당해 주는 서버에 전적으로 의존하기 때문에 서버가 다운되면 IP를 받을 수 없으므로 사설망의 모든 호스트가 인터넷을 사용할 수 없다.

NAT(Network Address Translation)는 재사용할 수 있는 사설망과 인터넷 사이에서 IP 주소를 변경하는 기능으로 자유롭게 사용할 수 있는 사설 IP 주소를 가진 네트워크가 인터넷에 연결할 수 있는 방법을 제공한다. 이로써 기존의 IP 주소 체제의 수명을 연장하면서 계속적인 인터넷 확장을 가능하게 한다. NAT는 데이타 링크 계층과 네트워크 계층 사이에서 이루어지기 때문에 응용 프로그램 및 TCP/IP와는 무관하게 동작되므로 어떠한 프로그램도 변경없이 기존 라우터에 직접 적용하여 사용할 수 있으며 인터넷이 사설망의 존재를 알 수 없어 Firewall으로도 사용할 수 있다. NAT는 인터넷의 모든 서비스에 대한 이해를 통한 TCP/IP를 기반으로 구현하며, 특히 사설망의 호스트 정보를 Payload로 전송하는 프로토콜에 대해서는 각 프로토콜에 적합한 ALG (Application Level Gateway)를 필요로 한다.

본 논문에서는 NAT 기능 구현을 위한 요구 사항 및 필요 모듈을 도출하고 구현에 필요한 상세 흐름도를 제시하였다. 그리고 상위 응용 서비스인 TELNET, FTP, WEB, PING 등의 서비스에서 필요한 ALG 구현의 요구 사항을 분석하였다. 그리고 본 논문에서 제시한 NAT와 ALG의 구현 요구 사항 및 흐름도를 기초로 라우터에 NAT 기능을 구현하고 시험 환경과 시험 과정을 제시하여 이 분야의 개발자들에게 도움을 주고자 하였다.

본 논문은 2장에서 NAT의 필요 기능과 요구 사항을 기술하고 3장에서 실제 구현 방법을 각각의 응용 계층 프로토콜에 따라 설명하였다. 그리고 4장에서는 NAT 구현 환경과 NAT를 사용한 시험 환경과 시험 결과를 보여주고 있으며 마지막으로 5장에서 결론을 보여준다.

2. NAT 기능

여러 네트워크에 재사용할 수 있는 사설 IP 주소를 갖는 패킷들은 라우터에서 통과되지 않아 사설망의 호스트들은 인터넷과 연결되지 않고 내부에서만 자유롭게 네트워크 기능이 수행된다[12]. 이러한 환경에서 NAT는 사설 IP 주소와 NAT가 보유하고 있는 인터넷 IP 주소 사이의 변환으로 사설망 호스트의 인터넷 접속을 가능하게 해 준다. NAT는 사설망 호스트가 인터넷에서 서비스를 받게 해 주는 것이 기본 기능이지만 인터넷에 서비스를 제공하는 확장 기능을 갖을 수도 있다[3][6].

TCP/IP는 인터넷에 접속하는 통신망의 프로토콜로 네트워크 억세스 계층 또는 네트워크 인터페이스 계층, 네트워크 계층, 응용 계층의 3계층으로 구성되어 있으며 IP는 TCP/IP 프로토콜중 가장 많은 역할을 수행하고 있는 프로토콜로서 TCP, UDP, ICMP에서 보낸 데이타를 모두 IP 데이타그램 형태로 전송한다. 한편, 라우터는 여러 개의 독립된 네트워크를 상호 연결시켜주는 상위수준의 네트워크 장비로 전송 패킷에 포함된 TCP/IP 주소를 근거로 하여 패킷을 전송한다. 따라서 인터넷과의 접속을 위해서는 인터넷 IP 주소를 갖는 패킷이 라우터를 통과하면 되는 것이기 때문에 데이타가 라우터로 전송되기 전에 TCP/IP 프로토콜 필드들을 정확하게 수정하여 전달하면 된다[7].

NAT에서는 공통적으로 TCP/IP 패킷을 해석하여 TCP/IP 프로토콜의 필드들을 변경할 수 있어야 하며 NAT 요구 사항의 범주에 따른 필요한 요소들을 갖고 있어야 한다. NAT의 IP 주소 할당 방식은 항상 일정한 사설 IP 주소와 인터넷 IP 주소가 대응되는 정적 할당 방식과 연결 설정이 발생할 때마다 대응되는 IP 주소가 바뀌는 동적 할당 방식으로 구분되는데, 동적 할당 방식에서는 NAT가 Address Pool에서의 IP 주소 할당 기능과 IP 주소 관리 기능을 갖고 있어야 한다. 또한, NAT Pool에 할당할 수 있는 인터넷 IP 주소가 한 개인 경우에는 인터넷 IP 주소는 항상 일정하게 할당되고 TCP/UDP의 포트 번호를 새로 할당하는 기능을 갖고 있어야 한다. 전달되는

패킷의 Payload에 사설망의 호스트 정보인 IP 주소와 TCP/UDP 포트 정보가 전달되는 경우에는 각각의 프로토콜에 따라서 할당된 IP 주소나 TCP/UDP 포트 정보로 변경할 수 있는 NAT ALG가 있어야 한다.

마지막으로 기존 기능의 NAT에서 확장된 NAT기능으로 인터넷 호스트가 사설망의 호스트에 접속을 시도할 때에는 사설망 호스트의 도메인 이름을 처리할 수 있는 도메인 네임 서비스 (domain name service; DNS) ALG를 갖고 있어야 하며 각 서비스 서버에 대한 설정을 NAT에 미리 할 수 있어야 한다.

NAT의 주소 변환 기능을 이용하여 최소의 인터넷 IP 주소로 사설망에 인터넷 접속을 제공하며, 인터넷에 사설망에 정보가 전달되지 않으므로 사설망의 존재를 알 수 없기 때문에 외부로부터의 접속을 막는 방화벽(Firewall)으로 사용할 수 있다. 또한 IPv6 네트워크를 기존의 IPv4 네트워크에 접속할 때에도 IPv6와 IPv4 사이의 IP 프로토콜의 변환을 수행할 수 있도록 응용하여 연속적인 네트워크 전이를 제공할 수도 있다[8]. NAT가 모든 패킷을 검사하게 되므로 TCP/IP 프로토콜에 따른 트래픽 분류를 통하여 네트워크 부하 균등 분배나 인터넷 QoS를 지원하기 위한 도구로도 활용할 수 있다.

3. NAT 구현 요구 사항

3.1 NAT 프로토콜 구성

NAT 라우터는 IP 계층과 데이타 링크 계층 사이에 NAT 기능을 위치시켜 사설망과 인터넷의 인터페이스로 입력되는 모든 패킷에 대해서 NAT를 수행하여 상위 계층으로 보내면 IP 계층에서는 정상적인 라우팅 작업만을 수행하면 된다. 그림1에서는 NAT 라우터의 프로토콜 계층 구성을 보여주며 인터넷과 사설망의 인터페이스인 서브넷1과 서브넷2로 패킷이 수신될 때의 NAT 실행 시점과 방향을 나타낸다. 라우터는 서브넷1 인터페이스에 수신된 패킷의 라우팅이 인터넷으로 전송될 때에 NAT를 수행하고 서브넷2 인터페이스에 수신된 패킷의 라우팅이 사설망으로 전송될 때에 NAT를 수행하며, 그 외에 경우에는 NAT를 수행하지 않은 정상적인 라우터 기능을 수행한다.

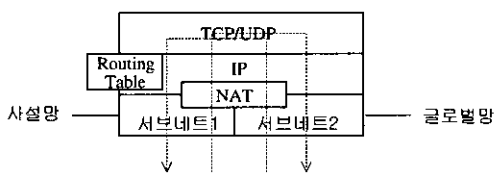


그림 1 NAT 라우터의 프로토콜 계층 및 패킷 진행 방향

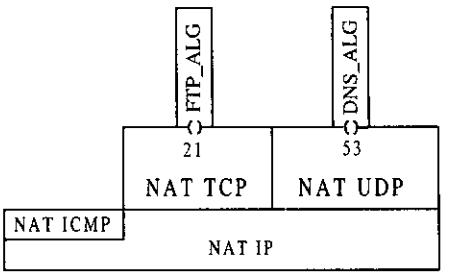


그림 2 NAT 구성 계층과 응용 프로그램에 따른 ALG

NAT 내부 구조는 기존의 TCP/IP 계층 구조와 유사한 형태로 구성되어 있지만, NAT 실제 처리 과정에서 볼 때는 가장 상위인 응용 계층에서부터 하위 계층으로 처리하도록 하여 상위 계층에서의 필드 변경이 하위 계층의 필드에 모두 반영되도록 해야 한다. 그림2에서는 NAT의 내부의 구성 계층과 각 응용 프로그램에 따른 ALG를 나타내고 있다. FTP나 DNS는 Payload에 사설망의 호스트 정보를 전송하는 경우가 발생하기 때문에 Payload의 호스트 정보를 처리하기 위한 ALG가 필요하지만 그 외의 TELNET과 같은 서비스는 Payload를 처리해야 하는 경우가 발생하지 않으므로 ALG가 필요없다[9][10][11].

3.2 NAT 라우터의 요구 사항 분석

기존의 라우터는 수신된 패킷의 목적지 IP 주소를 라우팅 테이블에서 찾아 그에 해당하는 포트로 패킷을 전송하는 기능을 갖고 있다. NAT는 기존 라우터를 변경하지 않고 적용하기 위하여 라우터의 각 포트로 수신되는 패킷을 중간에 가로채서 NAT 테이블에 저장된 IP 주소 맵핑 규칙에 따라 패킷의 TCP/IP 필드들을 적절하게 변경한 후에 라우터의 TCP/IP 계층으로 패킷을 전달한다.

NAT 라우터는 사설망과 인터넷에 대한 최소 한 개 이상의 인터페이스를 갖고 있어야 하고, 두 개 이상의 인터넷 인터페이스가 존재해도 공통의 NAT 테이블을 사용하도록 한다. NAT의 IP 할당 방식에는 여러 개의 IP 주소를 사용하는 방법과 한 개의 IP 주소와 Port 번호 할당 방법으로 구분할 수 있는데, 할당 가능한 IP 주소나 TCP/UDP 포트의 부족으로 인한 경우에는 패킷을 버리거나 ICMP 패킷(Host Unreachable)을 보낼 수 있어야 한다. 또한, NAT 라우터는 사설망의 구성 정보 및 라우팅 정보를 인터넷에 전송되지 않도록 해야 하고 인터넷에서 유입되는 모든 라우팅 정보는 라우터가 모두 보유하고 있어야 한다. 사설망에서 생성된 패킷을 수신하는 인터넷 호스트는 패킷을 생성한 호스트에 대한 MAC 주소를 모르기 때문에 ARP 패킷을 보내게 되는데, NAT 라우터는 ARP 패킷의 목적지 IP 주소가 자신의 보유 인터넷 IP 주

소와 일치하는 경우에는 NAT 라우터의 인터넷 IP 인터페이스 MAC 주소로 설정하여 응답해야 된다.

NAT 라우터가 NAT를 수행하기 위해서는 각 연결 정보를 저장할 수 있는 NAT 테이블을 갖고 있어야 한다. NAT 테이블에는 각 연결마다 근원지 IP 주소, 변환된 IP 주소(근원지 포트 번호, 변환된 포트 번호), 목적지 IP 주소, 어플리케이션 유형, Seq_Delta, 타이머 등을 저장하도록 하지만, 각 응용 프로그램에 따라 저장되는 필드가 변경될 수 있다.

FTP나 DNS처럼 ALG를 요구하는 응용 프로그램 경우에는 IP 주소가 변경되어 전체 데이타의 크기가 변할 때마다 TCP 헤더의 Sequence 번호와 Acknowledge 번호를 보정해 줄 수 있는 크기 변경 필드를 NAT 테이블에 저장하고 있어야 항상 정확한 TCP/IP 헤더가 유지될 수 있다.

NAT 테이블의 연결 정보 생성과 삭제는 동적으로 유지되기 위해서는 NAT 테이블에 존재하지 않는 새로운 연결 요청 패킷이 수신되었을 때에 인터넷 IP 주소와 새로운 포트 번호를 할당하여 패킷이 갖고 있던 TCP/IP 필드와 함께 NAT 테이블에 저장하도록 하여 새로운 연결 정보가 생성되게 하고, TCP 헤더의 Code 필드에 FIN bit가 설정된 패킷이 수신될 때 NAT 테이블의 연결 정보를 삭제하도록 한다. 물론 서버와 클라이언트간의 연결 자체에 문제가 발생하여 서비스의 진행이 일어나지 않는 경우와 UDP 헤더처럼 Code 필드를 갖고 있지 않는 경우에는 일정한 시간 경과 후에 해당 연결 정보를 삭제하도록 타이머 필드를 NAT 테이블에 설정하는 것이 필요하다. FTP와 TELNET처럼 TCP 연결을 요구하는 서비스의 타이머 설정은 15분(900초) 정도로 하고 PING과 같은 일회성 UDP 연결을 요구하는 서비스의 타이머 설정은 3분(180초) 정도로 한다.

NAT 라우터의 대부분은 사설망의 호스트가 서비스를 요청하는 경우만을 고려하지만 특별한 경우로 사설망 호스트가 인터넷 서비스를 제공하기 위해서는 NAT 테이블에 각 서비스에 적합한 사설망 호스트가 아래와 같은 표1 형태로 지정되어 있어 인터넷 호스트의 서비스 요청 패킷이 수신되었을 때 새로운 연결 정보를 생성,저장하지 않고 단지 패킷의 목적지 IP 주소를 NAT 테이블의 사설망 호스트 IP 주소로 변경하도록 한다.

표 1 사설망 호스트의 인터넷 서비스 제공시의 NAT 테이블의 예

근원지 IP	변환된 IP	어플리케이션 유형
150.150.56.35	10.1.1.2	ftp
150.150.56.35	10.1.1.3	telnet
150.150.56.35	10.1.1.4	HTTP

3.3 IP/TCP/UDP의 NAT 요구 사항 분석

NAT에서는 기본적으로 IP 헤더의 완결성을 보장하기 위하여 IP 프로토콜 버전과 헤더 checksum을 검사한다. IP 프로토콜 버전은 IPv4에 준하도록 4로 설정되어야 하고, 헤더 checksum은 전송되는 Payload (TCP 헤더와 실제 데이타)를 제외한 IP 헤더로만 계산된 것으로 계산 결과가 IP 헤더의 필드값과 차이가 없어야 하며, IP 헤더가 변경되면 그에 따라 IP 헤더 값의 합을 구하여 1의 보수를 취하는 방식으로 변경할 수 있어야 한다[12]. 전체 길이 필드(Total Length Field)는 IP 헤더 길이와 Payload 길이의 합을 나타낸 것으로 NAT가 데이타 내용을 변경하여 패킷의 길이가 바뀌면 이 필드도 길이 변경만큼 변경해야 한다. NAT는 사설망 호스트에서 수신된 패킷의 경우에는 목적지 IP 주소가 인터넷일 때 근원지 IP 주소를 NAT가 보유한 인터넷 IP 주소로 변환시키고 반대로 인터넷에서 전달된 패킷의 경우에는 목적지 IP 주소가 사설망일 때 목적지 IP 주소를 NAT 테이블에 저장된 해당 사설 IP 주소로 변환시킨다.

TCP/UDP 헤더 중 근원지 포트 번호와 목적지 포트 번호는 접속 양끝에 있는 응용 프로그램과 사용자를 구분하는 필드로써 인터넷 IP 주소를 하나만을 사용할 때는 사설망 호스트를 구별하기 위하여 사설망에서 전송하는 패킷의 근원지 포트 번호와 인터넷에서 전송하는 패킷의 목적지 포트 번호를 변경시킬 수 있어야 한다. TCP/UDP Checksum은 TCP/UDP 헤더와 실제 데이타로 계산된 것으로 헤더값이나 실제 데이타 내용이 변경될 경우 TCP/UDP Checksum을 다시 계산해야 한다. TCP/UDP Checksum 계산할 때에는 그림3과 같은 Pseudo IP 헤더도 포함시켜서 계산해야 한다[13][14]. 또한, NAT에서는 Payload에 사설망 호스트 정보가 포함된 경우에는 인터넷 IP 주소로 변경을 해야 하는데 그에 따라 데이타 패킷 길이가 변해서 Sequence 번호와 Acknowledgement 번호도 증가감소시켜야 한다. 이를 위해서는 Sequence 번호와 Acknowledgement 번호도 증감감소 크기를 NAT가 저장하고 있어야 한다.

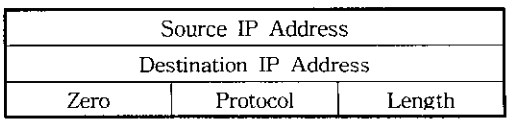


그림 3 Pseudo IP Header Format

4. 응용 서비스의 NAT 구현 요구 사항

4.1 TELNET/FTP/PING 서비스 시나리오

인터넷의 모든 서비스는 TCP/IP 상에서 제공되며 각 서비스는 TCP/UDP 포트 번호와 IP 프로토콜 번호가 정해져 있어 그에 따라 각 서비스를 구분할 수 있다[13][14][15]. 현재 FTP를 제외한 모든 인터넷 서비스는 한 개의 연결마다 한 개의 연결 정보를 저장해 놓으면 NAT 라우터가 해당 연결 정보를 사용하여 인터넷과의 연결에 이용한다. 인터넷 서비스는 TCP 혹은 UDP를 사용하는데, TCP/UDP의 모든 연결에 대하여 타이머 정보를 사용한 NAT테이블의 연결 정보 삭제가 가능하도록 한다. TCP 연결인 경우에는 연결 해제를 의미하는 패킷을 수신하였을때에도 연결 정보 삭제가 가능하도록 하고, UDP인 경우에는 단발적인 연결을 요구하므로 필요 정보의 수신 이후에 해당 연결 정보를 삭제하도록 한다.

그림 4와 그림 5은 NAT 라우터를 이용하여 사설망 호스트가 인터넷 서비스를 받기 위한 NAT 처리 시나리오를 사설망에서 인터넷으로 송신하는 경우와 인터넷에서 사설망으로 송신하는 경우로 나누어서 설명하고 있다. 사설망이 인터넷 서비스를 하기 위해서는 단지 NAT 테이블에 서비스 제공 호스트만을 설정해 놓고 그에 해당하는 IP 주

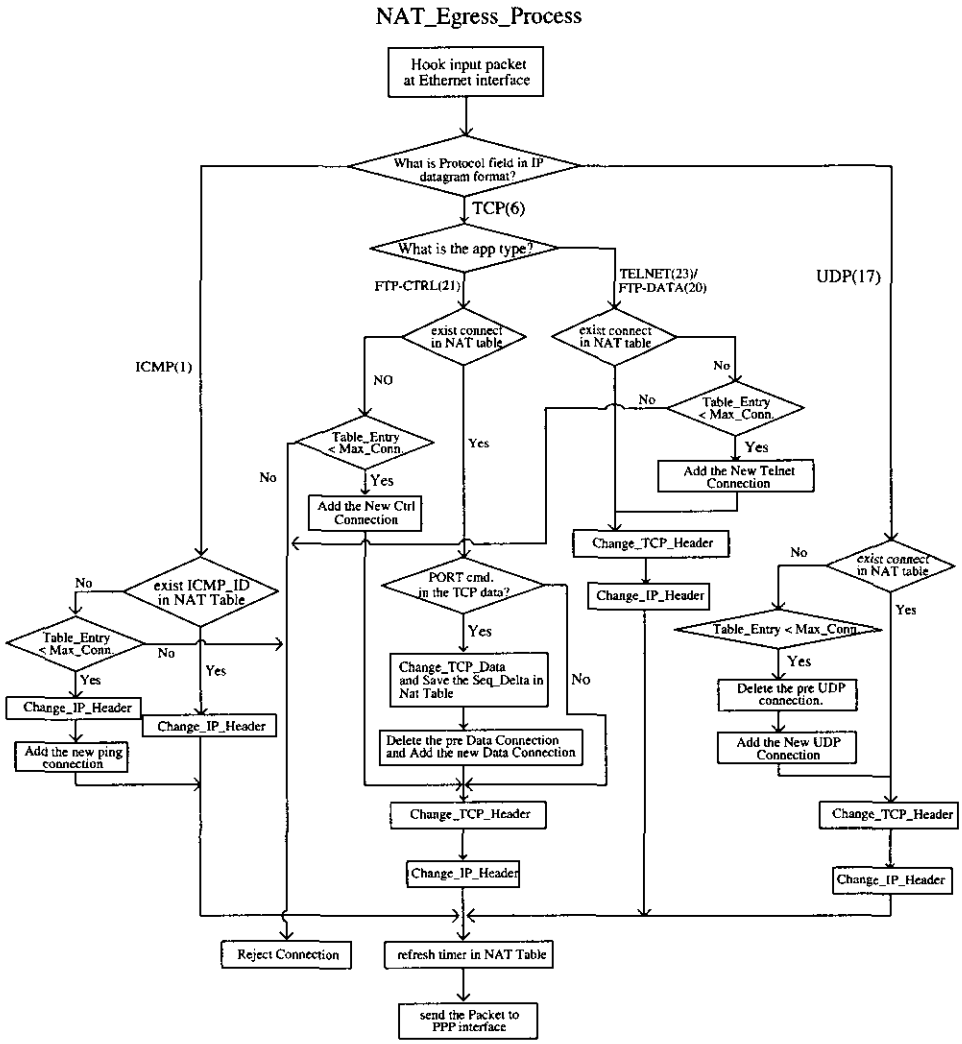


그림 4 NAT 라우터의 패킷 송신시 처리 절차

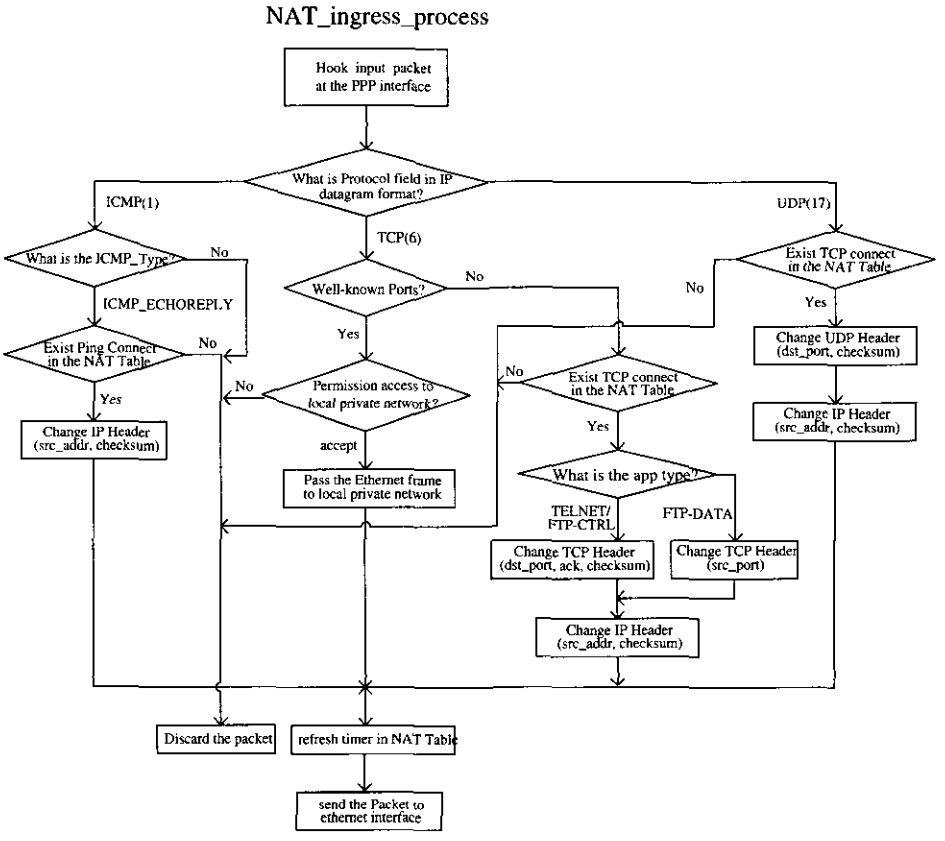


그림 5 NAT 라우터의 패킷 수신시 처리 절차

소만을 변경하면 된다.

두개의 서브넷 인터페이스로부터 패킷을 NAT가 수신하면 일반 라우터처럼 TCP/IP 헤더를 점검하여 잘못된 필드를 갖고 있는 패킷인 경우에는 NAT를 수행하지 않고 버리도록 한다. NAT는 TCP/IP 계층별로 필드들을 변환하도록 되어 있어 응용 프로그램에 따라 약간의 차이는 있지만 가장 먼저TCP/UDP가 갖고 있는 데이타 내용을 수정하고 그에 따라 TCP/UDP 헤더의 필드를 변경하고 마지막으로 IP 헤더를 변경하도록 한다. 이와 같은 방식으로 현재 NAT에서 처리할 수 있는 인터넷 서비스는 FTP, TELNET, PING, HTTP 등이 될 수 있다.

FTP는 제어 채널과 데이타 채널이 따로 존재하므로 하나의 FTP 연결에 두개의 연결 정보를 따로 NAT 테이블에 저장해야 하며, 제어 채널로 클라이언트(사설망 호스트)의 IP 주소와 데이타 패킷 전송 포트 번호가 PORT 명령 발생시에 전송되므로 사설망 호스트의 IP 주소를 변경해야 한다. TELNET 서비스는 TCP를 이용하며 한 채널로 제어 정보와 데이타를 모두 전송하므로 하나의 연결 정보만을 저장하여 TCP/IP 헤더 변경만을 수행하면 된다. PING 서비스는 네트워크 계층 없이 IP 계층에 ICMP type 0/8를 이용하여 제공되기 때문에 각 연결을 구분하기 위한 포트 번호가 없어 각 연결을 구분하기 위해서는 다른 필드를 이용해야 한다. PING에서 사용하는 ICMP에는 각 연결마다 Identifier 필드가 다른 값을 갖게 되므로 그 필드를 이용하면 각 연결마다 구별이 가능하다[11]. 따라서 ICMP에 있는 Identifier 필드를 NAT 테이블에 저장하여 해당 IP 주소로의 변환을 수행한다.

모든 연결 정보에는 타이머를 갖고 있어 일정 주기로 타이머 필드를 확인하고 타이머를 재설정을 하여 NAT 테이블의 연결 정보 유지가 가능하도록 한다.

4.2 TELNET 서비스를 위한 NAT 소프트웨어 구성

TELNET 서비스는 하나의 채널로 모든 정보 전송이 이루어지고 어떠한 경우에도 사설망 호스트의 정보 전달이 발생하지 않으므로 NAT는 하나의 연결 정보만을

NAT 테이블에 저장하여 기본적인 TCP/IP헤더 변환을 수행하도록 구성하면 된다[12]. NAT 테이블에는 근원지 IP 주소, 목적지 IP 주소, 근원지 포트 번호, 할당 포트 번호, 어플리케이션 유형, 타이머를 저장하도록 하는데, 어플리케이션 유형에는 목적지 포트 번호를 타이머에는 900초로 설정하도록 한다. TCP 헤더의 목적지 포트 번호가 23인 패킷이 수신되면 TELNET 서비스로 보고 NAT 테이블에서 근원지 IP 주소, 목적지 IP 주소, 근원지 포트 번호가 일치하는 연결 정보를 찾아 존재하지 않을 시에는 새로운 연결의 시작으로 보고 NAT 테이블에 연결 정보를 생성, 저장하며 TCP 헤더의 Code 필드 중 FIN bit가 설정된 패킷을 수신하였을 때를 TELNET 서비스의 종료로 보고 패킷의 TCP/IP 헤더 변경 후에 NAT 테이블에서 해당 연결 정보를 삭제한다.

4.3 FTP 서비스를 위한 NAT 소프트웨어 구성

FTP 서비스에서 데이타 전송을 필요로 하는 모든 사용자 명령은 사설망 호스트 정보를 포함한 PORT 명령으로 시작된다. PORT 명령에 포함된 호스트 정보를 사용하여 데이타 연결을 수행하기 때문에 사설망 호스트 IP 주소를 NAT 라우터의 인터넷 IP 주소로 변경하여 보내주지 않으면 데이타 연결을 수행할 수 없게 된다[13]. 따라서 NAT 라우터는 PORT 명령이 포함된 패킷을 수신했을 때에 사설망 호스트 정보를 데이타 연결 정보로 사용할 수 있도록 사설망 호스트 IP 주소, 포트 번호, 인터넷 IP 주소를 NAT 테이블에 새로 저장한 후, 사설망 호스트 IP 주소를 인터넷 IP 주소로 변경하고 그에 따른 Sequence 번호의 증감 크기를 NAT 테이블의 해당 제어 채널에 저장해야 한다. 그림6은 실제로 NAT FTP에서의 IP 주소와 포트 번호의 변화 흐름을 보여주는 예로써 사설망 호스트의 IP 주소는 10.10.0.20이고 인터넷 IP 주소는 150.150.56.47로 IP주소 변경으로 전체 데이타의 길이가 3만큼 증가하므로 TCP 헤더의Sequence를 3만큼 증가시키고 NAT 테이블에 3을 저장하여 인터넷으로부터 패킷이 수신되었을 때에는 3만큼 Sequence를 감소시켜 TCP Sequence를 보전할 수 있도록 한다.

4.4 PING 서비스를 위한 NAT 소프트웨어 구성

PING 서비스는 TCP/UDP를 사용하지 않고 IP 계층에서 ICMP를 이용하여 수행되므로 NAT 라우터는 IP와 ICMP를 처리하는 부분만으로 구성된다. ICMP Type 0인 PING 요청 패킷이 수신되면 ICMP Identifier 필드로 NAT 테이블에서 연결 정보를 찾아 연결 정보가 존재하지 않으면 근원지 IP 주소, 목적지 IP 주소, ICMP Identifier, 어플리케이션 유형과 타이머를 NAT 테이블에 저장하고 ICMP Type 8인 PING 응답 패킷이 수신되면 역시 ICMP

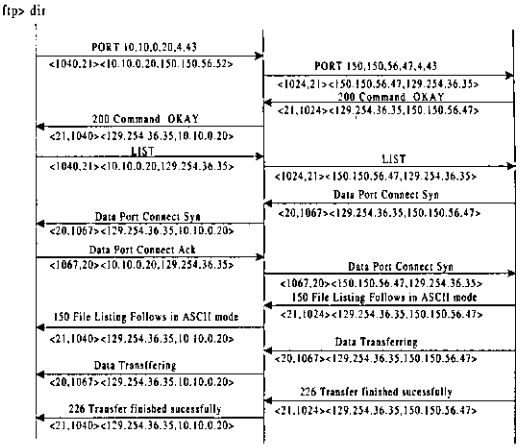


그림 6 FTP에서의 NAT Port Flow

Identifier를 이용하여 NAT 테이블에서 연결 정보를 찾아 NAT 기능을 수행한다[16].

5. NAT 구현과 시험 환경

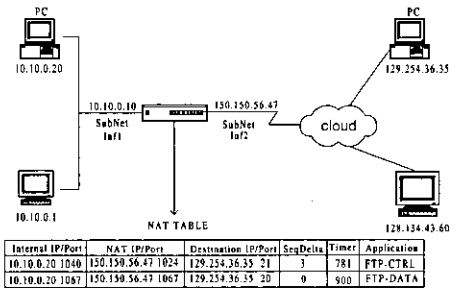
5.1 구현 환경

PowerPC 계열의 Microprocessor 860이 장착된 MBX 보드에 128Mbyte 메모리와 2개의 Ethernet 포트를 설치하였으며, 실시간 OS로 VxWorks와 개발 환경으로 Tornado를 선택하였다. NAT 프로그램은 vxWorks의 사용자 공간에서 실행시키며, 2개의 Ethernet 포트로 수신되는 패킷은 VxWorks의 Hooking 기능으로 NAT에 전달되도록 한다. 본 연구에서 선택한 구현 방법은 한 개의 인터넷 IP 주소와 TCP/UDP 포트를 함께 할당하는 방식으로 할당 가능한 TCP/UDP 포트 수는 전체 포트 65536개 중 각 인터넷 서비스에 할당된 1024개를 제외한 64512개까지 가능하며, 한 호스트에서 인터넷 접속 수를 256개로 제한한다. 각 서비스마다 혹은 TCP/UDP 연결 종류에 따라 NAT 테이블을 따로 생성할 때는 64512개 이상의 인터넷 연결을 허용할 수 있다.

5.2 시험 환경

그림 7은 NAT 라우터를 사용하여 사설망과 인터넷을 연결하는 네트워크 구성도로 사설망에 연결된 인터페이스는 IP 10.10.0.10로, 인터넷에 연결된 인터페이스는 IP 150.150.56.47로 설정하여 구성한다. 사설망(10.x.x.x)의 모든 호스트와 인터넷의 연결 시에 두개의 인터페이스 사이의 IP 주소 변환을 NAT 맵핑 규칙으로 설정할 때, 사설망에서 NAT 라우터로 수신되는 패킷의 현재IP주소, TCP/UDP 포트와 함께 새로 할당된 TCP/UDP 포트가 NAT 테이블에 등록되고 패킷의 TCP/IP 헤더를 라우터

의 맵핑 규칙에 따라 변환되어 송신된다. 그리고 인터넷 서버에서 NAT 라우터에 수신되는 패킷은 NAT 테이블에서 저장되어 있는 연결 정보를 찾아 다시 역으로 변환하여 사설망 호스트에 송신되기 때문에 두 호스트간의 통신은 가능하게 된다. 그 외에 NAT 테이블에 저장되는 필드는 인터넷 접속을 유지하기 위한 타이머, 사용하는 응용 프로그램과 Sequence 번호와 Acknowledgement 번호 유지를 위한 데이타 길이 변경분 정보 등이다. 사설망의 모든 호스트는 기본 라우팅 경로를 서브넷 Inf1인 10.10.0.10으로 설정하며, 그 외의 설정은 일반적인 경우로 한다.



Internal IP/Port	NAT IP/Port	Destination IP/Port	SeqDelta	Timer	Application
10.10.0.20 1040	150.150.56.47 1024	129.254.36.35 21	3	781	FTP-CTRL
10.10.0.20 1067	150.150.56.47 1067	129.254.36.35 20	0	900	FTP-DATA

그림 7 시험망 구성도 및 NAT 표

사설망 호스트에서 인터넷 호스트에 FTP, TELNET, PING, HTTP 등의 응용 프로그램을 사용하여 인터넷 접속을 시도한다. NAT 라우터를 사용하여 사설망 호스트(10.10.0.20)에서 인터넷 호스트 128.134.43.60으로 PING 요청 패킷을 전송할 경우 그림 8과 같은 결과를 나타내어 인터넷과의 연결을 볼 수 있다.

인터넷 호스트에서는 ping request 패킷을 받은 다음 Reply 패킷을 전송하기 전에 자신의 ARP 테이블을 참조하여 보낼 호스트의 MAC 주소를 검색하게 되는데, 이때 변환된 주소의 MAC 주소는 NAT 라우터의 인터넷 포트 MAC 주소가 된다. 이외에도 FTP, TELNET, HTTP 등의 응용 프로그램을 이용하여 사설망 호스트의 인터넷 접속이 가능하였다.

```
[vxWorks] > ping 128.134.43.60
PING 128.134.43.60: 56 data bytes
64 bytes from 128.134.43.60 : icmp_seq=0 ttl=254 time=0.32 ms
64 bytes from 128.134.43.60 : icmp_seq=1 ttl=254 time=0.1 ms
2 packets transmitted, 2 packets received, 0% packet loss
```

그림 8 NAT 기능을 이용한 PING 접속 시험 결과

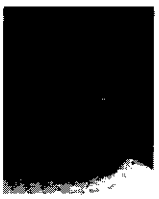
6. 결 론

본 연구에서는 IP 주소 고갈 문제를 해결하기 위한 NAT 기능을 네트워크 사이에서 데이타 전송을 중개하는 라우터에 적용하여 구현하고, NAT 기능은 인터넷에 등록되지 않은 IP 주소를 사용하는 사설망 호스트가 인터넷에 접속할 때, 사설망 호스트 IP 주소와 인터넷 IP 주소간의 상호 변환을 수행하여 사설망을 현상태로 유지시키면서 인터넷에 접속시킬 수 있다. 이는 NAT 라우터가 적절한 개수의 인터넷 IP 주소를 확보하고 있다가 사설망에서 인터넷으로의 접속 요청이 있으면 보유하던 인터넷 주소 중에서 사용되지 않고 있는 주소를 할당하여 준다. 물론 NAT 테이블에 미리 사설망이 지원하는 인터넷 서비스를 설정해 놓으면 사설망 호스트가 인터넷 서비스를 지원할 수도 있다. 네트워크를 구성하여 TCP/IP에서 보편적으로 사용되고 있는 PING, TELNET, FTP, HTTP와 같은 응용 프로그램들을 이용하여 사설망과 인터넷의 접속이 가능함을 확인하였다. NAT 라우터를 이용할 경우, 인터넷 라우팅 테이블에 사설망의 라우팅 정보가 없어도 사설망과 인터넷의 연동을 가능하게 하며, 인터넷 호스트들은 사설망의 존재를 알 수 없기 때문에 외부로부터의 접속을 막는 방화벽 기능도 함께 확인할 수 있었다. 비교적 적은 호스트들이 동시에 인터넷에 연결할 때 유용하지만 적절한 망 구성에 따라 일정 규모로도 확장될 수 있다.

참 고 문 헌

[1] E. Fleischman, A Large Corporate User's View of IPng, RFC 1687, August 1994.
[2] Y. Rekhter., B. Moskowitz, D. Karrenberg, and G. de Groot, Address Allocation for Private Internets, RFC 1597, March 1994.
[3] K. Egevang and P. Francis, The IP Network Address Translation (NAT), RFC 1631, May 1994.
[4] R. Droms, Dynamic Host Configuration Protocol, RFC 1531, October 1993.
[5] V. Fuller, T. Li , J. Yu, and K. Varadhan, Classless Inter-Domain Routing (CIDR) : an Address Assignment and Aggregation Strategy, RFC 1519, September 1993.
[6] P. Srisuresh and M. Holdrege, IP Network Address Translator (NAT) Terminology and Considerations, RFC 2663, August 1999.
[7] F. Baker, Requirements for IP Version 4 Routers, RFC 1812, June 1995.
[8] G. Tsirtsis and P. Srisuresh, Network Address Translation - Protocol Translation (NAT-PT), RFC 2766, February 2000.
[9] J. Postel and J.K. Reynolds, File Transfer Protocol , RFC 959, October 1985.
[10] J. Postel and J. Reynolds, Telnet Protocol Specification, RFC 854, May 1983.

[11] P. Mockapetris, Domain Names Implementation and Specification, RFC 1035, November 1987.
[12] R. Braden and D. Borman, C. Partridge, Computing the Internet Checksum, RFC 1071, September 1988.
[13] J. Postel, Transmission Control Protocol (TCP) Specification, RFC 793, September 1981.
[14] J. Postel, User Datagram Protocol (UDP), RFC 768, August 1980.
[15] J. Postel, Internet Control Message Protocol (ICMP), RFC 792, September 1985.
[16] 고문준, 민상원, TCP/IP 주소 및 포트 변환 기능에 관한 연구, 한국정보과학회 추계학술대회, 제 26 권 제 2호 pp 463 ~ 465, 1999년
[17] 민상원, 김황남, 이숙영, IP over ATM 장비들간 상호 운용성을 위한 구현 요구 사항, 한국정보과학회 논문지 (C), 제 5권 제 4호 pp. 488~498, 1999 년 8월



고 문 준

1994년 광운대학교 전산학과 학사. 1996년 광운대학교 전산학과 석사. 1996년 8월 ~ 2000년 9월 LG정보통신(주) 연구원. 2000년 10월 ~ 현재 SJTEK(주) 선임연구원. 관심분야는 IP/ATM, Traffic Control, Access Network

민 상 원

1988년 광운대학교 전자통신공학과 학사. 1990년 한국과학기술원 전기 및 전자공학과 석사. 1996년 한국과학기술원 전기 및 전자공학과 박사. 1990년 ~ 1999년 2월 LG 정보통신(주) 연구원. 1999년 ~ 현재 광운대학교 전자공학부 교수. 관심분야는 IP/ATM, Traffic Management, Network Performance