TCP/IP 주소 및 포트 변환 기능 구현에 관한 연구

고문준*, 민상원**
* LG 정보통신㈜ 고속교환실
경기도 안양시 동안구 호계동 (전화 0343-450-2025, FAX 0343-450-7104)
** 광운대학교 전자공학부
서울 노원구 월계동 447-1(전화·02-940-5552,FAX.02-942-5552)

Implementation of TCP/IP Network Address Translation and Port Network Address Translation

Moon-Jun Ko* and Sang-Won Min**
*ATM Division LGIC Ltd (mjko@lgic co kr)
**School of Electronics Engineering Kwangwoon University (min@daisy.kwangwoon ac.kr)

요 약

인터넷으로 연결된 모든 장치는 각 나라마다 정해진 권위기관으로부터 고유한 IP 주소를 할당 받게 되는데, 현재 Internet Network Information Center (Inter NIC)라는 조직에서 이를 전체적으로 관장하고 있다. 최근 인터넷 사용이 급속히 확산되면서 인터넷을 이용하는 모든 장치에 고유 IP 주소를 할당하게 될 경우 고유 주소 체계의 사용 가능한 IP 주소 고갈이라는 문제에 직면하게 되었다 그러나 이러한 문제는 내부 근거리 통신망(LAN)과 인터넷 사이에 IP 주소를 변환시켜 주는 역할을 하는 네트워크 주소 변환(NAT : Network Address Translation) 기능을 이용하여 보완할 수 있다 본 연구에서는 사설망 사용자의 인터넷 접속을 제공하는 것으로 기존 라우터에 NAT 기능을 적용하여 라우터가 보유한 공인 주소를 각 사용자가 공유하여 인터넷 접속을 시도하는 것으로 사설망의 IP 주소를 공인된 인터넷 주소로 변환시켜 외부로 전송하므로써 가능하다. 또한, 주소 변환 과정으로 사설망에서 사용하는 IP 주소가 NAT 기능으로 IP 주소가 변경되어 외부 침입자가 사설망의 존재를 알 수 없어 침입을 막는 간접적인 방화벽 기능도 수행한다.

1. 개요

최근 인터넷의 수요가 폭발적으로 증가하면서 인터넷에 새로 연결되는 모든 호스트들에게 고유한 IP 주소를 제공할 경우 IP 주소 부족을 발생한다[1] 그 결과 사용중인 IPv4 의 제한을 극복하고자 IP 주소 필드 길이가 대폭 확장되는 IPv6 또는 IPng라 불리는 새로운 인터넷 프로토콜을 개발하게 된다. 그러나 새로운 표준안은 인터넷에 적용되어 운영되기까지는 수년이 걸릴 것으로 예상되므로 IP 수명을 연장하기 위한 방법이 필요하게 되었다. NAT 기능은 주소 변경 방법을 이용하여 사설망 IP 주소를 인터넷 IP 주소로 변환시켜 주는 기능으로 NAT의 IP 주소 변환은 데이터 링크 계층에서 이루어지기 때문에 대부분의 응용프로그램 및 TCP/IP와는 무관하게 동작하게 되며 인터넷의 표준 프로토콜인 TCP/IP를 기준으로 구현한다.

2. NAT 기능 및 기능 구현 요구 사항

2.1 NAT 기능

NAT 기능은 인터넷에 등록되지 않은 IP 주소를 재사용한 사설망의 호스트를 인터넷에 연결시켜 인터넷의 모든 서비스를 받을 수 있게 한다. 비교적 적은 호스트들이 동시에 인터넷에 연결할 때 유용하지만 적절한 망 구성에 따라 적절한 규모도 확장될 수 있다[2] NAT 기능이 수행되는 라우터에서는 사설망과 인터넷 각각에 대한 최소 한 개 이상의 인터페이스를 갖고 있어야 하며 두 개 이상의 인터넷 인터페이스가 존재할 때에도 같은 NAT 테이블을 이용해야 하고 할당 가능한 주소 혹은 포트의 부족으로 인한 경우에는 패킷을 버리거나 ICMP Host Unreachable packet 을 보내야 한다 NAT는 사설망에 대한 구성 정보를 인터넷에 알려지지 않도록 해야 하지만 인터넷에서 유입되는 라우팅 정보는 사설망의 모든 호스트에게 전달되어야 한다.

NAT 기능은 기존 라우터를 변경하지 않고 사용할 수 있어야 하며 라우터의 각 포트에서 사설망 호스트의 패킷을 받아 NAT 맵핑 규칙(Mapping Rule)에 따라 IP 패킷의 발신 주소를 라우터의 인터넷 IP 주소로 변환하여 전송해야 한다 라우터가 인터넷 IP 주소를 여러 개를 보유하고 있을 때에는 IP 주소만을 변경하도 되지만 한 개의 IP 주소를 갖고 있을 시에는 TCP/UDP Port 번호도 변경해야 한다.

시설망에 쓰일 수 있는 IP 주소 범위는 표 1 과 같으며 다음과 같은 IP 주소를 갖은 패킷은 인터넷에서 동과 되지 않아 NAT 기능으로 인터넷에 연결한다.

Address Class Range	Network Address Range
A	10.0.0.0-10 255 255.255
B	172.16 0 0-172.31.255 255
C	192 168.0.0-192 168.255.255

표 1. 사설망 주소 범위

2.2 각 계층별 구현 요구 사항

IP는 TCP, UDP, ICMP를 위해 호스트간 데이터를 전송하는 역할을 담당하는 프로토콜로써 인터넷에서 사용되는 데이터 전송의 기본 단위를 정의한다 NAT 기능을 수행하면서 IP 헤더 중 Total Length는 IP 헤더 길이와 IP 데이터 길이의 합을 나타낸 것으로 NAT 라우터가 데이터 내용을 변경하여 데이터의 길이가 변경되면 Total Length 필드도 증감해야 한다

TCP에서는 가상적인 통신회선을 획립해서 통신을 하여 신뢰성 있는 통신을 하고 데이터를 적당한 세그먼트 크기로 전송단위에 맞게 분할한다. TCP 헤더 중 Source/Destination Port 번호는 양단간 연결을 구분하는 필드로 인터넷에 연결되는 공인 IP 주소가 한 개만 보유할 때는 사설망 호스트를 구별하기 위하여 NAT에서 Port 번호를 변경해야 한다. Checksum은 TCP Header와 데이터 전체로 계산된 것으로 TCP 헤더나 데이터 내용이 변경될 경우 Checksum을 다시 계산한다 *Sequence* 번호는 접속된 동안 데이터 흐름에서 데이터의 위치를 나타내고 Acknowledgement 번호는 발신지에게 다음에 들어와야 할 Octet 번호를 나타낸다. NAT 기능에서는 데이터 패킷 길이 변경에 따라서 Sequence 번호와 Acknowledgement 번호도 증감시켜 주어야 한다

2.3 NAT 와 FTP

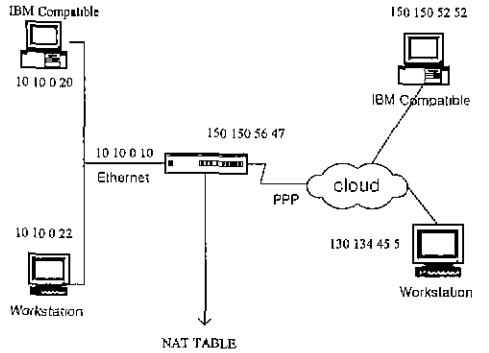
FTP는 FTP server와 client 사이에 제어 채널과 데이터 채널를 따로 유지하는데 제어 채널은 양단간의 연결 설정부터 연결 유지에 필요한 정보 전달 및 연결 해제에 관한 기능을 수행하고 데이터 채널은 양단간의 순수 데이터 전달 기능을 수행한다. 제어 채널에서 데이터 채널 연결를 위한 PORT command가 발생하는데 사설망 IP 주소가 패킷 데이터로 전달되므로 인터넷 IP 주소로 변환해야 한다. 패킷 데이터 크기 변경은 Sequence 번호와 Acknowledgement 번호에도 영향을 미쳐 크기 변화에 따른 Sequence/Acknowledgement 번호도 증감되어야 한다. 이렇게 하기 위해서 크기 변경에 대한 변경분을 계속 NAT 테이블에 저장하고 있어야 한다[3].

3. NAT 구현

3.1 라우터에서의 NAT 동작

기존 라우터는 수신된 패킷의 목적지 IP 주소를 라우팅 테이블에서 찾아 그에 해당하는 포트로 패킷을 전송하는 기능을 가지고 있지만 NAT 라우터에서는 이러한 기능이외에도 사설망 호스트에서 생성된 패킷의 발신 IP 주소를 인터넷 IP 주소로 변환 시켜주어 사설망의 라우팅 정보가 목적지 라우팅 테이블에 없더라도 인터넷에 접속이 가능하게도 하고, 반대의 역할도 수행하여 사설망 호스트에 정확하게 패킷이 전달되게 한다[4].

NAT 기능은 기존 라우터에 적용시켜 각 포트에서 패킷을 받아 NAT 맵핑 규칙에 따라 IP 패킷의 발신지 IP 주소를 고유한 인터넷 IP 주소로 변환하여 전송한다 패킷 수신 호스트는 패킷 송신 호스트에 대한 MAC 주소를 모르기 때문에 ARP 패킷을 보내게 되는데 NAT 라우터는 ARP 패킷의 목적 IP 주소가 자신의 인터넷 IP 주소와 일치할 경우 자신의 인터넷 IP 인터페이스 MAC 주소를 응답하게 된다.



Internal IP/Port	NAT IP/Port	Destination IP/Port	SeqDelta	Timer	Application
10 10 0 20 1040	150 150 56 47 1024	150 150 52 52 21	0	900	FTP-CTRL
10 10 0 20 1041	150 150 56 47 1041	150 150 52 52 1067	3	-	FTP-DATA

그림 1 시험망 구성도 및 NAT TABLE

본 연구에서 선택한 구현 방법은 외부로의 모든 통신에 대해 하나의 인터넷 IP 주소만을 사용하는 것으로 이는 IP 주소뿐만 아니라 각 접속마다 TCP의 포트도 함께 변환하여 사설망의 호스트를 구별할 수 있도록 한다. 이때 사용 가능한 TCP 포트 수가 64512개이고, 한 호스트에서 인터넷 접속 수를 256개로 제한하면, 한번에 접속할 수 있는 사설망 호스트의 최대 수는 254개로 결정된다. 사설망 호스트는 사용가능한 포트 범위 내에서 일부를 할당받게 된다.

그림 1과 같이 사설망(10.x.x.x) 모든 호스트들은 인터넷 IP 주소인 150.150.56.47로 변환되도록 NAT 맵핑 규칙을 설정할 때 사설망에서 라우터로 수신되는 패킷의 기존 TCP 포트와 함께 새로 할당된 TCP 포트가 NAT 테이블에 등록되고 이 패킷의 사설망 주소는 라우터의 맵핑 규칙에 따라 IP 주소와 TCP 포트가 함께 변환되어 송신된다. 그리고 목적지 호스트에서 라우터에 수신되는 패킷은 다시 역으로 변환되어 사설망 호스트에 송신되기 때문에 두 호스트간의 통신은 가능하게 된다. 그외에 NAT 테이블에 저장되는 필드는 인터넷 접속에 대한 갱신을 위한 타이머, 사용하는 응용 프로그램과 Sequence/Acknowledgement 번호 보전을 위한 패킷 길이 변경 정보 등이다

3.2 FTP에서의 NAT 구현

FTP 사용자가 실행하는 모든 명령은 PORT 명령과 함께 소켓 정보(IP 주소와 포트 번호)가 포함된 패킷이 생성된다. 소켓 정보에

사설망 호스트 정보가 전달되기 때문에 인터넷 호스트는 이러한 패

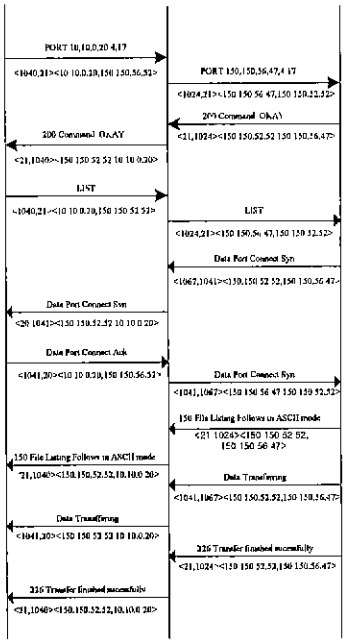


그림 2 FTP 에서의 NAT Port Flow

킷을 수신하면 새로운 데이터 연결을 수행할 수 없게 된다. 그래서 사설망 IP 주소 10.10.0.20 를 인터넷 IP 주소 150.150.56.47 로 변경하고 포트 번호 1041 는 NAT 테이블에 저장시킨다. 후에 해당 포트 번호로 데이터 패킷 수신될 때에 인터넷 IP 주소를 사설망 IP 주소로 변경하고 인터넷 Source port 번호 1067 를 FTP-DATA 포트 번호인 20 으로 변경해 줄 수 있게 한다. 이런 IP 주소 변경으로 전체 데이터 길이가 3 만큼 증가되는데 그에 따라 IP Total Length, TCP Sequence 번호도 3 만큼 증가하고 TCP Acknowledgement 번호는 3 만큼 감소하며 TCP/IP Checksum 도 재계산을 해 준다. 그림 2 는 FTP server 와 client 사이에서의 주고 받는 정보에 따른 포트 정보의 변경을 보여준다.

4.3 NAT 시험

NAT 기능을 시험하기 위해서 각 호스트의 IP 주소는 그림 1 과 같이 할당하고 NAT 라우터의 사설망 인터페이스로 IP 주소 10.1.1.10(0xffffff00)을 설정하고 인터넷 인터페이스로는 IP 주소 150 150 56 47(0xffffff00)을 할당한다. 인터넷의 모든 호스트가 갖고 있는 라우팅 테이블에는 사설망에 대한 라우팅 정보를 임의로 설정하지 않으며 사설망의 모든 호스트는 Default Router 로 10 10 0 10 을 설정한다. 사설망 호스트에서 인터넷 호스트에 FTP, telnet,ping, HTTP 등의 응용 프로그램을 사용하여 접속을 시도한다.

NAT 를 구현한 라우터를 사용하여 사설망의 호스트(10 10.0.20)에서 인터넷 호스트 150.150.52.52 로 ping 패킷을 전송할 경우 그림 3 과 같이 접속이 가능하게 된다 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 통하여도 사설망의 IP 주소만으로도 인터넷 접속이 가능하였다

```
[vxWorks] > ping 150 150 52 52
PING 150 150 52 52 : 56 data bytes
64 bytes from  150 150 52 52 : icmp_seq=0 ttl=254 time=0 32 ms
64 bytes from  150 150.52 52  icmp_seq=1 ttl=254 time=0 ms
2 packets transmitted, 2 packets received, 0% packet loss
```

그림 3 NAT 기능을 이용한 ping 접속 시험

4. 결론

본 연구에서는 IP 주소 고갈 문제를 해결하기 위한 NAT 기능을 네트워크간의 데이터 전송을 중개하는 라우터에 적용하여 구현, 시험하였다. NAT 기능은 인터넷에 등록되지 않은 IP 주소를 사용하는 사설망 호스트가 인터넷에 접속할 때 인터넷 IP 주소로 상호 변환시켜 줌으로써 사설망을 현상태로 유지시키면서 인터넷에 접속시켜 준다. 이는 라우터의 인터넷 주소 Pool 에 적절한 개수의 인터넷 IP 주소를 확보하고 있다가 사설망에서 인터넷으로의 접속 요청이 있으면 보유하던 인터넷 주소 중에서 사용되지 않고 있는 주소를 할당하여 준다. TCP/IP 에서 보편적으로 사용되고 있는 ping, telnet, HTTPD 와 같은 응용 프로그램들을 이용하여 사설망과 인터넷과의 접속을 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 firewall 기능도 함께 확인할 수 있었다.

참고문헌

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

[2] K.Washburn, J T Evans, "TCP/IP Running a Successful Network," Addison-Wesley Publishing Company, 1993

[3] Postel, J., Reynolds, J.K., "File Transfer Protocol," RFC 959, October 1985.

[4] Postel, J., " INTERNET CONTROL MESSAGE PROTOCOL," RFC 792, September 1981