호스트 라우팅을 이용한 공인 IP 주소 공유 기법

이광희°, 오명환, 최훈
충남대학교 컴퓨터공학과
{khlee°, mhoh, hchoi}@ce.cnu.ac.kr

Global IP Address Sharing Method using Host Routing

Kwang Hee Lee°, Myoung Hwan Oh, Hoon Choi
Department of Computer Engineering, Chungnam National University

요 약

IP 주소 부족 문제를 해결하기 위한 방법은 크게 두 가지로 나누어 볼 수 있다. 32bit 의 주소체계를 갖는 IPv4 를 128bit 의 주소체계를 갖는 IPv6 로 대체하는 장기적인 관점에서의 해결책과 네트워크 주소 변환(NAT : Network Address Translation) 기술을 이용하여 로컬 네트워크의 호스트들이 부족한 공인 IP 주소를 공유하는 단기적인 관점의 해결책이 있다. IPv4 에서 IPv6 로의 전이는 현재 구축된 모든 네트워크 장비와 인터넷에 연결된 호스트들의 수정이 필요하므로 많은 시간과 비용을 필요로 한다. 네트워크 주소 변환 기법은 로컬 네트워크에서 사설 IP 주소를 사용하고 로컬 네트워크의 호스트가 인터넷 접속 시 사설 IP 주소를 공인 IP 주소로 변환하여 인터넷 접속을 지원하는 범용적인 기술이다. 기존 네트워크 주소 변환 기술은 인터넷 통신의 기본 특성인 종단간 연결성(end-to-end connectivity)을 지원하지 못하고 종단 호스트간의 연결 매개 기술이므로 IPSEC 과 같은 종단간 통신 보안 지원을 목적으로 하는 기술에는 적용할 수 없다.

본 논문에서는 NAT 기술의 한계를 분석하고 이를 극복하기 위해 호스트 라우팅을 이용한 공인 IP 주소 공유 기법을 제안한다. 제안된 IP 공유 기법은 IP 패킷의 헤더나 페이로드의 어떠한 수정 없이 단지 참조에 의해 사설 네트워크의 호스트들에게 인터넷 풀 액세스 및 종단간 IPSEC 세션을 지원한다.

1. 서 론

단순하게 텍스트 기반 문서나 메일을 전송하기 위해 구축된 초창기 인터넷은 WWW 의 등장과 다양한 인터넷 응용의 등장으로 비약적인 성장을 거듭해 2005 년에는 약 10 억개의 호스트가 인터넷에 연결될 것으로 전망되고 있다.[1] IP 주소의 비효율적인 할당과 사용으로 인해 대두된 IP 주소 부족 문제는 현재 IPv4 의 주소체계의 인터넷에서 홈 네트워킹 등 다양한 응용들의 출현에 심각한 위협이 되었다. 주소 부족 문제를 해결하기 위한 방법은 크게 장기적인 관점과 단기적인 관점의 해결책이 있다. 장기적인 해결책으로 인터넷 데이터 전달 프로토콜인 IPv4 에서 IPv6 로의 전이는 현재 IPv4 의 문제점인 IP Security, 멀티캐스트, 이동성 지원, IP 주소 부족 문제를 해결하는 가장 좋은 방법이지만, 현재 구축되어 있는 IPv4 의 모든 네트워크 장비와 호스트를 수정해야 하므로 많은 시간과 비용이 필요하다. 현재 IPv4 에서 IPv6 의 전이에 대해 많은 연구가 수행 중이며 이미 실험 망이 구축되어 있으나 실제 완전한 IPv6 인터넷은 정확하게 언제 이루어 질지 아무도 예측하지 못한다. 따라서 현재 시급한 IP 주소 부족 문제를 해결하기 위해 가장 보편적으로 이용하고 있는 기술이 NAT [2][3][4] 기술이다.

NAT 기술은 로컬 네트워크에서 사설 IP 주소를 이용하고 로컬 네트워크의 호스트가 글로벌 네트워크와의 통신을 하려 할 때 호스트에서 생성된 패킷의 발신지 주소/발신지 포트를 변환하여 통신을 지원한다. 이러한 네트워크 주소 변환 기술은 발신지 사설 IP 주소를 정적으로 공인 IP 주소로 매핑하는 정적 NAT 와 동적으로 매핑하는 동적 NAT 가 있다. 또한 발신지 주소 뿐만 아니라 발신지 포트 번호를 변환하는 NAPT(Network Address Port Translation)로 나누어 볼 수 있다. 정적/동적 NAT 기술은 변환 테이블이 간단하고 발신지 주소 변환만을 수행하므로 단순하고 쉽게 구현할 수 있지만 IP 주소 재 사용률이 떨어진다. NAPT 기술은 발신지 주소와 발신지 포트를 변환하므로 정적/동적 NAT 기술보다는 우수한 IP 주소 재 사용률을 제공함으로써 현재 대부분의 네트워크 주소 변환 기술은 NAPT 방식을 채택하고 있다. 그러나 NAPT 는 포트 번호까지 변환하므로 IP 패킷 단편화(fragmentation)와 양방향 통신을 지원하지 못하는 단점이 있다. NAT 기술은 주로 로컬 네트워크의 게이트웨이나 에지 라우터에서 수행되며 IP 주소 부족을 해결하기 위한 단기적인 해결책이지만 본래 IP 네트워크의 통신 특성인 종단간 연결성을 제공하지 못하고 종단 호스트간 연결 매개 기술이므로 종단간 연결성을 요구하는 종단간 IPSEC[5] 세션을 지원할 수 없으며 IP 페이로드에 호스트의 인식 정보(호스트 IP 주소, 사용할 TCP/UDP 포트)를 포함하는 응용들을 지원 위해 각 응용 별 ALG(Application Level Gateway)가 필요하다.

본 논문에서 제안하는 호스트 라우팅을 이용한 공인 IP 주소 공유 기법은 로컬 호스트의 호스트 라우팅 테이블을 참조하여 발신지 주소가 결정되는 호스트 라우팅과, 발신지 주소에 의한 데이터 플로우 식별 방법, 로컬

o 본 연구는 산업자원부의 지역전략산업 석,박사 연구인력 양성사업의 지원으로 수행된 것임.

네트워크의 에지 라우터에서 로컬 호스트로 데이터 패킷을 전송하기 위한 L2 포워딩으로 구성된다. 본 논문에서 제안된 IP 공유 기법은 데이터 패킷에 어떠한 수정 없이 단지 참조에 의해서 데이터 플로우를 식별함으로써 ALG 없이 FTP, H.323, Messenger 와 같은 응용을 지원할 수 있으며 종단간 보안 통신을 요구하는 종단간 IPSEC 세션을 지원할 수 있다.

2. 관련 연구

2. 1 NAT/NAPT

NAT 는 로컬 네트워크와 글로벌 네트워크 경계에 존재하는 라우터에서 동작하며 네트워크 주소 변환을 수행한다. 이 방식은 현존하는 다양한 네트워크 주소 변환 방법들 중 가장 간단하며 양방향 네트워크 주소 변환을 지원한다. 또한, 주소 변환이 네트워크 계층에서만 일어나므로 주소 변환 속도도 빠르고 인터넷에서 이용되는 모든 서비스를 지원할 수 있다.

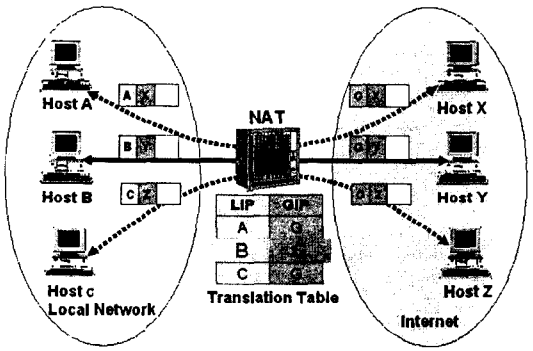

그림 1 NAT

NAPT 는 NAT 기법의 IP 주소 공유 효율성 문제를 극복하기 위해 나온 네트워크 주소 변환 방법이며 현재 가장 많이 사용되고 있는 기법이다. NAPT 기법은 IP 주소 하나를 로컬 네트워크의 여러 호스트가 공유하여 동시에 글로벌 네트워크와 통신할 수 있는 네트워크 주소 변환 방법이며 TCP/UDP 계층의 포트 변환을 통해 하나의 글로벌 IP 를 여러 대의 로컬 호스트가 공유할 수 있도록 N:1 바인딩을 지원한다.

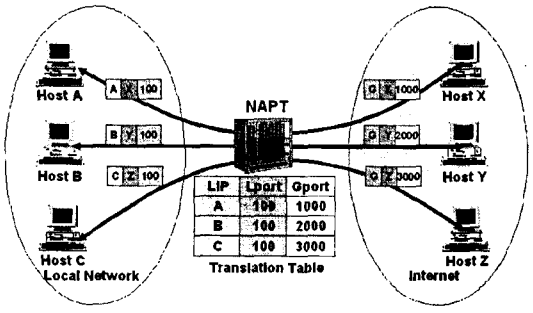

그림 2 NAPT

2.2 NAT-FS

NAT-FS(Network Address Translation by Flow Separation)[6] 는 기존의 네트워크 주소 변환 방식들과는 달리 <발신지주소, 목적지주소, 발신지포트, 목적지포트>로 데이터 플로우를 구분하고 이를 바탕으로 데이터 패킷 헤더의 주소만을 변환하는 특징을 가지고 있다. 따라서 기존의 NAPT 와 같이 하나의 공인 IP 주소를 로컬 네트워크의 모든 호스트가 공유하면서도 NAT 방식과 같이 DNS 와 연동한 양방향 통신 지원도 가능한 방식이다.

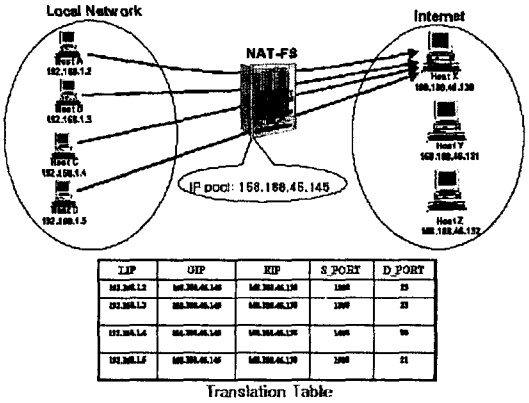

그림 3 NAT-FS

3. 네트워크 주소 변환 기술 분석

IPv4 에서 IPv6 로의 전이 과정에서 발생하는 IP 부족 문제의 단기적인 해결책인 다양한 네트워크 주소 변환 기법은 인터넷과 같은 글로벌 네트워크와의 경계에 존재하는 라우터/게이트웨이에서 사설 IP 주소를 공인 IP 주소로 변환하는 기술이다. 네트워크 주소 변환의 본질적인 특성인 데이터 패킷의 수정은 현재 존재하는 많은 인터넷 응용에게는 심각한 위협이 되고 있다. 예를 들어, 종단간 보안 통신을 제공하는 IPSEC 은 패킷을 전송하는 장비(라우터/게이트웨이)에서 일반적으로 패킷 전송 시 수정되는 패킷 헤더 정보 (TTL, Checksum 등) 외에는 패킷의 수정을 허용하지 않는다. 네트워크 주소 변환은 패킷의 정보를 수정해야 하는 기술이므로 IPSEC 과 같이 사용될 수 없다. H.323, FTP, Messenger 와 같은 인터넷 응용은 패킷의 페이로드에 패킷 생성 호스트의 인식 정보(발신지 주소, 발신지 포트)를 포함하므로 ALG 없이는 네트워크 주소 변환 장비에서 응용을 지원하지 못한다. 따라서 다양한 인터넷 응용을 지원하기 위해서 많은 ALG 가 필요하다. 이러한 문제점들은 모든 네트워크 주소 변환 기술이 갖고 있는 본질적인 문제이다.

4. 호스트 라우팅을 이용한 IP 주소 공유 기법

호스트 라우팅을 이용한 IP 주소 공유 기법은 기존의 네트워크 주소 변환 기술의 본질적 문제를 극복하기 위해 패킷에 어떠한 수정을 하지 않고 단지 패킷 헤더 정보 참조에 의해 로컬 네트워크와 글로벌 네트워크의 통신을 지원한다. 이를 위해서 로컬 호스트는 로컬 네트워크 내의 통신을 위해 하나의 사설 IP 주소를 할당 받고 글로벌 네트워크와의 통신을 위해 로컬 네트워크와 글

로컬 네트워크와의 경계에 존재하는 라우터/게이트웨이에 할당된 공인 IP 주소를 공유한다. 로컬 호스트는 할당된 두 개의 IP 주소를 하나의 이더넷 카드에 할당하기 위해 네트워크 환경 설정을 하면 다음 예와 같이 호스트 라우팅 테이블이 구성된다.

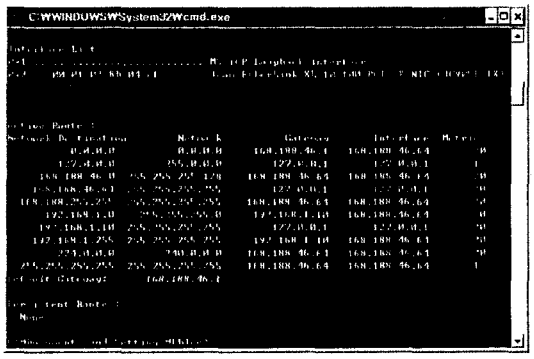

그림 4 호스트 라우팅 테이블

그림 4 에서, 로컬 호스트는 RFC 1918 에 정의된 사설 IP 주소 192.168.1.10 과 공인 IP 주소 168.188.46.64 를 통해 호스트 라우팅 테이블이 구성되어 있다. 로컬 호스트는 두개의 발신지 주소를 이용하여 통신할 수 있으며 통신하려는 목적지 주소에 따라 발신지 주소를 선택하기 위해 호스트 라우팅을 수행한다. 만약 통신하려고 하는 호스트가 로컬 네트워크내에 존재하는 호스트라면 192.168.1.0 의 네트워크 접두사를 공유함으로 라우팅 테이블을 참조하여 192.168.1.10 을 발신지 주소로 패킷을 생성하여 통신하고 글로벌 네트워크에 존재하는 호스트인 경우 디폴트 게이트웨이 주소인 168.188.46.1 를 참조하여 168.188.46.64 를 발신지 주소로 패킷을 생성하여 통신하게 된다. 따라서 네트워크 경계에 존재하는 라우터/게이트웨이에서는 패킷의 어떠한 수정 없이 단지 참조에 의해 데이터 플로우를 식별하고 일반적인 라우팅 만을 수행하면 로컬 네트워크와 글로벌 네트워크와의 통신을 지원할 수 있다.

다음은 네트워크 경계에 존재하는 라우터/게이트웨이에서 수행해야 할 데이터 플로우 식별 알고리즘을 플로우 차트로 나타낸 것이다.

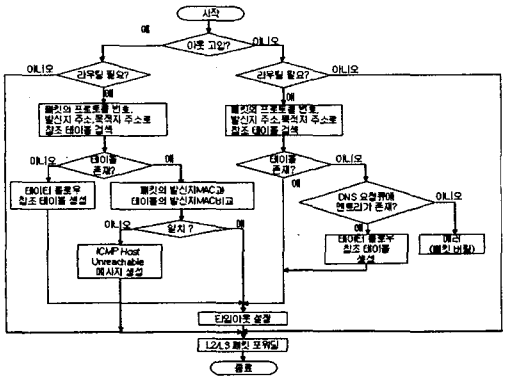

그림 5 데이터 플로우 식별 플로우 차트

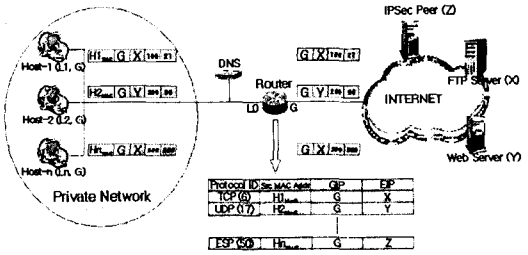

그림 6 호스트 라우팅을 이용한 공인 IP 주소 공유 기술 적용 예

그림 6 에서, 로컬 네트워크의 호스트는 사설 IP Ln 과 공인 IP G 로 네트워크 설정이 되어 있다. 로컬 네트워크 내의 통신은 호스트 라우팅 테이블을 참조하여 사설 IP Ln 을 이용하여 통신하고 인터넷의 서버와 통신하려 할 때는 공인 IP G 를 이용하여 패킷을 생성하고 라우터에게 전송한다. 라우터는 그림 5 의 데이터 플로우 식별 알고리즘에 따라 참조 테이블을 생성하고 일반 라우팅에 의해 패킷을 목적지 호스트로 전송한다. 서버로부터 전송되는 응답 패킷을 로컬 호스트에게 전송하기 위해 생성되어 있는 참조 테이블을 검색하여 엔트리를 찾고 엔트리에 이미 기록되어 있는 MAC 주소를 이용하여 L2 포워딩을 수행함으로써 로컬 호스트는 인터넷의 서버와 통신을 할 수 있다.

5. 결 론

본 논문에서 제안한 호스트 라우팅을 이용한 IP 주소 공유 기법은 기존의 네트워크 주소 변환 기술의 한계를 극복한 기법이며 패킷의 어떠한 수정 없이 단지 참조에 의해 데이터 플로우를 식별함으로 종단간 IPSEC 세션을 지원할 수 있으며 로컬 호스트에서 호스트 라우팅에 의해 발신지 주소가 결정되어 패킷이 생성되므로 ALG 없이 FTP, H.323, Messenger 등의 인터넷 응용을 지원할 수 있다. 그러나 동시에 다수의 로컬 호스트가 동일한 인터넷의 서버로 통신하려고 하는 경우는 현재의 데이터 플로우 식별 알고리즘에 의해선 지원하지 못하며 이는 향후 연구과제로 남긴다.

6. 참고 문헌

[1] Internet Growth, http://navigators.com/statall.gif
[2] P. Srisuresh and M. Holredge. " P Network Translator (NAT) Terminology and Considerations" , RFC 2663, IETF, August 1999.
[3] P. Srisuresh and K. Egevang. " Traditional IP Network Address Translation (Traditional NAT)" , RFC 3022, IETF, January 2001.
[4] M. Holdrege and P. Sriuresh. " Protocol Complications with the IP Network Address Translation" , RFC 3027, IETF, January 2001.
[5] Kent, S., and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.
[6] 윤승용, 이광희, 최창국, 전우직, " 데이터 플로우 구별에 의한 네트워크 주소 변환" , 한국정보과학회 2000 가을 학술발표논문집(III) pp.393-395.