다중 NAT-PT를 이용한 IPv4/IPv6 변환 개선방법

최원순° 노희영
강원대학교 컴퓨터과학과
{wonsoon°, rohhy}@kangwon.ac.kr

Improvement Method for IPv4/IPv6 Transformation using Multiple NAT-PT

Won-soon Choi° Hi-yong Roh
Dept. of Computer Science, Kangwon University

요 약

IPv6는 IPv4 기반의 인터넷의 주소고갈과 새로운 부가 기능등의 필요성 때문에 IETF에서 IPv4를 대체하기 위해 채택된 프로토콜이다. 하지만 IPv4를 어느 한순간에 IPv6로 대체하는 것은 불가능하기 때문에 기존 IPv4와의 호환및 연동을 위한 여러 메커니즘이 연구되었다. 그 중 NAT-PT(Network Address Translation-Protocol Translation)는 IPv4/IPv6 헤더 변환기술을 적용한 대표적인 변환 메커니즘이며, IP 패킷을 통과하는 망의 IP버전에 맞게 변환 시켜서 전송하는 방식이다. 그러나 모든 패킷들이 하나의 NAT-PT 노드로 집중되므로 병목현상이 발생하며, 이로 인해 성능저하가 발생한다. 본 논문은 NAT-PT 병목현상을 줄이기 위한 방안으로 DNS-ALG 기반된 서버를 이용하여 다중 NAT-PT를 사용한 방법을 제안한다.

1. 서 론

현재 인터넷에서 사용되는 IPv4는 32비트 주소체계를 사용하기 때문에 이론적으로 약 43억개의 인터넷 주소공간을 제공할 수 있다. 그러나 클래스 기반으로 주소를 할당하기 때문에 실제로 사용 가능한 주소는 B클래스, C클래스 주소로서 약 5~10억개로 추정된다. 따라서 기하급수적으로 늘어나는 인터넷 수요자와 이동통신의 All IP, 스마트 정보가전 서비스등에 따른 예상되는 주소 수요를 충족시킬 수 없다. 또한 IPv4의 멀티캐스트, QoS, 보안 기술은 패킷 헤더의 구조상 구현하기 어려운 부분들이 다수 내포되어 있다. 기존의 연구에서는 이러한 결점을 극복하기 위해 IETF에서는 IPng(IP next gengeration)그룹을 구성하여 IPv6프로토콜을 제안하고, 인터넷 주소체계로 채택되었다[1].

그러나, IPv6가 비록 이전버전보다 향상된 기능을 제공하고 있음에도 불구하고 기존의 IPv4네트워크를 IPv6네트워크로 일시에 대체하는 것은 현실적으로 어려운 일이므로 기존 IPv4와의 호환 및 연동을 위한 여러 메커니즘들이 연구되었다.

그 중 NAT-PT(Network Address Translation-Protocol Translation)는 IPv4/IPv6 헤더 변환기술을 적용한 대표적인 변환 메커니즘이며, IP 패킷을 통과하는 망의 IP 버전에 맞게 변환 시켜서 전송하는 방식이다. 즉, 기존의 패킷을 다른 버전의 IP헤더로 변형시키게 되므로 망의 호스트는 별다른 설정이 필요 없이 사용 할 수 있다.

그러나 한 세션에 대한 모든 응답과 요청은 동일한 NAT-PT를 통해 라우팅되어야 하는 제약으로 모든 패킷들이 하나의 NAT-PT 노드로 집중하기 때문에 병목현상이 발생하며, 이로 인해 성능저하가 발생된다.. 본 논문은 기존의 DNS-ALG 기반된 서버를 이용하여 다중 NAT-PT를 사용한 방법을 제안한다.

2. 관련연구

2.1 IPv4/IPv6 전환기술

현재까지 표준화되고 있는 IPv6 전환 메커니즘은 헤더 변환기술로 IPv6 전용호스트가 IPv4 전용 호스트와 통신하기 위해 IPv4/IPv6 변환(translation)기술이 있고, 망관점에서는 IPv6 호스트가 타 망의 IPv6호스트와 통신하고자 할때 망 사이에 IPv4망이 존재하다면, IPv6-in-IPv4 터널링 기술이 사용된다.

변환 기술은 IP 패킷을 통과하는 망의 IP 버전에 맞게 변환시켜서 전송하는 방식이다. 변환방식은 기존의 패킷을 다른 버전의 IP헤더로 변형시키게 되므로 망의 호스트는 별다른 설정이 필요 없이 그대로 사용할 수 있는 장점을 가지고 있다. 그러나 IP패킷의 변형으로 인해서 IP망의 전체적인 투명성을 제공하지 못하는 단점을 가지고 있다. 변환기술을 적용한 연동기술로는 NAT-PT, SIIT, BIS, BIA등이 있다.

터널링 방식은 전송하려는 IP패킷과 통과하는 망에서 사용하는 IP의 버전이 서로 다른 경우에 전송되는 IP 패킷을 통과하는 망의 IP헤더로 캡슐화화여 전달하는 방식이다. 터널링 방식은 IP해더를 추가하므로 오버헤드가 생기지만 기존의 패킷을 변형시키지 않으므로 어플리케이션에 대해서 투명한 통신이 가능하다. 터널링 방식을 적용한 연동방안으로 DSTM, ISATP 그리고 6to4등이 있다[2].

아래의 그림1은 여러 프로토콜 전환 메커니즘의 특징 및 주된 용도, 및 장·단점 등을 정리하고 있다[3].

[illegible]	[illegible]			
NAT-PT	•IPv6-only 호스트와 IPv4-only 호스트간 통신	•듀얼스택 필요 없음	•종단간 IPSec 부재 •전용 서버가 네트워크 실패(failure)의 요소	•전용 서버 필요 •IPv6를 위한 DNS 지원 필요
TCP-UDP 릴레이	•전용 서버에서 IPv6와 IPv4 간의 변환	•프리웨어	•종단간 IPSec 부재 •전용 서버가 네트워크 실패의 요소	•전용 서버 필요 •IPv6를 위한 DNS 지원 필요
BIS	•IPv4-only 호스트가 IPv6-only 호스트와 통신개시	•종단시스템만 변화 필요	•모든 스택의 업그레이드 필요	•업그레이드된 IPv4 프로토콜 스택 필요
DSTM	•IPv6 주소만 가지고 있는 dual-stack 호스트	•주소 풀에서 할당된 임시 IPv4 주소 사용	-	•일시적인 global IPv4 주소 할당을 위해 전용 서버 필요
SOCKS-based *ipv6/IPv4* Gateway	•IPv6-only 호스트와 IPv4-only 호스트간 통신	•프리웨어	•라우터에 부가적인 소프트웨어 설치 필요	•호스트와 라우터에 client와 gateway 소프트웨어 설치

그림 1 IPv6/IPv4 전환 메커니즘의 비교

2.2 NAT-PT의 구조

NAT-PT는 SIIT 프로토콜 변환과 NAT(Network Address Translation) 및 DNS-ALG(Application Level Gateway)등 적절한 ALG의 동적 주소 변환을 조합하여 IPv6 전용 노드와 IPv4 전용 노드 사이에서 상호 통신을 가능하도록 한다. 아래 그림2는 NAT-PT의 구조이다.

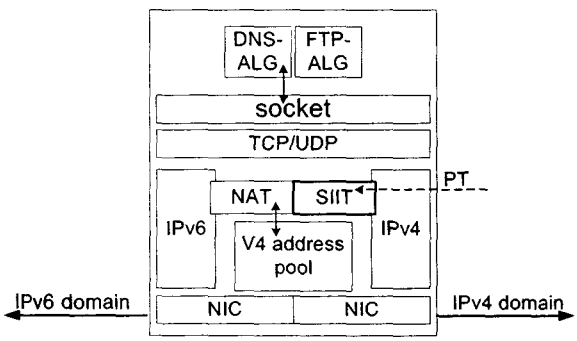

그림 2 NAT-PT 구조

NAT-PT는 NIC(Network Interface Card)로부터 패킷을 캡쳐하여 해당 IPv6 주소에 할당된 IPv4주소가 현재 IPv4/IPv6 맵핑 테이블에 없으면 IPv4 주소풀로부터 동적으로 IPv4 주소를 선택하여 IPv6주소에 할당하고, 그 결과를 IPv4/IPv6 맵핑 테이블에 기록한다. NAT-PT는 IPv6-IPv4 주소를 서로 바인딩(Binding)하여 각 주소 영역 사이에 오가는 데이터그램에 투명한 라우팅을 제공한다[4].

NAT-PT는 패킷 변환을 SIIT를 기반으로 수행한다. 또한 동적으로 주소를 할당하고 변환하기 위해서는 페이로드(Payload) 영역에 IP 주소나 포트 정보를 포함한 응용들에 의해 추가적인 요구사항이 발생하는데, 이를 지원하기 위해ALG를 사용한다. 대표적인 예로 DNS-ALG와 FTP-ALG등이 있으며, DNS -ALG는 AAAA와 A형식의 변환 및 DNSv4와 DNSv6간의 주소 정보 교환 역할을 수행한다[5].

2.3 NAT-PT의 제약조건

NAT-PT 각 요소별 제약조건은 다음과 같다. 우선 토폴로지 제약을 받는다. NAT-PT를 거쳐 IPv4망과 IPv6망이 통신할 경우, 한 세션에 대한 모든 응답과 요청은 동일한 NAT-PT를 거쳐 라우팅되어야 한다. 그 이유는 NAT-PT의 IPv4/IPv6 맵핑 테이블에 등록되어 있지 않는 IP통신은 무효화 되기 때문이다. 이러한 라우팅 경로를 보장하기 위해서는 NAT-PT를 유일한 경계 라우터로써 설치하는 것이다.

또한 프로토콜변환 제약을 받는다. 상당수의 IPv4 필드가 IPv6에서 상당히 많이 변화되었으므로 직접적인 의미 변환을 수행할 수 없다. IPv4와 IPv6 프로토콜 변환에 대한 상세한 내용은 SIIT에 따른다. 그리고 NAT-PT는 IP 계층의 주소변환을 수행하므로, 상위계층에서 IP주소를 사용하는 어플리케이션은 정상적인 동작을 수행할 수 없다. 이 경우에는 해당 어플리케이션을 지원하는 ALG가 필요하다.

NAT-PT는 종단간 네트워크 계층 보안이 불가능하다는 단점이 있다. 또한 전송 및 응용 계층 보안에서 IP주소를 사용할 경우에도 불가능하다. 이는 NAT 기능의 자체적인 한계이다. 예를 들어, NAT-PT와 독립적인 종단간 IPSec의 경우, IPSec의 특성상 서로 다른 주소 영역사이(IPv4망과 IPv6망 사이)를 교차하는 것이 불가능하다. 따라서 IPSec 네트워크 레벨 보안을 추구하는 두 종단 노드들은 IPv4 또는 IPv6 중 하나를 둘 다 제공해야 한다.

일반 DNS 변환에서 DNS-ALG는 사용될 수 있으나, 보안 DNS에는 적용할 수 없다. IPv6 도메인내에 있는 신뢰 DNS서버는 IPv4영역으로부터 수신한 DNS 요청에 대한 응답에 서명할 수 없으며, 결과적으로 서명된 DNS 응답을 기다리는 IPv4 종단노드는 NAT-PT에 의해 변형된 응답을 거부할 것이다. 그러나 이러한 단점은 IPv4 영역으로부터

접근하는 IPv6 도메인내의 서버만이 이러한 제약을 겪게 된다[4].

3. NAT-PT의 개선방안

NAT-PT는 토폴로지의 제약에 의해 NAT-PT를 거쳐 IPv4 망과 IPv6망이 통신할 경우, 한 세션에 대한 모든 응답과 요청은 동일한 NAT-PT를 거쳐 라우팅되어야 한다.

모든 IPv6노드들이 하나의 NAT-PT노드로 집중되고 병목현상이 생길 수 있으며, 이로 인해 성능저하가 문제시되어 그림 3과 같이 도메인 경계에 다중의 NAT-PT를 두어 병목현상을 해결하고자 한다[6].

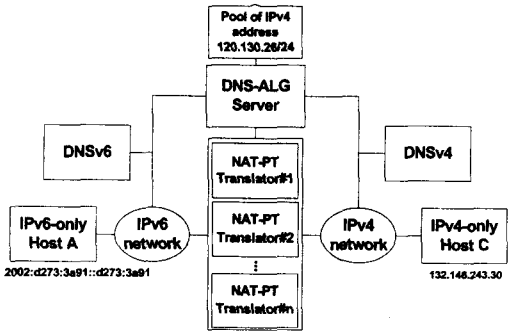

그림 3 개선된 NAT-PT

IPv4망과 IPv6망이 서로 다른 망과 통신하고자 하며 반드 시 DNS서버로 도메인 네임 해석과정을 거쳐서 응답받은 IP주소를 목적지로 하여 접속한다는 것을 이용하였다. 이를 이용하여 사용자가 도메인 네임 해석 요구를 DNS-ALG서버에게 요구할 때 DNS-ALG 서버는 가지고 있는 IPv4주소풀을 이용하여 IPv4호스트와 IPv6호스트사이의 세션 정보를 구성하고 구성된 정보를 다중의 NAT-PT 전달해주고, 경계라우터는 다중의 NAT-PT에 라운드로빈 방식으로 해당 패킷을 전달해 주고 이를 변환하도록 한다.

그림 4는 IPv4 호스트 B가 IPv6 호스트 A와 통신하고자 할 때 NAT-PT와 DNS-ALG Server의 상호운영에 대해서 설명한 그림이다. 맨 처음 호스트 B의 name resolver는 통신하고자 하는 호스트 A에 대해 ①와 같이 데이터그램을 보낸다. 이 데이터 그램은 IPv4/IPv6 네트워크 사이의 경계라우터에 위치하는 DNS-ALG Server를 거치게 되고 DNS-ALG Server는 ②와 같이 IPv6 도메인으로 가는 A 레코드에 대해 DNS query를 변형시킨다.

IPv6 네트워크의 DNS서버로부터 IPv4 네트워크로 전송되는 DNS response는 DNS-ALG server에 의해 ⑤처럼 매핑정보를 구성하고 IPv4 호스트와 IPv6 호스트 사이의 세션 정보를 다중의 NAT-PT에 전달해 준다. DNS-ALG Server가 호스트 B에게 "A" 레코드를 전달하면 호스트 B는 매핑정보를 이용하여 패킷을 전달한다.

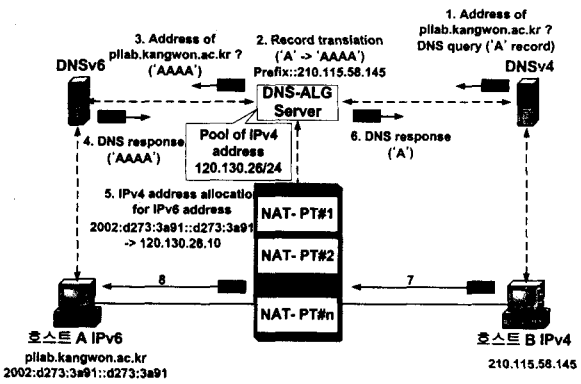

그림 4 개선된 NAT-PT 동작방식

경계라우터에 호스트 B로부터 패킷이 도착하면 라운드로빈 방식으로 NAT-PT에 전달되고 세션정보를 이용하여 패킷이 다시 변환되고 두 노드간의 통신이 가능해지게 된다.

4. 결론 및 향후과제

본 논문에서는 IPv4/IPv6 헤더 변환 기술인 기존의 NAT-PT의 단점인 하나의 NAT-PT를 통과하여 발생하는 병목현상을 줄이고자 DNS-ALG 서버를 이용한 NAT-PT 분산 방법을 제안하였다. DNS-ALG서버에 주소풀을 두어 IPv4/IPv6 호스트간의 세션정보를 다중NAT-PT를 전송해주는 서버로 설정하고 다중 NAT-PT를 이용하여 IPv4/IPv6 변환 서비스를 받게 됨으로 인해 NAT-PT의 토폴로지 제약을 해결할 수 있고 동시에 발생하는 병목현상 문제를 해결할 수 있을 것으로 기대된다. 그럼에도 불구하고 프로토콜 변환에 따른 어려움이 존재하고, 또한 종단간의 네트워크간의 보안도 불가능하다.

향후 연구과제로는 제안된 논문으로 시스템을 구축해보고 다중 NAT-PT에 따른 효과적인 Load Balance방법과 fail over를 고려해 봐야 할 것이다.

5. 참고 문헌

[1] S. Deering, R. Hinden, "Internet Protocol, Version 6(IPv6) Specification," IETF RFC 2460, December 1998

[2] 신명기 "IPv4/IPv6 변환기술", TTA저널 79호, 2002.

[3] 문영성 "IPv6 지원을 위한 상호운영성 연구를 기반으로 한 DNS 적용 방안 연구", 한국인터넷정보센터, Jan. 2004.

[4] G. Tsirtsis, "Network Address Translation-Protocol Translation(NAT-PT)", RFC2766, Feb 2000.

[5] E. Nordmark, "Stateless IP-ICMP Translation Algorithm(SIIT)", RFC2755, Feb 2000.

[6] S. Satapati, "NAT-PT Applicability, "draft-satapati-v6ops-natpt-applicability-00, Oct. 2003.